CWC

CrossWind | Consulting

Policies Only

April 2022

(Next Review Date: October 2022)

CWC

Contents

PEOPLE POLICIES - GENERAL 2

SCHEDULE 1 – DIVERSITY POLICY 2

SCHEDULE 2 – ANTI-HARASSMENT AND BULLYING POLICY 5

SCHEDULE 3 – ANTI-SLAVERY AND HUMAN TRAFFICKING POLICY 8

SCHEDULE 4 – CLIENT EXPENSES POLICY 10

SCHEDULE 5 – GRIEVANCE PROCEDURE POLICY 13

SCHEDULE 6 – SOCIAL MEDIA POLICY 15

PEOPLE POLICIES – TIME OFF & SICKNESS 18

SCHEDULE 7 – ANNUAL LEAVE POLICY 18

SCHEDULE 8 – SICKNESS ABSENCE POLICY 21

PEOPLE POLICIES – PERFORMANCE & DISCIPLINARY 25

SCHEDULE 9 – DISCIPLINARY AND CAPABILITY PROCEDURE 25

SCHEDULE 10 – DISCIPLINARY RULES POLICY 27

FRAUD & FINANCIAL CRIME 30

SCHEDULE 11 – ANTI-MONEY LAUNDERING POLICY 30

SCHEDULE 12 – FRAUD POLICY 34

SCHEDULE 13 – ANTI-CORRUPTION AND BRIBERY POLICY 37

SCHEDULE 14 – ANTI-FACILITATION OF TAX EVASION POLICY 43

HEALTH & SAFETY 48

SCHEDULE 15 – HEALTH AND SAFETY POLICY 48

SCHEDULE 16 – COVID-19 POLICY 50

DATA GOVERNANCE & PROTECTION 54

SCHEDULE 17 – DATA PROTECTION POLICY (GDPR) 54

SCHEDULE 18 – CONFIDENTIALITY POLICY 66

SCHEDULE 19 – RECORDS MANAGEMENT POLICY 71

INFORMATION TECHNOLOGY 73

SCHEDULE 20 – IT AND COMMUNICATIONS SYSTEMS SECURITY POLICY 73

SCHEDULE 21 – BRING YOUR OWN DEVICE TO WORK (BYOD) POLICY 79

OTHER POLICIES 86

SCHEDULE 22 – WHISTLEBLOWING POLICY 86

SCHEDULE 23 – ENVIRONMENTAL POLICY 90

CWC

PEOPLE POLICIES - GENERAL

SCHEDULE 1 – DIVERSITY POLICY

1. ABOUT THIS POLICY

1.1 This policy sets out our approach to diversity at work. It applies to all aspects of employment with us, including recruitment, pay and conditions, training, appraisals, promotion, conduct at work, disciplinary and grievance procedures, and termination of employment.

1.2 This policy covers all employee.

1.3 This policy forms part of your contract of employment.

2. HR has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness and dealing with any queries about it. The Managing Partners are responsible overall for diversity and inclusion.

3. BACKGROUND

3.1 The diversity strategy for CWC has been set by Lisa Whiffen, one of our Managing Partners. Lisa has been involved in promoting diversity throughout her career and has mentored many women and men in Banking and Finance. In 2011, Lisa worked closely with Sarah Churchman in re-launching the PWC diversity program in the UK. Led by Sarah – a very high-profile advocate for diversity in the UK - this program has since received numerous awards for inclusion and promotion of diversity in business. Lisa is also closely involved with Aspierations, an organisation with the aim of promoting and supporting those with high-functioning autism in Financial Services.

3.2 It is a stated strategy of CWC to actively promote diversity within all levels of the organisation, to support diversity in business, and to reflect the very best practices within Financial Services.

3.3 UK employment law legislation covers a number of requirements relating to both equality and diversity. Whilst CWC does of course adhere to such requirements, it is our belief that all organisations should stretch their practices beyond the confines of legislature; research has demonstrated that increased diversity has a strong positive effect on the financial performance of organisations[1], and we believe as an organisation that a commitment to diversity positively impacts the working experience of all employee and underpins the supportive culture of the organisation.

3.4 Our policy towards diversity covers all employment engagements. We expect our people to follow not just the details of the policy, but also the spirit underpinning this policy, and we also expect people to challenge practices that may constrain diversity within the organisation. We welcome all suggestions for improvements to our policy and encourage open dialogue in this area.

4. AIM

4.1 Ensure that no employee is held back as a result of age, disability, race, religion, gender, or gender/sexuality orientation.

4.2 Exceed all requirements under diversity legislation, and reflect the very highest industry standards.

[1] https://www.mckinsey.com/business-functions/organization/our-insights/delivering-through-diversity

4.3 Actively support any employee facing temporary or permanent work-life pressures, with a view to removing such pressures where possible, and supporting employee subject to these pressures with regard to continued progression through the organisation.

4.4 Actively support any employee with a defined physical or behavioural impairment, with a view to removing related pressures where possible, and supporting employee subject to these pressures with regard to continued progression through the organisation.

4.5 Be open and supportive at every level, and free from bullying, harassment and discrimination.

4.6 Ensure that all employee and associates are aware of the diversity policy and are engaged with the diversity agenda, and are aware that actions that are against both the spirit or the detail of the diversity policy may be considered disciplinary offences.

5. PROTECTED CHARACTERISTICS

5.1 The Equality Act 2010 protects nine groups of people from unlawful discrimination. These groups are known as 'protected characteristics'. They are:

- age
- disability
- sexual orientation
- religion and belief
- race
- sex
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity

5.2 All employees, no matter whether they are part-time, full-time, or temporary, will be treated fairly and with respect. When CWC selects candidates for employment, promotion, training, or any other benefit, it will be on the basis of their aptitude and ability.

5.3 All employees will be given help and encouragement to develop their full potential and utilise their unique talents. Therefore, the skills and resources of our organisation will be fully utilised and we will maximise the efficiency of our whole workforce.

6. COMMITMENTS

6.1 To create an environment in which individual differences and the contributions of all team members are recognised and valued.

6.2 To create a working environment that promotes dignity and respect for every employee.

6.3 To not tolerate any form of intimidation, bullying, or harassment, and to discipline those that breach this policy.

6.4 To make appropriate and proportionate training, development, and progression opportunities available to all employee in line with their role and length of contract.

6.5 To promote diversity in the workplace, which CWC believes is good management practice and makes sound business sense.

6.6 To encourage anyone who feels they have been subject to discrimination to raise their concerns so we can apply corrective measures.

6.7 To **require** anyone who feels they have witnessed a fellow employee be subjected to discrimination to raise their concerns so we can apply corrective measures.

6.8 To encourage employees to treat everyone with dignity and respect.

6.9 To regularly review all our employment practices and procedures so that fairness is maintained at all times.

6.10 CWC will inform all employees that a diversity policy is in operation and that they are obligated to comply with its requirements and promote fairness in the workplace. The diversity policy is fully supported by senior management. Our policy will be monitored and reviewed to ensure that equality and diversity is continually promoted in the workplace.

6.11 Excepting where we have specific legal requirements relating to Equality, CWC does NOT maintain an Equality policy. It is the view of senior management that where there is a conflict between equality and diversity, the commitment to diversity has the higher priority. Diversity is more complex than equality and requires a more thoughtful approach than applying equal treatment for all. This does not of course absolve the company from their obligations under employment law where they pertain to equality rights.

7. REPORTING PROCEDURES

7.1 CWC management fully support the diversity policy of the company. To this end we have established the following reporting mechanisms for anyone who wishes to raise a concern or suggestion regarding diversity.

7.2 In the first instance, diversity issues should be raised with line management wherever appropriate. Line management are expected to deal with the situation and to consider if formal reporting is required. Formal reporting is required whenever the HR agrees that a concern is justified – *whether or not it is fully resolved*. This enables CWC to monitor the culture of the workplace in this area.

7.3 All employee – whether permanent or contract – have the absolute right to formally report their concerns without approaching line management first.

7.4 Formal reporting should be via email in the first instance to the HR department, who may contact you for further detail and who will maintain the Diversity reporting log.

7.5 The HR department will take responsibility for engaging the correct personnel to deal with the matter, if it is still open.

7.6 The HR department will contact the parties involved at the conclusion of the process to obtain agreement that the matter has been satisfactorily dealt with, and will sign off the log accordingly.

7.7 Where any matter is not considered closed by all related parties, it will be forwarded to the Head of Diversity, who will then take responsibility for closing the matter and taking action as appropriate.

7.8 The Diversity reporting log will be reviewed regularly by the designated members, and may be used for disciplinary, appraisal and development purposes.

SCHEDULE 2 – ANTI-HARASSMENT AND BULLYING POLICY

1. ABOUT THIS POLICY

1.1 CWC is committed to providing a working environment free from harassment and bullying and ensuring all employee are treated, and treat others, with dignity and respect.

1.2 This policy covers harassment or bullying which occurs at work and out of the workplace, such as on business trips or at work-related events or social functions. It covers bullying and harassment by employee (which may include consultants, contractors and agency workers) and also by third parties such as customers, suppliers or visitors to our premises.

1.3 This policy covers all employees.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. WHAT IS HARASSMENT?

2.1 Harassment is any unwanted physical, verbal or non-verbal conduct that has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them. A single incident can amount to harassment.

2.2 It also includes treating someone less favourably because they have submitted or refused to submit to such behaviour in the past.

2.3 Unlawful harassment may involve conduct of a sexual nature (sexual harassment), or it may be related to age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation. Harassment is unacceptable even if it does not fall within any of these categories.

2.4 Harassment may include, for example:

(a) unwanted physical conduct or "horseplay", including touching, pinching, pushing and grabbing;

(b) continued suggestions for social activity after it has been made clear that such suggestions are unwelcome;

(c) sending or displaying material that is pornographic or that some people may find offensive (including emails, text messages, video clips and images sent by mobile phone or posted on the internet);

(d) unwelcome sexual advances or suggestive behaviour (which the harasser may perceive as harmless);

(e) racist, sexist, homophobic or ageist jokes, or derogatory or stereotypical remarks about a particular ethnic or religious group or gender;

(f) outing or threatening to out someone as gay or lesbian;

(g) offensive emails, text messages or social media content; or

(h) mocking, mimicking or belittling a person's disability.

2.5 A person may be harassed even if they were not the intended "target". For example, a person may be harassed by racist jokes about a different ethnic group if the jokes create an offensive environment.

3. WHAT IS BULLYING?

3.1 Bullying is offensive, intimidating, malicious or insulting behaviour involving the misuse of power that can make a person feel vulnerable, upset, humiliated, undermined or threatened. Power does not always mean being in a position of authority, but can include both personal strength and the power to coerce through fear or intimidation.

3.2 Bullying can take the form of physical, verbal and non-verbal conduct. Bullying may include, by way of example:

(a) physical or psychological threats;

(b) overbearing and intimidating levels of supervision;

(c) inappropriate derogatory remarks about someone's performance;

3.3 Legitimate, reasonable and constructive criticism of a worker's performance or behaviour, or reasonable instructions given to workers in the course of their employment, will not amount to bullying on their own.

4. YOUR RESPONSIBILITIES

4.1 All employee have a responsibility to help create and maintain a working environment that respects the dignity of employees. You should be aware of the serious and genuine problems, which harassment and bullying can cause, ensure that your behaviour is beyond question and could not be considered in any way to be harassment or bullying. You should discourage such behaviour by making it clear that you find it unacceptable and by supporting colleagues if they are experiencing harassment or bullying and are considering making a complaint. You should alert HR to any incidents to enable them to deal with the matter.

4.2 HR has a responsibility to ensure that harassment or bullying does not occur in work areas for which they are responsible. HR also has a responsibility to explain the CWC's policy to their employee and take steps to promote it positively. They will be responsive and supportive to any employee who makes a complaint, provide full and clear advice on the procedure to be adopted, maintain confidentiality in all cases and ensure that there is no further problem or any victimisation after a complaint has been resolved.

5. IF YOU ARE BEING HARASSED OR BULLIED: INFORMAL STEPS

5.1 If you are being harassed or bullied, consider whether you feel able to raise the problem informally with the person responsible. You should explain clearly to them that their behaviour is not welcome or makes you uncomfortable. If this is too difficult or embarrassing, you should speak to HR, who can provide confidential advice and assistance in resolving the issue formally or informally.

5.2 If informal steps are not appropriate, or have been unsuccessful, you should refer to our Grievance Procedure.

6. PROTECTION AND SUPPORT FOR THOSE INVOLVED

Employee who make complaints or who participate in good faith in any investigation must not suffer any form of retaliation or victimisation as a result. Anyone found to have retaliated against or victimised someone in this way will be subject to disciplinary action under our Disciplinary and Capability Procedure.

7. CONFIDENTIALITY AND RECORD-KEEPING

7.1 Confidentiality is an important part of the procedures provided under this policy. Details of the investigation and the names of the person making the complaint and the person accused must only be disclosed on a "need to know" basis. Breach of confidentiality may give rise to disciplinary action under our Disciplinary and Capability Procedure.

7.2 Information about a complaint by or about an employee may be placed on the employee's personnel file, along with a record of the outcome and of any notes or other documents compiled during the process. These will be processed in accordance with our Data Protection Policy.

SCHEDULE 3 – ANTI-SLAVERY AND HUMAN TRAFFICKING POLICY

1. POLICY STATEMENT

1.1 Modern slavery is a crime and a violation of fundamental human rights. It takes various forms, such as slavery, servitude, forced and compulsory labour and human trafficking, all of which have in common the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain. We have a zero-tolerance approach to modern slavery and we are committed to acting ethically and with integrity in all our business dealings and relationships and to implementing and enforcing effective systems and controls to ensure modern slavery is not taking place anywhere in our own business or in any of our supply chains.

1.2 We are also committed to ensuring there is transparency in our own business and in our approach to tackling modern slavery throughout our supply chains, consistent with our disclosure obligations under the Modern Slavery Act 2015. We expect the same high standards from all of our contractors, suppliers and other business partners, and as part of our contracting processes, we endeavour to include specific prohibitions against the use of forced, compulsory or trafficked labour, or anyone held in slavery or servitude, whether adults or children, and we expect that our suppliers will hold their own suppliers to the same high standards.

1.3 This policy applies to all employees at all levels, including Managing Partners, officers, volunteers and interns.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. COMPLIANCE WITH THE POLICY

2.1 You must ensure that you read, understand and comply with this policy.

2.2 The prevention, detection and reporting of modern slavery in any part of our business or supply chains is the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

2.3 You must notify HR as soon as possible if you believe or suspect that a conflict with this policy has occurred, or may occur in the future.

2.4 You are encouraged to raise concerns about any issue or suspicion of modern slavery in any parts of our business or supply chains of any supplier tier at the earliest possible stage.

2.5 If you believe or suspect a breach of this policy has occurred or that it may occur you must report it in accordance with our Whistleblowing Policy as soon as possible. You should note that where appropriate, and with the welfare and safety of local workers as a priority, we may give support and guidance to our suppliers to help them address coercive or exploitative work practices in their own business and supply chains.

2.6 If you are unsure about whether a particular act, the treatment of workers more generally, or their working conditions within any tier of our supply chains constitutes any of the various forms of modern slavery, raise it with HR.

2.7 We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. We are committed to ensuring no one suffers any detrimental treatment as a result of reporting in good faith their suspicion that modern slavery of

whatever form is or may be taking place in any part of our own business or in any of our supply chains. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the HR immediately. If the matter is not remedied, you should raise it formally using our Grievance Procedure.

3. COMMUNICATION AND AWARENESS OF THIS POLICY

3.1 We are a specialist consultancy firm operating in the financial industry and regulatory market. We provide exceptional solutions, services and talent, engaging with experienced consultants and with the support of a general back office.

3.2 Training on this policy, and on the risk our business faces from modern slavery in its supply chains, forms part of the induction process for all individuals who work for us, with training provided as necessary. We would refer to the information provided by the Home Office[2], including:

- Modern slavery training: resource page - links to training materials to help inform about modern slavery so that we are all better able to spot the signs of modern slavery if a potential case is encountered.
- Modern slavery awareness booklet - aimed at informing about some of the key facts of modern slavery.
- a typology of modern slavery offences in the UK, which identifies seventeen types of modern slavery offences in the UK and includes case studies where offenders have been convicted for modern slavery offences in the UK.
- a toolkit to 'spot the signs' indicators and details of bespoke approaches and tactics to tackle the different types of modern slavery.

3.3 Our commitment to addressing the issue of modern slavery in our business and supply chains must be communicated to all suppliers, contractors and business partners as appropriate.

3.4 Due diligence processes include assessing actual and potential human rights impacts, integration and acting upon the findings, tracking responses, and communicating how impacts are addressed.

3.5 Risk assessments are used to identify what might be a country risk, sector risk, transaction risk, or business partnership risk, as well as the level of risk and its importance to ensure that appropriate remedies are in place.

4. BREACHES OF THIS POLICY

4.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

4.2 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

[2] https://www.gov.uk/government/publications/modern-slavery-training-resource-page/modern-slavery-training-resource-page

SCHEDULE 4 – CLIENT EXPENSES POLICY

1. ABOUT THIS POLICY

1.1 This policy deals with claims for reimbursement of expenses, whether on behalf of CWC or to be reimbursed from a Client.

1.2 This policy applies to all employees.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. OVERVIEW AND OBJECTIVES

2.1 It is CWC's responsibility to ensure that costs are controlled and expenses are only permitted when the relevant client's Statement of Work (SOW) allows for such expenditure, or in the rare situation that a claim is permitted on behalf of CWC.

2.2 These guidelines facilitate the control of company funds and create a clear and transparent reimbursement process, indicating the evidence and authorisation required to be provided by an employee when submitting a claim for expenses, whether incurred during an engagement with a client, which are rechargeable to the client or incurred on behalf of CWC.

2.3 Under the UK general tax law, some expense payments rank as taxable remuneration and CWC may be required to complete annual P11D returns. This expense claim process has been designed to satisfy HMRC requirements.

2.4 The overarching rules (Overarching Rules) for claiming client expenses are that they:

2.4.1 must have been budgeted for in the SOW;

2.4.2 must comply with the client's expense policy;

2.4.3 must be specifically authorised with the prior-written approval directly from the client; and

2.4.4 must be claimed under clause 4.1 below within 2 months of the end of the expense.

If there is a situation where the ability to claim client expenses is unclear then clarity can be provided by a Finance.

2.5 If the expense has arisen as a result of a client's ad hoc request, the expense must still satisfy the Overarching Rules in 2.4 above.

2.6 Adhering to this policy will result in timely recharges to clients and reimbursements to employees, the prevention of fraud and compliance with company tax and legal obligations.

2.7 If the expense claim is on behalf of CWC and does not relate to a client, then the following rules must apply:

2.7.1 must be reasonable in relation to the activity and circumstances;

2.7.2 must be supported by prior-written approval from Finance; and

2.7.3 must be claimed under clause 4.1 below within two months of the date of the expense

2.8 In all situations, if a service that you are claiming reimbursement of is VATable, (i.e. meals) then a full VAT receipt must be provided within the supporting documents when making a claim.

3. EVIDENCE AND APPROVAL

3.1 Familiarise yourself with the client's expense policy and be aware of any specific requirements and limitations. In the absence of a client's expense policy stating spend limits for mileage or meals then the HMRC standard limits will apply. In order to reclaim any expense which is to be recharged to the client, the following process must be followed:

3.2 Prior to committing to any expenditure, check with Finance that the type of expense being sought is allowed under the client's SOW, together with all requirements and limitations.

3.3 Obtain the prior-written approval of the intended expense from the appropriate person (Approver) within the client's organisation, unless the SOW provides for an overarching expenses recharge (e.g. accommodation and meals whilst at client site due to its remote location). The Approver cannot be another CWC employee or representative and their identity will be confirmed on case-by-case basis.

3.4 CWC will reimburse all expenses permitted under the client SOW, approved by the Approver and in line with the client's expenses policy and will recharge the expense to the client. Failure to comply with the client's expense policy will result in CWC not being able to recharge the expense back to the client, therefore an employee's expense claim will be declined.

4. MAKING A CLAIM

4.1 Expenses should be claimed within two months of the date of the expense, after this time a claim will only be paid at a discretion of Finance. A claim form should include all of your claimable expenses for that month.

4.2 A valid client expense claim (Claim) must include the following:

4.2.1 A fully completed 'Employee Expense and Mileage Claim Form';

4.2.2 Evidence of the client's prior-written approval;

4.2.3 The original expense receipts or invoices. Receipts must be itemised on the form referred to in 4.2.1, showing the total charge, full description of the goods or services supplied, full VAT details including registration number and amounts (if applicable), name and address of supplier and the date of supply. Credit card receipts on their own will not be accepted; and

4.2.4 additional commentary, where appropriate

4.2.5 Please note that if a service that you are claiming reimbursement of is VATable, (i.e. meals) then a full VAT receipt may not automatically be provided to you from the supplier so may need to be requested at the point of purchase. **A VATable service will not be reimbursed without full VAT information and VAT receipt.**

4.3 The completed Claim must be submitted electronically to Finance via invoices@cwc.co.uk. You may be requested to provide original receipts from time-to-time as part of our fraud spot-checks, so you must retain copies of your claim.

5. REIMBURSEMENTS

5.1 We will reimburse expenses properly incurred in accordance with this policy. Any attempt to claim expenses fraudulently or in breach of this policy may result in disciplinary action.

5.2 Expenses will be paid in accordance with the regulations and interpretation of HM Revenue & Customs or suspended if necessary at its instruction.

5.3 Any special ad hoc arrangements made to suit particular circumstances will not be considered as setting any form of precedent.

5.4 If your Claim is approved then the funds will be reimbursed directly into the bank account which is used for payroll within 10 working days.

5.5 If your claim is declined or the amount to be reimbursed is less than the total of the claim then a Finance will contact you to discuss the reasons for this and request further information as required.

6. EXPENSE CATEGORIES

Specific guidance per expense category will not be provided by CWC when it comes to claiming client expenses, instead please adhere to the expense policy of the individual client. The Overarching Rules will apply at all times.

SCHEDULE 5 – GRIEVANCE PROCEDURE POLICY

1. ABOUT THIS PROCEDURE

1.1 It is our policy to ensure that all employees have access to a procedure to help deal with any grievances relating to their employment fairly and without unreasonable delay. We aim to investigate any formal grievance you raise, hold a meeting to discuss it with you, inform you in writing of the outcome, and give you a right of appeal if you are not satisfied.

1.2 This procedure applies to all employee regardless of length of service.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. RAISING GRIEVANCES INFORMALLY

Most grievances can be resolved quickly and informally through discussion with HR. If you feel unable to speak to your HR, for example, because the complaint concerns him or her, then you should speak informally to Managing Partner. If this does not resolve the issue, you should follow the formal procedure below.

3. FORMAL WRITTEN GRIEVANCES

3.1 If your grievance cannot be resolved informally you should put it in writing and submit it to HR, indicating that it is a formal grievance. If the grievance concerns HR, you may submit it to the Managing Partners instead.

3.2 The written grievance should contain a brief description of the nature of your complaint, including any relevant facts, dates, and names of individuals involved. In some situations, we may ask you to provide further information.

4. INVESTIGATIONS

4.1 It may be necessary for us to carry out an investigation into your grievance. The amount of any investigation required will depend on the nature of the allegations and will vary from case to case. It may involve interviewing and taking statements from you and any witnesses, and/or reviewing relevant documents. The investigation may be carried out by HR or someone else appointed by us.

4.2 You must co-operate fully and promptly in any investigation. This may include informing us of the names of any relevant witnesses, disclosing any relevant documents to us and attending interviews, as part of our investigation.

4.3 We may initiate an investigation before holding a grievance meeting where we consider this appropriate. In other cases, we may hold a grievance meeting before deciding what investigation (if any) to carry out. In those cases, we will hold a further grievance meeting with you after our investigation and before we reach a decision.

5. RIGHT TO BE ACCOMPANIED

5.1 You may bring a companion to any grievance meeting or appeal meeting under this procedure. You must tell the HR department who your chosen companion is, in good time before the meeting.

5.2 At the meeting, your companion may make representations to us and ask questions, but should not answer questions on your behalf. You may talk privately with them at any time during the meeting.

5.3 Acting as a companion is voluntary and your colleagues are under no obligation to do so. If they agree to do so they will be allowed reasonable time off from duties without loss of pay to act as a companion.

5.4 If your chosen companion is unavailable at the time a meeting is scheduled and will not be available for more than five working days afterwards, we may ask you to choose someone else.

5.5 We may, at our discretion, allow you to bring a companion who is not a colleague (for example, a member of your family) if this will help overcome a disability, or if you have difficulty understanding English.

6. GRIEVANCE MEETINGS

6.1 We will arrange a grievance meeting, normally within one week of receiving your written grievance.

6.2 You and your companion (if any) should make every effort to attend grievance meetings. If you or your companion cannot attend at the time specified, you should inform us immediately and we will try, within reason, to agree an alternative time.

6.3 The purpose of a grievance meeting is to enable you to explain your grievance and how you think it should be resolved, and to assist us to reach a decision based on the available evidence and the representations you have made.

6.4 After an initial grievance meeting, we may carry out further investigations and hold further grievance meetings as we consider appropriate. Such meetings will be arranged without unreasonable delay.

6.5 We will write to you, usually within one week of the final grievance meeting, to inform you of the outcome of your grievance and any further action that we intend to take to resolve the grievance. We will also remind you of your right of appeal. Where appropriate we may hold a meeting to give you this information in person.

7. APPEALS

7.1 If the grievance has not been resolved to your satisfaction you may appeal in writing to the HR department, stating your full grounds of appeal, within one week of the date on which the decision was sent or given to you.

7.2 We will hold an appeal meeting, normally within one week of receiving your written appeal. This will be dealt with impartially by someone who has not previously been involved in the case (although they may ask anyone previously involved to be present). You have a right to bring a companion to the meeting (see Paragraph 6).

7.3 We will confirm our final decision in writing, usually within one week of the appeal hearing. This is the end of the procedure and there is no further appeal.

SCHEDULE 6 – SOCIAL MEDIA POLICY

1. ABOUT THIS POLICY

1.1 This policy is in place to minimise the risks to our business through use of social media.

1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, TikTok, Twitter, Wikipedia, Whisper, Instagram, Tumblr and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

1.3 This policy covers all employee.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

2.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum.

2.2 Employee should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

2.3 Employee who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

3. PERSONAL USE OF SOCIAL MEDIA

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

4. PROHIBITED USE

4.1 You must avoid making any social media communications that could damage our business interests or reputation, even indirectly. You must not post entries on a blog or social networking site which are derogatory, defamatory, discriminatory or offensive in any way, or which could bring CWC, its employees, its clients, or partners into disrepute or is likely to have a negative impact on the reputation of any of these parties. You should be aware that blogs and social networking posts may create documents which the courts can order to be disclosed for use in litigation. Consequently, you will be assumed to have written any contentious items unless you can prove definitively that you have not done so.

4.2 You must not use social media to defame or disparage us, our employee or any third party; to harass, bully or unlawfully discriminate against employee or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

4.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by HR. You may be required to undergo training in order to obtain such authorisation.

4.4 You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

4.5 You must not post on social media and/or update your blogs with any information or opinion related to your employment, or information or opinion obtained as a result of your employment. This includes information relating to CWC, its employees, its clients or its partners. This includes information that has been 'anonymised'.

4.6 You are not permitted to add business contacts made during the course of your employment to personal social networking accounts, unless otherwise agreed with senior management.

4.7 Any misuse of social media should be reported to the senior management.

5. GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

5.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.

5.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

5.3 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf as set out in Paragraph 5.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

5.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with HR.

5.5 If you see social media content that disparages or reflects poorly on us, you should contact HR.

6. MONITORING

6.1 We reserve the right to monitor, intercept and review, without further notice, employee activities using our IT resources and communications systems, including but not limited to social media postings and activities, for legitimate business purposes which include ascertaining and demonstrating that expected standards are being met by those using the systems and for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

6.2 For further information, please refer to our IT and Communications Systems Policy.

7. RAISING A CONCERN

7.1 You should raise any concerns regarding our social media channels or related posts with HR, either in person or put the matter in writing if you prefer.

7.2 We will carry out an initial assessment and decide the appropriate action and whether a formal report and/or further training or guidance is required.

8. RECRUITMENT

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

9. BREACH OF THIS POLICY

9.1 Breach of this policy may result in disciplinary action up to and including dismissal. Any employee suspected of committing a breach of this policy will be required to co-operate with our investigation.

9.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

PEOPLE POLICIES – TIME OFF & SICKNESS

SCHEDULE 7 – ANNUAL LEAVE POLICY

1. ABOUT THIS POLICY

1.1 This policy sets out our arrangements for employee wishing to take annual leave.

1.2 This policy covers all employee.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time. We may also vary the policy as appropriate in any case.

2. YOUR ANNUAL LEAVE ENTITLEMENT

2.1 The company's annual leave year runs from 1 January to 31 December. If your employment starts or finishes part way through the year, your entitlement during that year shall be calculated on a pro-rata basis rounded up to the nearest half day.

2.2 Unless otherwise set out in your employment contract, you are entitled to 28 days paid annual leave in each year, or the pro rata equivalent if you work part time. This includes the usual eight public holidays in England and Wales or days in lieu where we require employees to work on a public holiday.

2.3 Payment for annual leave will be at your normal rate of pay.

2.4 Except as set out in this policy, annual leave entitlement must be taken during the year in which it accrues. Any annual leave not taken by the end of the year will be lost and you will not receive any payment in lieu.

2.5 Unused annual leave can only be carried over into another year:

(a) in cases of absence, including long-term sickness, maternity, paternity, adoption, parental or shared parental leave; and

(b) if otherwise required by law.

2.6 The content of these clauses does not affect your statutory entitlement under the Working Time Regulations (as amended).

3. TAKING ANNUAL LEAVE

3.1 All annual leave requests must be booked and approved in advance, with as much notice being given as possible. You must not make travel bookings until approval has been given and you must follow the annual leave booking process as set out in our Annual Leave Booking – Timesheet Portal Guide, which you will find on the Consultant Portal. Further guidance on the process may be issued from time to time.

3.2 We may require you to take (or not to take) annual leave on particular dates, including when the business is closed, particularly busy, when clients request it (such as during furlough periods during the 'festive break) or during your notice period.

3.3 If you decide not to take the time off that you have booked, we are not obliged to agree, so you should seek our prior approval if you do not intend to take your annual leave as planned. Failure to obtain our approval could result in you having to take the dates as annual leave anyway.

3.4 You should not seek to avoid taking time off as annual leave by 'making up' the time outside office hours or at the weekend, unless with the prior written approval of both us and our client. Any agreement to 'make up' time is not standard procedure and should not be seen as setting a precedent. This does not apply to short absences of under an hour, which can be easily adjusted into your working day.

4. UNPAID OR UNPLANNED ANNUAL LEAVE

4.1 We recognise there may be occasions when you require unpaid leave, or unavoidable unplanned leave and we would seek to accommodate all requests where appropriate.

4.2 You should follow the same procedure as for paid leave, but we would ask that you discuss the matter with HR first, before approaching our client.

5. LONG-TERM SICKNESS ABSENCE AND ANNUAL LEAVE ENTITLEMENT

5.1 Annual leave entitlement continues to accrue during periods of sick leave.

5.2 If you are on a period of sick leave which spans two annual leave years, or if you return to work after sick leave so close to the end of the year that you cannot reasonably take your remaining annual leave, you may carry over unused annual leave to the following year.

5.3 Carry-over under this rule is limited to the 28 days (or pro-rata equivalent) minimum annual leave entitlement under EU law (which includes bank holidays), less any leave taken during the year that has just ended. If you have taken 28 days (or pro-rata equivalent) annual leave by the end of the year, you will not be allowed to carry anything over under this rule. If you have taken less than 28 days (or pro-rata equivalent), the remainder may be carried over under this rule.

5.4 Any annual leave that is carried over under this rule but is not taken within six months of the next annual leave year will be lost.

5.5 Alternatively you can choose to take your accrued annual leave during your sick leave, in which case it will be paid at your normal rate.

6. FAMILY LEAVE AND ANNUAL LEAVE ENTITLEMENT

Annual leave entitlement continues to accrue during periods of maternity, paternity, adoption, parental or shared parental leave (referred to collectively in this policy as family leave) and you should refer to the relevant policy.

7. ARRANGEMENTS ON TERMINATION

7.1 On termination of employment you may be required to use any remaining annual leave entitlement during your notice period. Alternatively, HR can exercise their discretion for you to be paid in lieu of any accrued but untaken annual leave entitlement, plus any annual leave that was permitted to be carried over from previous years under this policy or as required by law.

7.2 If you have taken more annual leave than you have accrued during the year then the balance will be deducted from any outstanding pay.

7.3 Where termination of your employment is due to gross misconduct or where the full contractual notice period is not served and worked, unused annual leave will not be paid, apart from any payment required to meet the statutory minimum annual leave obligations.

7.4 During your notice period, we reserve the right to decide on the dates of which some or all of your outstanding annual leave entitlement may be taken.

SCHEDULE 8 – SICKNESS ABSENCE POLICY

1. ABOUT THIS POLICY

1.1 This Sickness Absence Policy sets out our procedures for reporting sickness absence and for the management of sickness absence in a fair and consistent way.

1.2 Sickness absence can vary from short intermittent periods of ill-health to a continuous period of long-term absence and have a number of different causes (for example, injuries, recurring conditions, or a serious illness requiring lengthy treatment).

1.3 We wish to ensure that the reasons for sickness absence are understood in each case and investigated where necessary. In addition, where needed and reasonably practicable, measures will be taken to assist those who have been absent by reason of sickness to return to work.

1.4 This policy applies to all employee.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

1.6 Any information you provide to us about your health will be processed in accordance with our Data Protection Policy. We recognise that such data is sensitive and will handle it in a confidential manner.

2. DISABILITIES

2.1 We are aware that sickness absence may result from a disability. At each stage of the sickness absence meetings procedure (set out in Paragraph 12 of this policy), particular consideration will be given to whether there are reasonable adjustments that could be made to the requirements of a job or other aspects of working arrangements that will provide support at work and/or assist a return to work.

2.2 If you consider that you are affected by a disability or any medical condition which affects your ability to undertake your work, you should inform the HR department. Any information you provide will be handled in a confidential manner and proceeded in accordance with our Data Protection Policy.

3. SICKNESS ABSENCE REPORTING PROCEDURE

3.1 If you are taken ill or injured while at work you should contact HR to be given permission to leave work, or to receive medical treatment where necessary.

3.2 If you cannot attend work because you are ill or injured you should telephone HR as early as possible and no later than 30 minutes after the time when you are normally expected to start work.

3.3 As part of the reporting procedure you must also complete and submit our Absence Form. Further guidance on the process may be issued from time to time.

3.4 You should expect to be contacted during your absence by the office who will want to enquire after your health and be advised, if possible, as to your expected return date and any urgent work matters to be handled in your absence.

4. EVIDENCE OF INCAPACITY

4.1 For sickness absence of up to seven calendar days you must complete a self-certification form which is available from the HR department.

4.2 For absence of more than a week you must obtain a certificate from your doctor (a "Statement of Fitness for Work") stating that you are not fit for work and the reason(s) why. If your absence continues, further medical certificates must be provided to cover the whole period of absence.

4.3 If your doctor provides a certificate stating that you "may be fit for work" you should inform the HR department immediately. We will discuss with you any additional measures that may be needed to facilitate your return to work, taking account of your doctor's advice. If appropriate measures cannot be taken, you will remain on sick leave and we will set a date to review the situation.

6. SICK PAY

6.1 You may be entitled to Statutory Sick Pay (SSP) if you satisfy the relevant statutory requirements. Qualifying days for SSP are Monday to Friday, or as set out in your employment contract. The rate of SSP is set by the government in April each year. No SSP is payable for the first three consecutive days of absence. It starts on the fourth day of absence and may be payable for up to 28 weeks.

6.2 If a period of sickness absence is or appears to be occasioned by actionable negligence, nuisance or breach of any statutory duty on the part of a third party, in respect of which damages are or may be recoverable, you must immediately notify HR of that fact and of any claim, compromise, settlement or judgment made or awarded in connection with it and all relevant particulars that we may reasonably require. If we require you to do so, you must co-operate in any related legal proceedings and refund to us that part of any damages or compensation you recover that relates to lost earnings for the period of sickness absence as we may reasonably determine, less any costs you incurred in connection with the recovery of such damages or compensation, provided that the amount to be refunded to us shall not exceed the total amount we paid to you in respect of the period of sickness absence.

6.3 You will retain the use of any benefits in kind such as company car or mobile telephone for the first 13 weeks after which they shall be at our discretion.

6.4 Any employer and employee pension contributions will continue subject to the relevant scheme rules during any period of company sick pay or SSP.

6.5 You should forward relevant documents and any correspondence to the HR department as soon as possible. Failure to do so may result in sick pay being delayed or withheld and action under the Disciplinary and Capability Procedure being taken.

8. KEEPING IN CONTACT DURING SICKNESS ABSENCE

If you are absent on sick leave you should expect to be contacted from time to time by HR in order to discuss your wellbeing, expected length of continued absence from work and any of your work that requires attention. Such contact is intended to provide reassurance and will be kept to a reasonable minimum.

9. MEDICAL EXAMINATIONS

9.1 We may, at any time in operating this policy, require you to consent to a medical examination by a doctor nominated by us (at our expense).

9.2 You will be asked to agree that any report produced in connection with any such examination may be disclosed to us and that we may discuss the contents of the report with our advisers and the relevant doctor.

10. RETURN-TO-WORK INTERVIEWS

After a period of sick leave we may arrange for you to have a return-to-work interview, which enables us to confirm the details of your absence. It also gives you the opportunity to raise any concerns or questions you may have, and to bring any relevant matters to our attention, such as your doctor's advice.

11. MANAGING LONG-TERM OR PERSISTENT ABSENCE

11.1 The following paragraphs set out our procedure for dealing with long-term absence or where your level or frequency of short-term absence has given us cause for concern. The purpose of the procedure is to investigate and discuss the reasons for your absence, whether it is likely to continue or recur, and whether there are any measures that could improve your health and/or attendance. We may decide that medical evidence, or further medical evidence, is required before deciding on a course of action.

11.2 We will notify you in writing of the time, date and place of any meeting, and why it is being held. We will usually give you a week's notice of the meeting.

11.3 Meetings will be conducted at a mutually convenient time by HR and you may bring a companion to any meeting or appeal meeting under this procedure. If you have a disability, we will consider whether reasonable adjustments may need to be made to the sickness absence meetings procedure, or to your role or working arrangements.

12. INITIAL SICKNESS ABSENCE MEETING

12.1 The purposes of a sickness absence meeting or meetings will be to discuss the reasons for your absence, how long it is likely to continue, whether it is likely to recur, whether to obtain a medical report, and whether there are any measures that could improve your health and/or attendance.

12.2 In cases of long-term absence, we may seek to agree a return-to-work programme, possibly on a phased basis.

12.3 In cases of short-term, intermittent absence, we may set a target for improved attendance within a certain timescale.

13. IF MATTERS DO NOT IMPROVE

If, after a reasonable time, you have not been able to return to work or if your attendance has not improved within the agreed timescale, we will hold a further meeting or meetings. We will seek to establish whether the situation is likely to change, and may consider redeployment opportunities at that stage. If it is considered unlikely that you will return to work or that your attendance will improve within a short time, we may give you a written warning that you are at risk of dismissal. We may also set a further date for review.

14. FINAL SICKNESS ABSENCE MEETING

Where you have been warned that you are at risk of dismissal, and the situation has not changed significantly, we will hold a meeting to consider the possible termination of your employment. Before we make a decision, we will consider any matters you wish to raise and whether there have been any changes since the last meeting.

15. APPEALS

15.1 You may appeal against the outcome of any stage of this procedure. If you wish to appeal you should set out your appeal in writing to [POSITION], stating your grounds of appeal, within [one week] of the date on which the decision was sent or given to you.

15.2 If you are appealing against a decision to dismiss you, we will hold an appeal meeting, normally within two weeks of receiving the appeal. This will be dealt with impartially and, where possible, by a Managing Partner who has not previously been involved in the case.

15.3 We will confirm our final decision in writing, usually within one week of the appeal hearing. There is no further right of appeal.

15.4 The date that any dismissal takes effect will not be delayed pending the outcome of an appeal. However, if the appeal is successful, the decision to dismiss will be revoked with no loss of continuity or pay.

PEOPLE POLICIES – PERFORMANCE & DISCIPLINARY

SCHEDULE 9 – DISCIPLINARY AND CAPABILITY PROCEDURE

1. ABOUT THIS PROCEDURE

1.1 This procedure is intended to help maintain standards of conduct and performance and to ensure fairness and consistency when dealing with allegations of misconduct or poor performance.

1.2 Minor conduct or performance issues can usually be resolved informally with HR. This procedure sets out formal steps to be taken if the matter is more serious or cannot be resolved informally.

1.3 This procedure applies to all employees regardless of length of service.

1.4 This procedure does not form part of any employee's contract of employment and we may amend it at any time.

2. INVESTIGATIONS

2.1 Before any disciplinary hearing is held, the matter will be investigated. Any meetings and discussions as part of an investigation are solely for the purpose of fact-finding and no disciplinary action will be taken without a disciplinary hearing.

2.2 In some cases of alleged misconduct, we may need to suspend you from work while we carry out the investigation or disciplinary procedure (or both). While suspended, you should not visit our premises or contact any of our clients, customers, suppliers, contractors or employee, unless authorised to do so. Suspension is not considered to be disciplinary action.

3. THE HEARING

3.1 We will give you written notice of the hearing, including sufficient information about the alleged misconduct or poor performance and its possible consequences to enable you to prepare. You will normally be given copies of relevant documents and witness statements.

3.2 You may be accompanied at the hearing by a trade union representative or a colleague.

3.3 You should let us know as early as possible if there are any relevant witnesses you would like to attend the hearing or any documents or other evidence you wish to be considered.

3.4 We will inform you in writing of our decision, usually within one week of the hearing.

4. DISCIPLINARY ACTION AND DISMISSAL

The usual penalties for misconduct or poor performance are:

(a) Stage 1: First written warning [or improvement note]. Where there are no other active written warnings or improvement notes on your disciplinary record, you will usually receive a first written warning or improvement note. It will usually remain active for six months.

(b) Stage 2: Final written warning. In case of further misconduct or failure to improve where there is an active first written warning or improvement note on your record, you will usually receive a final written warning. This may also be used without a first written warning [or improvement note] for serious cases of misconduct or poor performance. The warning will usually remain active for 12 months.

(c) Stage 3: Dismissal or other action. You may be dismissed for further misconduct or failure to improve where there is an active final written warning on your record, or for any act of gross misconduct. Examples of gross misconduct are given below (paragraph 6). You may also be dismissed without a warning for any act of misconduct or unsatisfactory performance during your probationary period.

We may consider other sanctions short of dismissal, including demotion or redeployment to another role (where permitted by your contract), and/or extension of a final written warning with a further review period.

5. APPEALS

5.1 You may appeal in writing within one week of being told of the decision.

5.2 The appeal hearing will, where possible, be held by someone other than the person who held the original hearing. You may bring a colleague or trade union representative with you to the appeal hearing.

5.3 We will inform you in writing of our final decision as soon as possible, usually within one week of the appeal hearing. There is no further right of appeal.

6. GROSS MISCOUNDUCT

6.1 Gross misconduct will usually result in dismissal without warning, with no notice or payment in lieu of notice (summary dismissal).

6.2 Please refer to our Disciplinary Rules Policy for further details.

SCHEDULE 10 – DISCIPLINARY RULES POLICY

1. POLICY STATEMENT

1.1 These Disciplinary Rules should be read in conjunction with our Disciplinary and Capability Procedure. The aim of the Disciplinary Rules and Disciplinary and Capability Procedure is to set out the standards of conduct expected of all employee and to provide a framework within which HR can work with employee to maintain those standards and encourage improvement where necessary.

1.2 It is our policy to ensure that any disciplinary matter is dealt with fairly and in accordance with the Disciplinary and Capability Procedure.

1.3 If you are in any doubt as to your responsibilities or the standards of conduct expected you should speak to the HR department.

1.4 This policy covers all employee.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. RULES OF CONDUCT

2.1 While working for us you should at all times maintain professional and responsible standards of conduct. In particular you should:

(a) observe the terms and conditions of your contract;

(b) ensure that you understand and follow out Code of Conduct which is set out in this handbook;

(c) observe all our policies, procedures and regulations which are included in this handbook or notified to you from time to time by means of notice boards, email, the intranet or otherwise;

(d) take reasonable care in respect of the health and safety of colleagues and third parties and comply with our Health and Safety Policy;

(e) comply with all reasonable instructions given by HR; and

(f) act at all times in good faith and in our best interests and those of our customers and employee.

2.2 Failure to maintain satisfactory standards of conduct may result in action being taken under our Disciplinary and Capability Procedure.

3. MISCONDUCT

The following are examples of matters that will normally be regarded as misconduct and will be dealt with under our Disciplinary and Capability Procedure:

(a) Minor breaches of our policies including the Sickness Absence Policy, IT and Communications Systems Policy, and Health and Safety Policy;

(b) Minor breaches of your contract;

(c) Damage to, or unauthorised use of, our property;

(d) Poor timekeeping;

(e) Time wasting;

(f) Unauthorised absence from work;

(g) Refusal to follow instructions;

(h) Excessive use of our telephones for personal calls;

(i) Excessive personal email or internet usage;

(j) Obscene language or other offensive behaviour;

(k) Negligence in the performance of your duties; or

(l) Smoking in no-smoking areas.

This list is intended as a guide and is not exhaustive.

4. GROSS MISCONDUCT

4.1 Gross misconduct is a serious breach of contract and includes misconduct which, in our opinion, is likely to prejudice our business or reputation or irreparably damage the working relationship and trust between us. Gross misconduct will be dealt with under our Disciplinary and Capability Procedure and will normally lead to dismissal without notice or pay in lieu of notice (summary dismissal).

4.2 The following are examples of matters that are normally regarded as gross misconduct:

(a) Fraud, forgery, theft or other dishonesty, including fabrication of expense claims and time sheets;

(b) Actual or threatened violence, bullying or behaviour which provokes violence;

(c) Deliberate damage to our buildings, fittings, property or equipment, or the property of a colleague, contractor, customer or member of the public;

(d) Serious misuse of our property or name;

(e) Deliberately accessing internet sites containing pornographic, offensive or obscene material;

(f) Repeated or serious failure to obey instructions, or any other serious act of insubordination;

(g) Unlawful discrimination or harassment;

(h) Bringing the organisation into serious disrepute;

(i) Being under the influence of alcohol, illegal drugs or other substances during working hours;

(j) Causing loss, damage or injury through serious negligence;

(k) Serious or repeated breach of health and safety rules or serious misuse of safety equipment;

(l) Unauthorised use or disclosure of confidential information or failure to ensure that confidential information in your possession is kept secure;

(m) Breach of our Anti-corruption and bribery policy;

(n) Accepting a gift above the value of £50 from a customer, supplier, contractor or other third party in connection with your employment without prior consent from HR;

(o) Conviction for a criminal offence that in our opinion may affect our reputation or our relationships with our employee, customers or the public, or otherwise affects your suitability to continue to work for us;

(p) Possession, use, supply or attempted supply of illegal drugs;

(q) Serious neglect of duties, or a serious or deliberate breach of your contract or operating procedures;

(r) Knowing breach of statutory rules affecting your work;

(s) Unauthorised use, processing or disclosure of personal data contrary to our Data Protection Policy;

(t) Harassment of, or discrimination against, employees, contractors, clients or members of the public, related to gender, marital or civil partner status, gender reassignment, race, colour, nationality, ethnic or national origin, disability, religion or belief or age contrary to The Equality Act 2010 or our Anti-harassment and Bullying Policy;

(u) Refusal to disclose any of the information required by your employment or any other information that may have a bearing on the performance of your duties;

(v) Giving false information as to qualifications or entitlement to work (including immigration status) in order to gain employment or other benefits;

(w) Knowingly taking parental, paternity or adoption leave when not eligible to do so or for a purpose other than supporting a child;

(x) Making a disclosure of false or misleading information under our Whistleblowing Policy maliciously, for personal gain, or otherwise in bad faith;

(y) Making untrue allegations in bad faith against a colleague;

(z) Victimising a colleague who has raised concerns, made a complaint or given evidence or information under our Whistleblowing Policy, Anti-corruption and bribery policy, Anti-harassment and Bullying Policy, Grievance Procedure, Disciplinary and Capability Procedure or otherwise;

(aa) Serious misuse of our information technology systems (including misuse of developed or licensed software, use of unauthorised software and misuse of email and the internet) contrary to our Information and Communications Systems Policy;

(bb) Undertaking unauthorised paid or unpaid employment during your working hours;

(cc) Unauthorised entry into an area of the premises to which access is prohibited.

This list is intended as a guide and is not exhaustive.

FRAUD & FINANCIAL CRIME

SCHEDULE 11 – ANTI-MONEY LAUNDERING POLICY

1. POLICY STATEMENT

1.1 It is our policy to assist in the fight against crime and terrorist activities, both in the UK and globally. By depriving criminals and terrorists of the funds they need laundered and taking a zero tolerance approach to money-laundering methods.

1.2 We are committed to preventing our clients and employees from being exposed to money-laundering, identifying the risk where it might occur, complying with all legal and regulatory requirements, especially with regard to reporting suspected cases.

1.3 The Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Money Laundering Regulations 2007 place obligations on us to establish internal procedures to prevent the use of our services for money laundering.

1.4 This Anti-Money Laundering Policy sits within our wider counter fraud and corruption policies.

1.5 If you are in any doubt as to your responsibilities or the standards of conduct expected you should speak to HR.

1.6 This policy covers all employees.

1.7 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. ABOUT THIS POLICY

2.1 The purpose of this policy is to:

(a) set out our responsibilities, and of those working for us, in observing and upholding our position on anti-money laundering; and

(b) provide information and guidance to those working for us on how to recognise and deal with anti-money laundering issues.

2.2 There are serious criminal sanctions for breaching the legislation. We therefore take our legal responsibilities very seriously.

2.3 We have identified that the following are particular risks for our business:

- Appointment of a new equity partner
- Engagement with a new client

To address those risks we have taken the following steps:

- To perform due diligence

2.4 In this policy, third party means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors,

business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

3. WHO MUST COMPLY WITH THIS POLICY?

This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels. Anti-Money Laundering matters will be included in employee induction, and subsequent appropriate training will be provided ad hoc.

4. RESPONSIBILITY FOR THIS POLICY

HR has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in countering money laundering.

5. WHAT IS MONEY LAUNDERING?

5.1 The principal primary legislation is the Proceeds of Crime Act 2002, supplemented by the Terrorism Act 2000 and the Fraud Act 2006. The principal secondary legislation is the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

5.2 Money laundering is the process to move illegally acquired cash through financial systems so that it appears to be from a legitimate source. The various stages are termed placement, layering and integration:

- Placement: 'dirty money' is placed directly into the financial system
- Layering: the proceeds are moved through a series of financial transactions, making it harder to establish their origin.
- Integration: the money launderer creates a legitimate explanation for the source of funds allowing them to be retained, invested into the legitimate economy or to acquire assets.

5.3 The following constitute the act of money laundering:

- Concealing, disguising, converting or transferring criminal property removing it from the UK.
- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
- Acquiring, using or possessing criminal property.
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property.
- Tipping-off is where someone informs a person or people who are, or are suspected of, being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation.

6. MONEY LAUNDERING OFFICER (MLO)

The officer nominated to receive disclosure about money laundering activity within CWC is listed on the CWC Consultant Portal.

7. YOUR RESPONSIBILITIES

7.1 If you become concerned about your involvement in a matter that may amount to a prohibited act under the legislation, you must disclose this promptly to the MLO. The disclosure should be at the earliest opportunity of the information coming to your attention (not weeks or months later). Should you not do so, then you may be liable to prosecution.

7.2 You must follow any subsequent directions from the MLO and must not make any further enquiries yourself into the matter. Additionally, you must not take any further steps in the transaction without authorisation from the MLO.

7.3 You must not disclose or otherwise indicate your suspicions to the person(s) suspected of money laundering. The person concerned should be advised that routine procedures require secondary authorisation prior to large cash amounts being processed. You must not disclose matters with others or note on a file that a report has been made to the MLO in case this results in the suspect becoming aware of the suspicion.

8. CONSIDERATION OF THE DISCLOSRE BY THE MLO

8.1 The MLO must promptly evaluate any disclosure to determine whether there 1) is actual or suspected money laundering taking place, or 2) whether they should lodge a suspicious activity report with the National Crime Agency (NCA).

8.2 The MLO must, if they so determine, promptly report the matter to the NCA on the NCA's standard report form and in the prescriber manner and await consent from the NCA for the transaction to proceed (or the expiration of the relevant time limits without objection).

8.3 All disclosure reports referred to the MLO and reports made to the NCA must be retained by the MLO in a confidential file kept for that purpose, for a minimum of five years. This includes the internal Money Laundering Notification Form and any other notification and reports.

8.4 The MLO will commit a criminal offence if they know or suspect, or have reasonable ground to do so, through a disclosure being made to them, that another person is engaged in money and they do not disclose his as soon as practicable to the NCA.

8.5 Following the consideration of a disclosure, the MLO will carry out an analysis to consider how the event came about the what could be improved.

9. CUSTOMER IDENTIFICATION AND DUE DILIGENCE

9.1 Due diligence is performed on all third parties and employees, who must provide basic information including full name, address, date of birth/corporate registration details. Enhanced due diligence may be required if the matter is considered 'high risk' (new/not well known to company, high risk industries/jurisdictions, complex transaction or payment arrangements, involves politically exposed person, no face to face meetings).

9.2 You must assess the money laundering risk for each third party or employee and if you suspect enhanced due diligence is required, or if you need to speak with the MLO. Additional due diligence would include further information on the person/company, to include beneficial ownership, nature of business relationship and information on the source of funds and source of wealth. Also consider checking

personnel on website, attend their address, check public registers and ensure the first payment is made into a bank account in their name.

10. CASH PAYMENTS

10.1 Any cash payments should be treated with professional scepticism.

10.2 If the cash payment is less than £1,000 and there is no reason to suspect or know that money laundering activity is taking place, then it may be accepted with no need to seek guidance from the MLO.

10.3 Any payment over £1,000 should be referred to the MLO prior to accepting the payment.

10.4 When providing guidance, the MLO may require the payer's proof of identity.

11. RECORD-KEEPING

11.1 We must keep records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

11.2 The Money Laundering Officer will keep records of all referrals made to them and of any action taken or not taken.

12. COMMUNICATION

Our zero-tolerance approach money laundering should be communicated to all suppliers, contractors and business partners.

13. BREACHES OF THIS POLICY

13.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

13.2 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

14. FURTHER INFORMATION

14.1 Further information can be obtained from the Money Laundering Officer.

14.2 External information can be obtained from the following sources:

- National Crime Agency (NCA) www.nationcrimeagency.gov.uk
- CIPFA www.cipfa.org

SCHEDULE 12 – FRAUD POLICY

1. POLICY STATEMENT

1.1 CWC conducts its business in an honest, legal and ethical manner, and operates a zero-tolerance attitude to fraud, bribery and corruption.

1.2 We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter tax evasion facilitation.

1.2 We will uphold all laws relevant to fraud in all the jurisdictions in which we operate, including the Fraud Act 2006 & the Criminal Finances Act 2017.

2. ABOUT THIS POLICY

2.1 The purpose of this policy is to:

(a) provide definitions of fraud, and to set out our responsibilities for action and reporting lines in the event of suspected, attempted or actual fraud; and

(b) provide information and guidance to those working for us on how to recognise and avoid fraud.

2.2 CWC has a zero-tolerance approach to fraud, and as such all forms of fraud are prohibited.

2.3 This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels. It applies to all of CWC's activities and operations and to all of its dealings and negotiations with third parties in all countries in which its employees, agents, partners and associates operate.

2.4 CWC will address risks of fraud, bribery and corruption by ensuring adequate and proportionate measures are developed and implemented to mitigate them.

2.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

3. WHO IS RESPONSIBLE FOR THE POLICY?

HR has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in the prevention of fraud.

4. DEFINITION OF FRAUD

4.1 Fraud describes a number of activities including theft, false accounting, embezzlement, bribery and deception. The Fraud Act 2006 defines three class of fraud:

- False representation: a person commits fraud by intentionally and dishonestly making a false representation. A false representation includes intentionally giving a misleading or untrue statement.
- Failing to disclose information: a person commits a fraud if they dishonestly fail to disclose information.
- Abuse of position: a person commits a fraud if they dishonestly abuse their position.

4.2 To have committed a fraud a person must have acted dishonestly, and with the intent to:

- make a gain for themselves or anyone else

and/or

- cause loss to anyone else, or expose anyone else to a risk of loss

5. EMPLOYEE RESPONSIBILITIES

5.1 Employees should ensure that they read, understand and comply with this policy.

5.2 The prevention, detection and reporting of fraud are the responsibility of all those working for us or under our control. Employees are required to avoid any activity that might lead to, or suggest, a breach of this policy.

5.3 You must notify HR as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future. For example, if an employee or supplier asks to be paid into an alternative bank account, without good reason, or a supplier asks to be paid in cash, indicating that this will mean the payment is not subject to VAT.

6. COMMUNICATION

6.1 CWC ensures that its fraud, bribery and corruption prevention, and associated policies and procedures, are embedded and understood throughout the organisation through internal and external communication, including training that is proportionate to the risk it faces.

6.2 CWC will monitor and review their procedures and action plans to ensure their suitability, adequacy and effectiveness in relation to this policy and implement improvements as appropriate.

6.2 Our zero-tolerance approach to fraud should be communicated to all suppliers, contractors and business partners.

7. HOW TO RAISE A CONCERN

7.1 You are encouraged to raise concerns about any issue or suspicion of fraud at the earliest possible stage.

7.2 If you become aware of any fraudulent act by another person in the course of your work, or you are asked to assist another person in their fraudulent act (whether directly or indirectly), or if you believe or suspect that any fraudulent act has occurred or may occur, you must report it in accordance with our Whistleblowing Policy as soon as possible.

7.3 If you are unsure about whether a particular act constitutes a fraudulent act, raise it with HR as soon as possible.

8. PROTECTION

8.1 Individuals who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

8.2 We are committed to ensuring no one suffers any detrimental treatment as a result of:
(a) refusing to take part in, be concerned in, or facilitate fraud by another person;

(b) refusing to aid, abet, counsel or procure the commission of a fraudulent offence by another person; or

(c) reporting in good faith their suspicion that an actual or potential fraudulent offence has taken place, or may take place in the future.

8.3 Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform HR immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure.

9. BREACHES OF THIS POLICY

9.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

9.2 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

10. REFERRAL TO EXTERNAL AGENCIES

HR will decide at what stage a case should be reported to the police or other external agency such as the Serious Fraud Office (SFO). Certain offices carry criminal liability for individuals concerned and sanctions include significant fines and/or imprisonment.

11. POLICY REVIEW

This policy will be reviewed on an annual basis.

12. LINKS TO OTHER POLICIES

This policy links with, and is to be read in conjunction with, the following:

- Anti-Corruption and Bribery Policy
- Anti-Facilitation of Tax Evasion Policy
- Whistleblowing Policy

SCHEDULE 13 – ANTI-CORRUPTION AND BRIBERY POLICY

1. POLICY STATEMENT

1.1 It is our policy to conduct all of our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter bribery and corruption.

1.2 We will uphold all laws relevant to countering bribery and corruption in all the jurisdictions in which we operate. However, we remain bound by UK laws, including the Bribery Act 2010, in respect of our conduct both at home and abroad.

2. ABOUT THIS POLICY

2.1 The purpose of this policy is to:

(a) set out our responsibilities, and of those working for us, in observing and upholding our position on bribery and corruption; and

(b) provide information and guidance to those working for us on how to recognise and deal with bribery and corruption issues.

2.2 It is a criminal offence to offer, promise, give, request, or accept a bribe. Individuals found guilty can be punished by up to ten years' imprisonment and/or a fine. As an employer if we fail to prevent bribery we can face an unlimited fine, exclusion from tendering for public contracts, and damage to our reputation. We therefore take our legal responsibilities very seriously.

2.3 We have identified that the following are particular risks for our business:

To address those risks we have taken the following steps:

2.4 In this policy, third party means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

2.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2.6 Clients may require specific training and accreditation in this area as a condition of engagement: the policies herein do NOT constitute compliance with such Client requirements, and, in such instances, specific guidance should be sought from HR or from your client where appropriate.

3. WHO MUST COMPLY WITH THIS POLICY?

This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels.

4. RESPONSIBILITY FOR THIS POLICY

HR has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in countering bribery and corruption.

5. WHAT ARE BRIBERY AND CORRUPTION?

5.1 Bribery is offering, promising, giving or accepting any financial or other advantage, to induce the recipient or any other person to act improperly in the performance of their functions, or to reward them for acting improperly, or where the recipient would act improperly by accepting the advantage.

5.2 An advantage includes money, gifts, loans, fees, hospitality, services, discounts, the award of a contract or anything else of value.

5.3 A person acts improperly where they act illegally, unethically, or contrary to an expectation of good faith or impartiality, or where they abuse a position of trust. The improper acts may be in relation to any business or professional activities, public functions, acts in the course of employment, or other activities by or on behalf of any organisation of any kind.

5.4 Corruption is the abuse of entrusted power or position for private gain.

Examples:

Offering a bribe: You offer a potential client tickets to a major sporting event, but only if they agree to do business with us.

This would be an offence as you are making the offer to gain a commercial and contractual advantage. We may also be found to have committed an offence because the offer has been made to obtain business for us. It may also be an offence for the potential client to accept your offer.

Receiving a bribe: A supplier gives your nephew a job, but makes it clear that in return they expect you to use your influence in our organisation to ensure we continue to do business with them.

It is an offence for a supplier to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

Bribing a foreign official: You arrange for the business to pay an additional "facilitation" payment to a foreign official to speed up an administrative process, such as clearing our goods through customs.

The offence of bribing a foreign public official is committed as soon as the offer is made. This is because it is made to gain a business advantage for us. We may also be found to have committed an offence.

6. WHAT YOU MUST NOT DO

It is not acceptable for you (or someone on your behalf) to:

(a) give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;

(b) give or accept a gift or hospitality during any commercial negotiations or tender process, if this could be perceived as intended or likely to influence the outcome;

(c) accept a payment, gift or hospitality from a third party that you know or suspect is offered with the expectation that it we will provide a business advantage for them or anyone else in return;

(d) accept hospitality from a third party that is unduly lavish or extravagant under the circumstances.

(e) offer or accept a gift to or from government officials or representatives, or politicians or political parties, without the prior approval of the board;

(f) threaten or retaliate against another individual who has refused to commit a bribery offence or who has raised concerns under this policy; or

(g) engage in any other activity that might lead to a breach of this policy.

7. FACILITATION PAYMENTS AND KICKBACKS

7.1 We do not make, and will not accept, facilitation payments or "kickbacks" of any kind.

7.2 Facilitation payments, also known as "back-handers" or "grease payments", are typically small, unofficial payments made to secure or expedite a routine or necessary action (for example by a government official). They are not common in the UK, but may be common in some other jurisdictions in which we operate.

7.3 Kickbacks are typically payments made in return for a business favour or advantage.

7.4 You must avoid any activity that might lead to a facilitation payment or kickback being made or accepted by us or on our behalf, or that might suggest that such a payment will be made or accepted. If you are asked to make a payment on our behalf, you should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. You should always ask for a receipt which details the reason for the payment. If you have any suspicions, concerns or queries regarding a payment, you should raise these with the board.

8. GIFTS, HOSPITALITY AND EXPENSES

8.1 This policy allows reasonable and appropriate hospitality or entertainment given to or received from third parties, for the purposes of:

(a) establishing or maintaining good business relationships;

(b) improving or maintaining our image or reputation; or

(c) marketing or presenting our products and/or services effectively.

8.2 The giving and accepting of gifts is allowed if the following requirements are met:

(a) it is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits;

(b) it is given in our name, not in your name;

(c) it does not include cash or a cash equivalent (such as gift certificates or vouchers);

(d) it is appropriate in the circumstances, taking account of the reason for the gift, its timing and value. For example, in the UK it is customary for small gifts to be given at Christmas;

(e) it is given openly, not secretly; and

(f) it complies with any applicable local law.

8.3 Promotional gifts of low value such as branded stationery to or from existing customers, suppliers and business partners will usually be acceptable.

8.4 Reimbursing a third party's expenses or accepting an offer to reimburse our expenses (for example, the costs of attending a business meeting) would not usually amount to bribery. However, a payment in excess

of genuine and reasonable business expenses (such as the cost of an extended hotel stay) is not acceptable.

8.5 We appreciate that practice varies between countries and regions and what may be normal and acceptable in one region may not be in another. The test to be applied is whether in all the circumstances the gift, hospitality or payment is reasonable and justifiable. The intention behind it should always be considered.

9. DONATIONS

9.1 We may make contributions to political parties but these are never made in an attempt to influence any decision or gain a business advantage, and are always publicly disclosed.

9.2 We only make charitable donations that are legal and ethical under local laws and practices.

10. RECORD-KEEPING

10.1 We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

10.2 You must declare and keep a written record of all hospitality or gifts given or received, which will be subject to our review.

10.3 You must submit all expenses claims relating to hospitality, gifts or payments to third parties in accordance with our expenses policy and record the reason for expenditure.

10.4 All accounts, invoices, and other records relating to dealings with third parties including suppliers and customers should be prepared with strict accuracy and completeness. Accounts must not be kept "off-book" to facilitate or conceal improper payments.

11. YOUR RESPONSIBILITIES

11.1 You must ensure that you read, understand and comply with this policy.

11.2 The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

11.3 You must notify HR as soon as possible if you believe or suspect that a conflict with this policy has occurred, or may occur in the future. For example, if a client or potential client offers you something to gain a business advantage with us, or indicates to you that a gift or payment is required to secure their business. Further "red flags" that may indicate bribery or corruption are set out in Paragraph 15.

12. HOW TO RAISE A CONCERN

12.1 You are encouraged to raise concerns about any issue or suspicion of bribery or corruption at the earliest possible stage.

12.2 If you are offered a bribe, or are asked to make one, or if you believe or suspect that any bribery, corruption or other breach of this policy has occurred or may occur, you must report it in accordance with our Whistleblowing Policy as soon as possible.

12.3 If you are unsure about whether a particular act constitutes bribery or corruption, raise it with HR.

13. PROTECTION

13.1 Individuals who refuse to accept or offer a bribe, or who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

13.2 We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place, or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform HR immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure.

14. COMMUNICATION

Our zero-tolerance approach to bribery and corruption should be communicated to all suppliers, contractors and business partners.

15. BREACHES OF THIS POLICY

15.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

15.2 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

16. POTENTIAL RISK SCENARIOS: "RED FLAGS"

The following is a list of possible red flags that may arise during the course of you working for us and which may raise concerns under various anti-bribery and anti-corruption laws. The list is not intended to be exhaustive and is for illustrative purposes only.

If you encounter any of these red flags while working for us, you must report them promptly using the procedure set out in the whistleblowing policy:

(a) you become aware that a third party engages in, or has been accused of engaging in, improper business practices;

(b) you learn that a third party has a reputation for paying bribes, or requiring that bribes are paid to them, or has a reputation for having a "special relationship" with foreign government officials;

(c) a third party insists on receiving a commission or fee payment before committing to sign up to a contract with us, or carrying out a government function or process for us;

(d) a third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;

(e) a third party requests that payment is made to a country or geographic location different from where the third party resides or conducts business;

(f) a third party requests an unexpected additional fee or commission to "facilitate" a service;

(g) a third party demands lavish entertainment or gifts before commencing or continuing contractual negotiations or provision of services;

(h) a third party requests that a payment is made to "overlook" potential legal violations;

(i) a third party requests that you provide employment or some other advantage to a friend or relative;

(j) you receive an invoice from a third party that appears to be non-standard or customised;

(k) a third party insists on the use of side letters or refuses to put terms agreed in writing;

(l) you notice that we have been invoiced for a commission or fee payment that appears large given the service stated to have been provided;

(m) a third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us;

(n) you are offered an unusually generous gift or offered lavish hospitality by a third party.

SCHEDULE 14 – ANTI-FACILITATION OF TAX EVASION POLICY

1. POLICY STATEMENT

1.1 It is our policy to conduct all of our business in an honest and ethical manner. We take a zero-tolerance approach to facilitation of tax evasion, whether under UK law or under the law of any foreign country.

1.2 We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter tax evasion facilitation.

1.3 We will uphold all laws relevant to countering tax evasion in all the jurisdictions in which we operate, including the Criminal Finances Act 2017.

2. ABOUT THIS POLICY

2.1 The purpose of this policy is to:

(a) set out our responsibilities, and of those working for us, in observing and upholding our position on preventing the criminal facilitation of tax evasion; and

(b) provide information and guidance to those working for us on how to recognise and avoid tax evasion.

2.2 As an employer, if we fail to prevent our employees, workers, agents or service providers facilitating tax evasion, we can face criminal sanctions including an unlimited fine, as well as exclusion from tendering for public contracts and damage to our reputation. We therefore take our legal responsibilities seriously.

2.3 We have identified that the following are particular risks for our business:

To address those risks we have taken the following steps:

2.4 In this policy, third party means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisers, representatives and officials, politicians and political parties.

2.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

3. WHO MUST COMPLY WITH THIS POLICY?

This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels.

4. WHO IS RESPONSIBLE FOR THE POLICY?

HR has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in preventing the facilitation of tax evasion.

5. WHAT IS TAX EVASION FACILITATION?

5.1 For the purposes of this policy:

(a) Tax evasion means the offence of cheating the public revenue or fraudulently evading UK tax, and is a criminal offence. The offence requires an element of fraud, which means there must be deliberate action, or omission with dishonest intent;

(b) Foreign tax evasion means evading tax in a foreign country, provided that conduct is an offence in that country and would be a criminal offence if committed in the UK. As with tax evasion, the element of fraud means there must be deliberate action, or omission with dishonest intent; and

(c) Tax evasion facilitation means being knowingly concerned in, or taking steps with a view to, the fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person, or aiding, abetting, counselling or procuring the commission of that offence. Tax evasion facilitation is a criminal offence, where it is done deliberately and dishonestly.

5.2 Under the Criminal Finances Act 2017, a separate criminal offence is automatically committed by a corporate entity or partnership where the tax evasion is facilitated by a person acting in the capacity of an "associated person" to that body. For the offence to be made out, the associated person must deliberately and dishonestly take action to facilitate the tax evasion by the taxpayer. If the associated person accidentally, ignorantly, or negligently facilitates the tax evasion, then the corporate offence will not have been committed. The company does not have to have deliberately or dishonestly facilitated the tax evasion itself; the fact that the associated person has done so creates the liability for the company.

5.3 Tax evasion is not the same as tax avoidance or tax planning. Tax evasion involves deliberate and dishonest conduct. Tax avoidance is not illegal and involves taking steps, within the law, to minimise tax payable (or maximise tax reliefs).

5.4 In this policy, all references to tax include national insurance contributions (and their equivalents in any non-UK jurisdiction).

6 WHAT YOU MUST NOT DO

It is not acceptable for you (or someone on your behalf) to:

(a) engage in any form of facilitating tax evasion or foreign tax evasion;

(b) aid, abet, counsel or procure the commission of a tax evasion offence or foreign tax evasion offence by another person;

(c) fail to promptly report any request or demand from any third party to facilitate the fraudulent evasion of tax (whether UK tax or tax in a foreign country), or any suspected fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person, in accordance with this policy;

(d) engage in any other activity that might lead to a breach of this policy; or

(e) threaten or retaliate against another individual who has refused to commit a tax evasion offence or a foreign tax evasion offence or who has raised concerns under this policy.

7. YOUR RESPONSIBILITIES

7.1 You must ensure that you read, understand and comply with this policy.

7.2 The prevention, detection and reporting of tax evasion and foreign tax evasion are the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

7.3 You must notify HR as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future. For example, if an employee or supplier asks to be paid into an offshore bank account, without good reason, or a supplier asks to be paid in cash, indicating that this will mean the payment is not subject to VAT. Further "red flags" that may indicate potential tax evasion or foreign tax evasion are set out in Clause 12.

8. HOW TO RAISE A CONCERN

8.1 You are encouraged to raise concerns about any issue or suspicion of tax evasion or foreign tax evasion at the earliest possible stage.

8.2 If you become aware of any fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person in the course of your work, or you are asked to assist another person in their fraudulent evasion of tax (whether directly or indirectly), or if you believe or suspect that any fraudulent evasion of tax has occurred or may occur, whether in respect to UK tax or tax in a foreign country, you must report it in accordance with our Whistleblowing Policy as soon as possible.

8.3 If you are unsure about whether a particular act constitutes tax evasion or foreign tax evasion, raise it with the HR as soon as possible. You should note that the corporate offence is only committed where you deliberately and dishonestly take action to facilitate the tax evasion or foreign tax evasion. If you do not take any such action, then the offence will not be made out. However, a deliberate failure to report suspected tax evasion or foreign tax evasion, or "turning a blind eye" to suspicious activity could amount to criminal facilitation of tax evasion.

9. PROTECTION

9.1 Individuals who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

9.2 We are committed to ensuring no one suffers any detrimental treatment as a result of:

(a) refusing to take part in, be concerned in, or facilitate tax evasion or foreign tax evasion by another person;

(b) refusing to aid, abet, counsel or procure the commission of a tax evasion offence or a foreign tax evasion offence by another person; or

(c) reporting in good faith their suspicion that an actual or potential tax evasion offence or foreign tax evasion offence has taken place, or may take place in the future.

9.3 Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform HR immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure.

10. COMMUNICATION

Our zero-tolerance approach to tax evasion and foreign tax evasion should be communicated to all suppliers, contractors and business partners.

11. BREACHES OF THIS POLICY

11.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

11.2 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

12. POTENTIAL RISK SCENARIOS: "RED FLAGS"

The following is a list of possible red flags that may arise during the course of you working for us and which may raise concerns related to tax evasion or foreign tax evasion. The list is not intended to be exhaustive and is for illustrative purposes only.

If you encounter any of these red flags while working for us, you must report them promptly using the procedure set out in the whistleblowing policy:

(a) you become aware, in the course of your work, that a third party has made or intends to make a false statement relating to tax, has failed to disclose income or gains to, or to register with, HMRC (or the equivalent authority in any relevant non-UK jurisdiction), has delivered or intends to deliver a false document relating to tax, or has set up or intends to set up a structure to try to hide income, gains or assets from a tax authority;

(b) you become aware, in the course of your work, that a third party has deliberately failed to register for VAT (or the equivalent tax in any relevant non-UK jurisdiction) or failed to account for VAT;

(c) a third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;

(d) you become aware, in the course of your work, that a third party working for us as an employee asks to be treated as a self-employed contractor, but without any material changes to their working conditions;

(e) a supplier or other subcontractor is paid gross when they should have been paid net, under a scheme such as the Construction Industry Scheme;

(f) a third party requests that payment is made to a country or geographic location different from where the third party resides or conducts business;

(g) a third party to whom we have provided services requests that their invoice is addressed to a different entity, where we did not provide services to such entity directly;

(h) a third party to whom we have provided services asks us to change the description of services rendered on an invoice in a way that seems designed to obscure the nature of the services provided;

(i) you receive an invoice from a third party that appears to be non-standard or customised;

(j) a third party insists on the use of side letters or refuses to put terms agreed in writing or asks for contracts or other documentation to be backdated;

(k) you notice that we have been invoiced for a commission or fee payment that appears too large or too small, given the service stated to have been provided;

(l) a third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us;

HEALTH & SAFETY

SCHEDULE 15 – HEALTH AND SAFETY POLICY

1. ABOUT THIS POLICY

1.1 We are committed to ensuring the health and safety of employee and anyone affected by our business activities, and to providing a safe and suitable environment for all those attending our premises.

1.2 This policy sets out our arrangements in relation to:

(a) assessment and control of health and safety risks arising from work activities;

(b) preventing accidents and work-related ill health;

(c) consultation with employees on matters affecting their health and safety;

(d) provision and maintenance of a safe workplace and equipment;

(e) information, instruction, training and supervision in safe working methods and procedures;

(f) emergency procedures in cases of fire or other major incident.

1.3 This policy covers all employee.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time. We will continue to review this policy to ensure it is achieving its aims.

2. RESPONSIBILITY FOR HEALTH AND SAFETY MATTERS

Our board has overall responsibility for health and safety and the operation of this policy and has delegated the day-to-day responsibility for health and safety matters HR.

3. YOUR RESPONSIBILITIES

3.1 All employee share responsibility for achieving safe working conditions. You must take care of your own health and safety and that of others, observe applicable safety rules and follow instructions for the safe use of equipment.

3.2 You should report any health and safety concerns immediately to HR.

3.3 You must co-operate with HR on health and safety matters, including the investigation of any incident.

3.4 Failure to comply with this policy may be treated as misconduct and dealt with under our Disciplinary and Capability Procedure.

4. INFORMATION AND CONSULTATION

4.1 We will inform and consult directly with employee regarding health and safety matters.

4.2 We will ensure any health and safety representatives receive the appropriate training to carry out their functions effectively.

5. TRAINING

5.1 We will ensure that you are given adequate training and supervision to perform your work competently and safely.

5.2 Employee will be given a health and safety induction and provided with appropriate safety training.

6. EQUIPMENT

6.1 You must use equipment in accordance with any instructions given to you. Any equipment fault or damage must immediately be reported to HR.

6.2 No employee should attempt to repair equipment unless trained to do so.

7. ACCIDENTS AND FIRST AID

7.1 Details of first aid facilities and the names of trained first aiders are displayed on the notice boards.

7.2 All accidents and injuries at work, however minor, should be reported to HR and recorded in the Accident Book which is kept on the Office SharePoint.

7.3 HR is responsible for investigating any injuries or work-related disease, preparing and keeping accident records, and for submitting reports to the relevant authorities if required under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR).

8. NATIONAL HEALTH ALERTS

8.1 In the event of an epidemic or pandemic alert we will organise our business operations and provide advice on steps to be taken by employee, in accordance with official guidance, to reduce the risk of infection at work as far as possible. Any questions should be referred to HR.

8.2 It is important for the health and safety of all our employee that you comply with instructions issued in these circumstances.

9. FIRE SAFETY

9.1 All employee should familiarise themselves with the fire safety instructions, which are displayed on notice boards and near fire exits in the workplace.

9.2 If you hear a fire alarm, leave the building immediately by the nearest fire exit and go to the fire assembly point by the car park gates. Do not stop to collect belongings. Do not re-enter the building until told to do so.

9.3 If you discover a fire do not attempt to tackle it unless it is safe and you have been trained or feel competent to do so. You should operate the nearest fire alarm and, if you have sufficient time, call reception and report the location of the fire.

9.4 Nominated individuals will be trained in the correct use of fire extinguishers.

9.5 You should notify HR if there is anything (for example, impaired mobility) that might impede your evacuation in the event of a fire. A personal evacuation plan will be drawn up and brought to the attention of colleagues working in your vicinity.

9.6 Fire drills will be held at least every 12 months and must be taken seriously.

10. RISK ASSESSMENTS AND MEASURES TO CONTROL RISK

We carry out general workplace risk assessments periodically. The purpose is to assess the risks to health and safety of employees, visitors and other third parties as a result of our activities, and to identify any measures that need to be taken to control those risks.

11. COMPUTERS AND DISPLAY SCREEN EQUIPMENT

11.1 If you use a computer screen or other display screen equipment (DSE) habitually as a significant part of your work:

(a) You should try to organise your activity so that you take frequent short breaks from looking at the screen.

(b) You are entitled to a workstation assessment.

(c) You are entitled to an eyesight test by an optician at our expense.

11.2 You should contact HR to request a workstation assessment.

SCHEDULE 16 – COVID-19 POLICY

1. WHAT YOU NEED TO KNOW

CWC were operating a homeworking policy during the COVID-19 pandemic, which was a temporary measure in alignment with government advice. CWC are now managing a return to the office, where required and appropriate to do so, in alignment with the government's current advice to 'learn to life safely with coronavirus (Covid 19)'.

2. AIM OF THIS POLICY

2.1 This policy is designed to explain the arrangements in place for homeworking and returning to the office to protect our employees and adhere to government guidelines. This policy applies to all employees, workers and contractors.

2.2 This policy covers the current Covid pandemic only; our general policies apply in all other instances.

3. HOURS OF WORK

3.1 You will be expected to work your usual fixed hours of work within normal office hours, unless flexibility has been agreed generally, or at specific points in time. You should work your normal contractual hours while homeworking.

3.2 If you are working from home, you must ensure that you take adequate breaks as follows:

- a break of at least 20 minutes for every six hours worked;
- a daily rest break of at least 11 hours; and
- at least one 24-hour break per week

4. EQUIPMENT AND EXPENSES

4.1 You should continue to use the equipment you are currently using which is reasonably required for you to work from home. Any equipment provided by us and/or our client, which will remain our or our clients' property, as appropriate.

4.2 Where equipment is provided you must:

- only use it for the purposes for which it was provided; and
- take reasonable care of it; and make it available to us for collection on the termination of your employment and at any other time if requested to do so.

4.3 We shall maintain our equipment at our expense, but you shall be responsible for any damage to the equipment which goes beyond ordinary wear and tear.

4.4 If you require additional resources please speak to HR and/or our client.

4.5 We are not responsible for general costs associated with you working from home, including the costs of heating, lighting, electricity, broadband internet where we request reasonable use of.

5. MANAGEMENT OF HOMEWORKING

5.1 When working from home you will be subject to all our normal rules, procedures and expected standards of conduct and performance. Contractual obligations, duties and responsibilities remain in place, as do our workplace policies.

5.2 You will be expected to attend such online meetings as required to fulfil your role and comply with any formal reporting procedures in your contract. You should expect to be in regular contact with us and/or our client when you are homeworking via phone, email, and video conferencing. If at any point you feel isolated or lacking guidance or support, discuss this with HR

5.3 Where an IT or another problem prevents you from working effectively from home, contact HR as soon as possible.

5.4 If, because of illness or injury, you cannot work on a day on which it has already been agreed that you would work from home, follow the procedure set out in our Sickness Absence policy.

6. INSURANCE

Working from home may affect your home and contents insurance policy. You must make any necessary arrangements to provide adequate cover for the fact you will be working from home and to cover the equipment you will be provided with for homeworking.

7. SECURITY

You will be responsible for ensuring the security of all equipment, documents and information; and must take all necessary steps to ensure that private and confidential material is kept secure at all times. In particular, you are required to:

- password protect any confidential information held on your home computer;
- lock your computer terminal whenever it is left unattended;
- store confidential papers securely when not in use;
- ensure the secure disposal of any confidential papers (for example by using a shredder if one is available);
- comply with our Data Protection and Acceptable Use of IT policies; and
- report any data security breach to HR immediately.

8. HEALTH AND SAFETY

Homeworkers have the same health and safety duties as other workers. You will be required to take reasonable care of your own health and safety while working at home and should comply with our Health and Safety Policy and follow all health and safety instructions issued by us from time to time. The following applies:

- Do not give clients or any other third parties details of your home address or home phone number. We retain the right to check all homeworking areas for health and safety purposes, including risk assessments to consider, for example, work equipment; display screen equipment; manual handling risks; and first aid access. Any accidents at home must be reported immediately to HR in accordance with our Health and Safety policy. Any health and safety concerns should be reported to HR.

9. TERMINATION OF HOMEWORKING

We will notify you when we decide to bring the home-working arrangement to an end, whether wholly or in part. Any homeworking arrangements are exceptional, and this arrangement does not guarantee a right to work from home indefinitely.

10. RETURNING TO WORK

10.1 We will manage your return to work safely and in line with government guidance. There may be additional measures of health and safely in place. These are in addition to those outlined in your employee handbook. The responsibilities of CWC and you are set out in 10.2 and 10.3 below. Please note, our clients will have their own arrangements, which you must make yourself familiar with:

10.2 Responsibilities of CWC:

- Provide hand sanitizer at entry and exit of office building and in bathrooms and kitchens.
- Promote the use of good handwashing practices.
- Keep the office well ventilated and clean.
- Allow you to adjust your working times to obtain Covid 19 vaccinations.
- Monitor outbreaks of Covid 19 in the workplace

10.3 Responsibilities of the individual

- Be conscious of all interactions with colleagues and other people when at or outside of work and maintaining appropriate distancing where appropriate.
- Adhere to government guidelines where you may be in contact with someone who has contracted COVID-19 or suspected of having contracted COVID-19, informing HR immediately.
- Adhere to government guidelines where you have symptoms of a respiratory infection, including Covid 19.
- Wash your own dishes, clean down workspaces or any shared spaces where you cannot avoid sharing with other colleagues immediately.

11. EXCEPTIONS

11.1 In some instances, we recognise that it may be more challenging for you to return to work, wholly or in part. This may be because you are sick, living with someone who is sick, self-isolating because you are high risk or self-isolating because someone in your household is high risk.

11.2 If you believe clause 11.1 above may apply to you, you should contact HR immediately. CWC reserve the right to determine whether it is possible for you to continue to carry out your duties or whether a return to work is appropriate.

11.3 Statutory sick pay (SSP) will only be payable if you meet the criteria and in accordance with government guidelines.

12. CERTIFYING ABSENCE FROM WORK

12.1 By law, medical evidence is not required for the first 7 days of sickness. After 7 days, employers may use their discretion around the need for medical evidence if an employee is staying at home.

13. WHAT TO DO IF AN EMPLOYEE NEEDS TIME OFF WORK TO LOOK AFTER SOMEONE

13.1 Employees are entitled to time off work to help someone who depends on them (a 'dependant') in an unexpected event or emergency. This would apply to situations related to coronavirus (COVID-19). For example:

- if you have children they need to look after or arrange childcare for because their school has closed; or
- to help their child or another dependent if they're sick, or need to go into isolation or hospital

13.2 This would be unpaid and there is no statutory right to pay for this time off.

ADDITIONAL INFORMATION

14. WHAT YOU NEED TO KNOW ABOUT CORONAVIRUS AND FOOD

14.1 It is believed very unlikely that you can catch coronavirus from food, COVID-19 is a respiratory illness. It is not known to be transmitted by exposure to food or food packaging either.

14.2 Although it is believed very unlikely that coronavirus is transmitted through food, as a matter of good hygiene practice anyone handling food or using a shared food preparation area should wash their hands often with soap and water for at least 20 seconds. This should be done as a matter of routine, before and after handling food, and especially after being in a public place, blowing their nose, coughing, or sneezing.

15. BASIC HYGIENE

CWC stress the importance of more frequent handwashing and maintaining good hygiene practices in the shared offices in every instance. Employees should wash their hands for 20 seconds, especially after being in a public place, blowing their nose, coughing or sneezing or using any shared space. Employees are recommended to wear face coverings although this is not a requirement as per government advice.

16. MANGAGING EMPLOYEE SICKNESS

16.1 If you or an employee becomes unwell with a new, continuous cough or a high temperature in the business or workplace you will be sent home and advised to follow testing guidelines. If you or another employee are experiencing symptoms, visit NHS 111 online or call 111 if there is no internet access. In an emergency, call 999 if they are seriously ill or injured, or their or your life is at risk.

16.2 If you or another employee has helped someone who was taken unwell with a new, continuous cough or a high temperature, they do not need to go home unless they develop symptoms themselves. They should wash their hands thoroughly for 20 seconds after any contact with someone who is unwell with symptoms consistent with coronavirus infection.

DATA GOVERNANCE & PROTECTION

SCHEDULE 17 – DATA PROTECTION POLICY (GDPR)

This policy covers all employee and does not form part of any employee's contract of employment and we may amend it at any time.

1. INTERPRETATION

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: CrossWind Consulting LLP

Company Personnel: all employees, workers contractors, agency workers, consultants, Managing Partners, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 27 countries in the EU, and Iceland, Liechtenstein, Norway and the United Kingdom.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: the Company privacy and GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available on SharePoint.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available on SharePoint.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. The Company will treat the following types of data as if they are Special Categories of Personal Data.

2. INTRODUCTION

2.1 This Data Protection Policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

2.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

2.3 This policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this policy may result in disciplinary action.

2.4 Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this policy or otherwise then you must comply with the Related Policies and Privacy Guidelines.

2.5 This Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. SCOPE

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

3.2 All employee are responsible for ensuring all Company Personnel comply with this policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3 The DPO is responsible for overseeing this policy and, as applicable, developing Related Policies and Privacy Guidelines.

3.4 Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see Paragraph 5.1 below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see Paragraph 6 below);

(c) if you need to draft Privacy Notices (see Paragraph 7 below);

(d) if you are unsure about the retention period for the Personal Data being Processed (see Paragraph 11 below);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see Paragraph 12.1 below);

(f) if there has been a Personal Data Breach (Paragraph 13 below);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see Paragraph 14 below);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see Paragraph 15);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see Paragraph 19 below) or plan to use Personal Data for purposes other than what it was collected for;

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Paragraph 20 below);

(k) if you need help complying with applicable law when carrying out direct marketing activities (see Paragraph 21 below); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Paragraph 22 below).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(d) accurate and where necessary kept up to date (Accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

(f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

(g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS AND FAIRNESS

5.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices; or

5.4 You must identify and document the legal ground being relied on for each Processing activity in accordance with the Company's guidelines on Lawful Basis for Processing Personal Data.

6. CONSENT

6.1 A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

6.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

6.5 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that the Company can demonstrate compliance with Consent requirements.

7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

7.1 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7.4 If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

7.5 You must comply with the Company's guidelines on drafting Privacy Notices.

8. PURPOSE LIMITATION

8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

9. DATA MINIMISATION

9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

9.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

10. ACCURACY

10.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

10.2 You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

11.2 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time. You must comply with the Company's guidelines on Data Retention.

11.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

11.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

12. PROTECTING PERSONAL DATA

12.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

12.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

12.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

12.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data].

13. REPORTING A PERSONAL DATA BREACH

13.1 The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

13.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

13.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches and follow the Security Breach Response Plan. You should preserve all evidence relating to the potential Personal Data Breach.

14. TRANSFER LIMITATION

14.1 The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

14.2 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

14.3 You must comply with the Company's guidelines on cross-border data transfers.

15. DATA SUBJECT'S RIGHTS AND REQUESTS

15.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority;

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format; and

15.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

15.3 You must immediately forward any Data Subject request you receive to DPO (or equivalent) and comply with the company's Data Subject response process.

16. ACCOUNTABILITY

16.1 The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this policy, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly training Company Personnel on the GDPR, this policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. RECORD-KEEPING

17.1 The GDPR requires us to keep full and accurate records of all our data Processing activities.

17.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's record keeping guidelines.

17.3 These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To

create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. TRAINING AND AUDIT

18.1 We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

18.2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with the Company's mandatory training guidelines.

18.3 You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

19. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

19.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

19.2 You must assess what Privacy by Design measures can be implemented on all programmes, system or processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

19.3 Data controllers must also conduct DPIAs in respect to high-risk Processing.

19.4 You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) automated Processing including profiling and ADM;

(c) large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

(d) large-scale, systematic monitoring of a publicly accessible area.

19.5 A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

You must comply with the Company's guidelines on DPIA and Privacy by Design.

20. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

20.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

20.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but that Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

20.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

20.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

20.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

20.6 Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Company's guidelines on profiling or ADM.

21. DIRECT MARKETING

21.1 We are subject to certain rules and privacy laws when marketing to our customers.

21.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

21.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

21.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

21.5 You must comply with the Company's guidelines on direct marketing to customers.

22. SHARING PERSONAL DATA

22.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

22.3 You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

22.4 You must comply with the Company's guidelines on sharing data with third parties.

23. CHANGES TO THIS DATA PROTECTION POLICY

23.1 We keep this policy under regular review.

23.2 This policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

SCHEDULE 18 – CONFIDENTIALITY POLICY

1. ABOUT THIS POLICY

1.1 We keep certain types of information confidential for important business reasons, including to comply with legal requirements (such as data protection and competition law), and to maintain a competitive edge over competitors.

1.2 Because of the importance of maintaining the confidentiality of certain information, and because effective procedures for maintaining confidentiality require everyone's involvement and cooperation, we have implemented this confidential information policy.

1.3 This policy covers all employee.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

1.5 You will also be subject to such of our clients' Confidentiality and related policies as are relevant. Our policies take precedence in relation to our information and systems and our clients' policies take precedence in relation to their information and systems, to the extent they conflict.

2. RESPONSIBILITY FOR THIS POLICY

2.1 The board has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to HR.

2.2 HR has a specific responsibility to ensure the fair application of this policy and all members of employee are responsible for supporting colleagues and ensuring its success.

3. DEFINITION OF CONFIDENTIAL INFORMATION

Business Operations: operational information, including but not limited to, internal personnel and financial information, vendor names and other vendor information (including vendor characteristics, services and agreements), purchasing and internal cost information, internal services and operational manuals, and the manner and methods of conducting our business.

Confidential Information: data and information (whether or not recorded in documentary form, or stored on any magnetic or optical disk or memory) relating to the business, products, management, affairs and finances of us or any group company or our clients, for the time being confidential to us or any group company or our clients, and trade secrets including, without limitation, technical data and know-how relating to the business of ours or any group company or our clients, or any of their business contacts, as well as proprietary and trade secret technology and accounting records to which access is obtained by you, including Work Product, Computer Software, Other Proprietary Data, Business Operations, Marketing and Development Operations, and Client Information. Also includes any information that has been disclosed by a third party to us and is governed by data protection laws or by a non-disclosure agreement entered into between that third party and us. Also includes (but not limited to) information that you create, develop, receive or obtain in connection with this employment, whether or not such information (if in anything other than oral form) is marked confidential.

Computer Software: computer software resulting from or related to work or projects performed or to be performed for us or for our clients, of any type or form in any stage of actual or anticipated research and development, including but not limited to, programs and program modules, routines and subroutines, processes, algorithms, design concepts, design specifications (design notes, annotations, documentation, flowcharts, coding sheets, and the like), source code, object code and load modules, programming, program patches and system designs.

Client Information: client information, including but not limited to, names of clients and their representatives, contracts and their contents and parties, client services, data provided by clients and the type, quantity and specifications of products and services purchased, leased, licensed or received by our clients.

Other Proprietary Data: information relating to our proprietary rights prior to any public disclosure of such information, including but not limited to, the nature of the proprietary rights, production data, technical and engineering data, test data and test results, the status and details of research and development of products and services, and information regarding acquiring, protecting, enforcing and licensing proprietary rights (including patents, copyrights and trade secrets).

Marketing and Development Operations: marketing and development information, including but not limited to, marketing and development plans, price and cost data, price and fee amounts, pricing and billing policies, quoting procedures, marketing techniques and methods of obtaining business, forecasts and forecast assumptions and volumes, and future plans and potential strategies of ours which have been or are being considered.

Work Product: work product information, including but not limited to, work product resulting from or related to work or projects performed or to be performed for us or for our clients, of any type or form in any stage of actual or anticipated research and development.

4. CONFIDENTIALITY

4.1 You shall not (except in the proper course of your duties), either during the employment or at any time after its termination (however arising), use or disclose to any person, employer or other organisation whatsoever (and shall use your best endeavours to prevent the publication or disclosure of) any Confidential Information. This shall not apply to:

(a) any use or disclosure authorised by CWC or required by law;

(b) any information which is already in, or comes into, the public domain other than through your unauthorised disclosure; or

(c) any protected disclosure within the meaning of section 43A of the Employment Rights Act 1996.

4.2 The Confidential Information will not include anything developed or produced by you during your term of employment with us, including but not limited to, any intellectual property, process, design, creation, research, invention, know-how, trade name or copyright that:

(a) was not developed with the use of our equipment, supplies, facility or Confidential Information;

(b) was developed entirely on the Employee's own time;

(c) does not result from any work performed by you for us; and

(d) does not relate to any actual or reasonably anticipated business opportunity of ours.

5. DUTIES AND OBLIGATIONS CONCERNING CONFIDENTIAL INFORMATION

5.1 You agree that a material term of your contract with us is to keep all Confidential Information absolutely confidential and protect its release from the public. You agree not to divulge, reveal, report or use, for any purpose, any of the Confidential Information which you have obtained or which was disclosed to you by or through us as a result of your employment by us. You agree that if there is any question as to such disclosure then you will seek out HR prior to making any disclosure of our, or any group company, or our clients' information that may be covered by this policy.

5.2 You agree and acknowledges that the Confidential Information is of a proprietary and confidential nature and that any disclosure of the Confidential Information to a third party in breach of this policy cannot be reasonably or adequately compensated for in money damages, would cause irreparable injury to us, would gravely affect the effective and successful conduct of the our business, reputation and goodwill, and would be a material breach of your employment and this policy.

5.3 You agree and acknowledge that you will not send any Confidential Information outside of our or any group company, or our clients' secure email or IT systems, which includes not sending any Confidential Information to your personal email accounts, or a third party email address (unrelated to the work being undertaken) nor your own or third party owned laptops, PCs, external drives and any other removable electronic media.

5.4 The obligations to ensure and protect the confidentiality of the Confidential Information imposed on you in this policy and any obligations to provide notice under this policy will survive the expiration or termination, as the case may be, of your employment and will continue for one (1) year from the date of such expiration or termination, except in the case of any Confidential Information which is a trade secret or governed by data protection laws or non-disclosure agreement in which case those obligations will last indefinitely, or in line with our data protection policies and the non-disclosure agreement, as appropriate.

5.5 You may disclose any of the Confidential Information:

a) To a third party where we have consented in writing to such disclosure; or

b) To the extent required by law or by the request or requirement of any judicial, legislative, administrative or other governmental body after providing reasonable prior notice to us.

5.6 If you lose or make unauthorised disclosure of any of the Confidential Information, you will immediately notify us and take all reasonable steps necessary to retrieve the lost or improperly disclosed Confidential Information.

6. CO-OWNERSHIP AND TITLE TO CONFIDENTIAL INFORMATION

6.1 You acknowledge and agree that all rights, title and interest in any Confidential Information will remain the exclusive property of our, or our group company, or our clients, as appropriate. Accordingly, you specifically agree and acknowledge that you will have no interest in the Confidential Information, including, without limitation, no interest in know-how, copyright, trade-marks or trade names,

notwithstanding the fact that you may have created or contributed to the creation of the Confidential Information.

6.2 You waive any moral rights that you may have with respect to the Confidential Information.

6.3 You agree to immediately disclose to us all Confidential Information developed in whole or in part by you during your term of employment with us and to assign to us any right, title or interest you may have in the Confidential Information. You agree to execute any instruments and to do all other things reasonably requested by, both during and after your employment with us, in order to vest more fully in us all ownership rights in those items transferred by you to us.

7. RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

7.1 You agree that, upon our request or upon termination or expiration, as the case may be, of your employment, you will destroy and/or turn over to us all Confidential Information belonging to us, or a group company or our clients, including but not limited to, all documents, plans, specifications, disks or other computer media, as well as any duplicates or backups made of that Confidential Information in whatever form or media, in your possession or control that:

a) may contain or be derived from ideas, concepts, creations, or trade secrets and other proprietary and Confidential Information as defined in this policy; or

b) Is connected with or derived from your employment with us.

7.2 You agree to use your best endeavours to ensure any third party also destroys any Confidential Information you have shared with them in breach of this policy.

7.3 You agree to promptly provide such evidence as we may reasonable require of your compliance with 6.1 and 6.2 above.

8. CONFIDENTIALITY AGREEMENTS

We may require you and certain third parties to sign a confidentiality agreement when receiving any of our, or our clients', Confidential Information. You must help ensure the protection of this Confidential Information by complying with this requirement when communicating or sharing information with a third party with whom we are doing business.

9. MONITORING

9.1 We reserve the right to monitor, intercept and review, without further notice, employee activities using our IT resources and communications systems, including but not limited to social media postings and activities, for legitimate business purposes which include ascertaining and demonstrating that expected standards are being met by those using the systems and for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

9.2 For further information, please refer to our IT and Communications Systems Policy.

10. BREACH OF THIS POLICY

Breach of this policy may result in disciplinary action up to and including dismissal. Any employee suspected of committing a breach of this policy will be required to co-operate with our investigation. You

may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

SCHEDULE 19 – RECORDS MANAGEMENT POLICY

1. ABOUT THIS POLICY

1.1 This policy sets out our commitment to achieving high standards in records management.

1.2 This policy covers all employees and their day-to-day activity.

2. PURPOSE OF POLICY

2.1 Records management is vital to the delivery of our services in an orderly, efficient and accountable manner. Effective records management will help ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why, therefore protecting the interests of CWC.

2.2 Records, and the information they preserve, are an important corporate asset and corporate memory.

2.3 The life cycle of records and information must be managed, from creation, to use or handling, to retention, appraisal and either disposal or permanent preservation.

2.4 Through this policy we aim to ensure that the record, in whichever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

- Help us carry out day to day operational and business activity
- Help us to make informed decisions
- Protect the rights of employees
- Reduce costs through the better use of physical and online storage and use of employee time
- Track policy changes and development
- Make sure we comply with relevant legislation
- Provide an audit trail to meet business, regulatory and legal requirements
- Support continuity and consistency in management and administration
- Promote our aims and achievements

2.5 This policy will help us understand our duties and responsibilities within records management, to include legal obligation and statutory provisions and the 'information life cycle'.

3. SCOPE

This policy applies to the management of all documents and records, in all technical or physical formats or media, created or received by CWC in the conduct of its business activities, through their life cycle.

4. RESPONSIBILITIES

4.1 We have a responsibility to ensure that our records are managed well. Different employees have different roles in relation to records management and these responsibilities are detailed below:

4.2 **Accounting Officer (Data Privacy Officer)**: overall responsibility for records management

4.3 **Information Asset Owners**: responsible for ensuring local procedures and guidance is in place which comply with the records management policy and standards.

4.4 **Information Steering Group**: responsible for agreeing the records management policy and considering and approving changes to it.

4.5 **All employees and third parties**: everyone who receives, creates, maintains or has access to our documents and records is responsible for ensuring they act in accordance with our records management policy, standards guidance and procedures.

5. RELEVANT STANDARDS, GUIDANCE AND PROCEDURES

5.1 **Standards**: standards that set out how we will establish, implement, maintain and continually improve records management.

5.2 **Guidance**: sets out recommended best practice in support of the standards or to serve as a reference when no standard is in place.

5.3 **Procedures**: set out step-by-step instructions to assist employees in implementing this policy and its supporting standards.

6. MONITORING & COMPLIANCE

6.1 Ongoing monitoring of compliance with this policy and supporting standards will be undertaken on a regular basis by the Information Asset Owners and Information Steering Group.

6.2 Where we have identified a breach of our Records Management policy or procedures, we will carry out an assessment to identify the contributory causes and impact of the breach, which we may, in turn, use to improve our policy and/or procedures.

7. RECORDS INVENTORY & PROCEDURES

7.1 Our Records Inventory sets out (separately for each client and internal) a list of all records created, received, stored, processed or destroyed: identification and description (title, date, author, or reference number), format (language, software version, graphics) and media (paper, electronic).

7.2 Our records management system covers company, client and personal data and documents, which we manage through our policies and processes, which include:

- Records Retrieval
- Records Destruction
- Records Protection (accidental and malicious)
- Legal Hold
- Records Handover
- Records Retention
- Records Storage
- Personal Data

8. INFORMATION AND TRAINING

Records Management will be included in employee inductions, and subsequent appropriate training will be provided annually.

INFORMATION TECHNOLOGY

SCHEDULE 20 – IT AND COMMUNICATIONS SYSTEMS SECURITY POLICY

1. ABOUT THIS POLICY

1.1 Our, and our client's, IT and communications systems are intended to promote effective communication and working practices within our and their organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards and the standards set by our clients, where relevant.

1.2 This policy covers all employees and anyone who has access to our, or our clients', IT and communication systems. It applies to access both during and outside office hours and whether or not access takes place at your normal place of work and through any equipment.

1.3 Misuse of IT and communications systems can damage our and our clients' business and reputation. Breach of this policy may be dealt with under our Disciplinary and Capability Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

1.5 You will also be subject to such of our clients' IT and Communications and related policies as are relevant. Our policies take precedence in relation to our information and systems and our clients' policies take precedence in relation to their information and systems, to the extent they conflict.

2 SCOPE AND PURPOSE OF THE POLICY

2.3 When you access our, or our clients', systems you may be able to access data about us, our clients and other business connections and third parties, including information which is confidential, proprietary or private. The definition of data is very broad, and includes all written, spoken and electronic information held, used or transmitted by us or on our behalf, in whatever form (collectively referred to as company data in this policy).

2.4 When you access our, or our clients', systems, we and/or our clients are exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our and/or our clients' systems or company data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of company data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our and/or our clients' systems, business and reputation.

2.5 The purpose of this policy is to protect our and our clients' systems and company data, and to prevent company data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our and/or our clients' systems as appropriate. This policy sets out the circumstances in which we may monitor your use of our and our clients' (to the extent we are able) systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

2.6 Breach of this policy may lead to us revoking your access to our and/or our clients' systems. It may also result in disciplinary action up to and including dismissal or termination. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

3. EQUIPMENT SECURITY AND PASSWORDS

3.1 You are responsible for the security of the equipment allocated to or used by you and must not allow it to be used by anyone other than in accordance with this policy.

3.2 You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.

3.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the IT department.

3.4 You should use strong, dual authenticated passwords to access IT systems. Devices, particularly items that you take out of the office, must be protected by a strong and unique password. You must keep your passwords confidential you must not use another person's username and password or make available or allow anyone else to log on using your username and password unless explicitly authorised by the IT department. On the termination of employment (for any reason) HR will revoke your access to IT systems and you must return any equipment, key fobs or cards. For the avoidance of doubt, a strong password is one that contains a mixture of upper and lower cases, numbers and special characters.

3.5 Our IT system will log key events such as logins (whether failed or successful) to protect us against tampering and unauthorised access. These logs will be monitored by HR on a regular basis to detect for any unauthorised access attempts. Resulting actions will be monitored.

3.6 If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, nearby passengers on public transport.

4. SYSTEMS AND DATA SECURITY

4.1 You should not delete, destroy or modify existing systems, programmes, information or data (except as authorised in the proper performance of your duties).

4.2 You must not download or install software from external sources without authorisation from our, or our clients', IT, department (as appropriate). This includes software programmes, instant messaging programs, screensavers, photos, video clips and music files.

4.3 You must not attach any device or equipment to our or our clients' systems without authorisation from our, or our clients', IT department, as appropriate. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.

4.4 We monitor all emails passing through our system for viruses (and our clients are likely to do the same) and you must ensure that operating software is updated to the latest version at all times. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform our, or our clients', IT department, as appropriate, immediately if you suspect your computer may have a virus. We reserve the right for us or our clients to delete or block access to emails or attachments in the interests of security. We also reserve our and our clients' right not to transmit any email message.

4.5 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

4.6 You must be particularly vigilant if you use IT equipment outside the workplace and take such precautions as we, or our clients', may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

4.7 We operate a clear desk policy and you should ensure that monitor screens are locked when unattended. This applies whether you are working at client site or from home. Any and all client or CWC sensitive information must be disposed of in a secure manner, in line with its classification. Upon termination of your contract with us you must ensure that all client equipment is returned to your client and any client information is destroyed in line with their IT policy.

4.8 The backup and testing of IT software and systems is outsourced to Microsoft. This includes the controls for testing and applying security patches and controls for secure system development and testing. Further information on this can be sought from HR.

5. EMAIL

5.1 Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

5.2 You should access your emails at least once every working day, stay in touch by remote access when travelling in connection with our business, and use an out of office response when away from the office for more than a day. You should endeavour to respond to emails marked "high priority" within 24 hours.

5.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails. Anyone who feels that they have been harassed or bullied or are offended by material received from a colleague via email should inform HR.

5.4 You should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

5.5 Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

5.6 In general, you should not:

(a) send or forward private emails at work which you would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;

(d) sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

(e) agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

(f) download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

(g) send messages from another person's email address (unless authorised) or under an assumed name; or

(h) send confidential messages via email or the internet, or by other means of external communication which are known not to be secure; or

(g) send work or client emails to your personal email address, or any other email address unrelated to CWC, their clients or the work you are carrying out.

5.7 If you receive an email in error you should inform the sender.

5.8 Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account we have provided for you.

6. USING THE INTERNET

6.1 Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out in Paragraph 6.

6.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in Paragraph 8.1, such a marker could be a source of embarrassment to the visitor, us, or our clients, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature. This is further considered under Paragraph 8.

6.3 You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

6.4 You should not under any circumstances use our, or our clients', systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

6.5 The following must never be accessed from our network: online radio, audio and video streaming, instant messaging and webmail (such as such as Gmail or Hotmail) and social networking sites (such as Facebook, Instagram Twitter, YouTube). This list may be modified from time to time.

6.6 The use of the internet and internet based platforms to communicate and facilitate business meetings and exchange of information, including, but not limited to Teams is permitted, subject to prior approval of their use and related costs. The use of these services is subject to the policies set out in the Employee

Handbook, with particularly attention to Confidentiality, Data Protection and IT security. It is forbidden to conduct meetings on these services in a public place, or in such places where confidentiality cannot be maintained. It is further forbidden to record such meetings, without the authority of a Managing Partner.

7. PERSONAL USE OF IT SYSTEMS

7.1 We permit the incidental use of our internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion. You must adhere to the clients' standards in relation to their systems.

7.2 Personal use must meet the following conditions:

(a) use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm);

(b) personal emails should be labelled "personal" in the subject header;

(c) use must not interfere with business or office commitments;

(d) use must not commit us to any marginal costs; and

(e) use must comply with this policy (see in particular Paragraph 4 and 5) and our other policies including the Anti-harassment Policy, Data Protection Policy, Disciplinary Rules and The Equality Act 2010.

7.3 You should be aware that personal use of our and our clients' systems may be monitored (see Paragraph 7) and, where breaches of this policy are found, action may be taken under the Disciplinary and Capability Procedure (see Paragraph 8). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive. We reserve the right for our clients to monitor and restrict your access on their own systems.

8. MONITORING

8.1 Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes. We reserve the right for our clients to monitor your use of their telephone, email, voicemail, internet and other communications.

8.2 We reserve the right for us, or our clients, to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

9. PROHIBITED USE OF OUR SYSTEMS

9.1 Misuse or excessive personal use of our, or our clients', telephone or email system or inappropriate internet use will be dealt with under our Disciplinary and Capability Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our, or our clients', systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

(e) confidential information about us or any of our employee or clients (except as authorised in the proper performance of your duties);

(f) Unauthorised software;

(g) any other statement which is likely to create any criminal or civil liability (for you or us); or

(h) music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

9.2 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary and Capability Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses involved in the Disciplinary and Capability Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

SCHEDULE 21 – BRING YOUR OWN DEVICE TO WORK (BYOD) POLICY

1. ABOUT THIS POLICY

1.1 We recognise that many of our employee have personal mobile devices (such as tablets, smartphones and handheld computers), which they could use for business purposes, and that there can be benefits for both us and employee, including increased flexibility in our working practices, in permitting such use. However, the use of personal mobile devices for business purposes gives rise to increased risk in terms of the security of our and our clients' IT resources and communications systems, the protection of confidential and proprietary information and reputation, and compliance with legal obligations.

1.2 We have chosen to implement this policy as we recognise that using personal mobile devices for business purposes can offer increased flexibility and autonomy for our employee. However, we also encourage our employee to consider carefully how and when you use your device and maintain an effective balance between work and personal life.

1.3 This policy covers all employee.

1.4 Certain obligations under this policy are contractual and will form part of your contract of employment. These are clearly identified. The remaining sections of this policy do not form part of any employee's contract of employment and we may amend it at any time, including the contractual obligations that it places on employee, or remove the policy entirely, at any time.

1.5 This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our IT and Communications Systems Policy, Data Protection Policy, Data Retention Policy, and other IT related policies, which are available.

1.6 You will also be subject to such of our clients' BYOD related policies as are relevant. Our policies take precedence in relation to our information and systems and our clients' policies take precedence in relation to their information and systems, to the extent they conflict.

2. SCOPE AND PURPOSE OF THE POLICY

2.1 This policy applies to employee who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) for business purposes. It applies to use of the device both during and outside office hours and whether or not use of the device takes place at your normal place of work.

2.2 This policy applies to all devices used to access our, or our clients', IT resources and communications systems (collectively referred to as systems in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, tablets, and laptop or notebook computers.

2.3 When you access our, or our clients', systems you may be able to access data about us or our clients, as well as group companies, customers, clients, distributors, suppliers and other business connections, including information which is confidential, proprietary or private. The definition of data is very broad, and includes all written, spoken and electronic information held, used or transmitted by us or on our behalf, in whatever form (collectively referred to as company data in this policy).

2.4 When you access our, or our clients', systems using a device, we and/or our clients are exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our systems or company data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our, or our clients', systems via a device) and the loss or unauthorised alteration of company data (including personal and confidential information which could

expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our, or our clients', systems, business and reputation.

2.5 The purpose of this policy is to protect our, and our clients', systems and company data, and to prevent company data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our, and our clients', systems using a device. This policy sets out the circumstances in which we may monitor your use of our, and our clients', systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy. More information about how we monitor, record and process your personal data is contained in our separate Data Protection Policy. We reserve our clients' right to monitor your use in line with their own standards.

2.6 Breach of this policy may lead to us, or our clients revoking your access to our, or their, systems respectively, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal or termination of the engagement. It may also lead in some cases to possible criminal charges. Disciplinary action may be taken whether the breach is committed during or outside office hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

2.7 Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist employee in connecting to our systems.

3. CONNECTING DEVICES TO OUR SYSTEMS

3.1 Devices must comply with our and/or our clients' IT and Communications Policy, as appropriate.

3.2 Before using your device to connect to our, or our clients', systems, or to access company data, in accordance with this policy, you must comply with any reasonable requirements, to include approval and technical security.

3.3 We reserve the right to refuse or remove permission for any device to connect with our systems and will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, us and/or our clients, employee, business connections, systems, or company data at risk or that may otherwise breach this policy.

3.4 In order to access our systems it may be necessary for software applications to be installed on your device. If you remove any such software, your access to our systems may be disabled.

4. MONITORING

4.1 The contents of our, and our clients', systems and company data are our/their property respectively. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on our, or our clients', behalf is our, or our clients', property, as appropriate, regardless of who owns the device.

4.2 We reserve the right for us and our clients to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us, or our clients, or on our or our clients' behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-

ins, recordings and other uses of the device as well as keystroke capturing and other network monitoring technologies, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore you should have no expectation of privacy in any data on the device. Employee are advised not to use our systems for any matter intended to be kept private or confidential. If you use your device to process personal data about third parties (for example your family and friends) you should be aware that this may be inadvertently monitored, intercepted, reviewed or erased.

4.3 Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for us, or our clients, to comply with a legal obligation or for our or our clients' legitimate business purposes, including, without limitation, in order to:

(a) prevent misuse of the device and protect company data;

(b) ensure compliance with our, or our clients', rules, standards of conduct and policies in force from time to time (including this policy);

(c) monitor performance at work; and

(d) ensure that employee members do not use our, or our clients', facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

4.4 We and our clients may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

4.5 You acknowledge that we and our clients are entitled to conduct such monitoring where it has a legitimate basis to do so, and you confirm your agreement (without further notice or permission) to our and our clients' right to copy, erase or remotely wipe the entire device (including any personal data stored on the device). You also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

5. SECURITY REQUIREMENTS

5.1 You must comply with our IT and Communications Systems Policy when using your device to connect to our systems and our clients' relevant policies when using your device to connect to their systems.

5.2 In addition, and to the extent our, or our clients', IT and Communications Systems Policy does not address the issues below, you must:

(a) at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device;

(b) install any anti-virus or anti-malware software at our, or our clients', request before connecting to our, or our clients', systems and consent to our, and our clients', efforts to manage the device and secure its data, including providing us with any necessary passwords;

(c) comply with our, or our clients', device configuration requirements, as appropriate.

(d) protect the device with a PIN number or strong password, and keep that PIN number or password secure at all times. The PIN number or password should be changed regularly. If the confidentiality of a PIN number or password is compromised, you must change it immediately. The use of PIN numbers and passwords should not create an expectation of privacy by you in the device;

(e) maintain the device's original operating system and keep it current with security patches and updates. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing out systems or company data;

(f) not download or transfer any company data to the device, for example via e-mail attachments, unless specifically authorised to do so. Employee must immediately erase any such information that is inadvertently downloaded to the device;

(g) save any CWC or client information to your personal device. Ensure that all work is saved to either the client cloud or your CWC OneDrive account;

(h) not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of company data. Any such backups inadvertently created must be deleted immediately;

(i) where we, or our client, have permitted you to store company data on the device, ensure that the company data is encrypted using appropriate encryption technologies;

5.3 We reserve the right for us, and our client, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the company data on it for legitimate business purposes, which include (without limitation) enabling us to:

(a) inspect the device for use of unauthorised applications or software;

(b) inspect any company data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect company data;

(c) investigate or resolve any security incident or unauthorised use of our systems;

(d) conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and

(e) ensure compliance with our, or our clients', rules, standards of conduct and policies in force from time to time (including this policy).

You must co-operate with us, and our client, to enable such inspection, access and review, including providing any passwords or PIN numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal. This Paragraph 5.3 of the policy is contractual.

5.4 If we, or our clients, discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we, or our clients may, immediately remove access to our or their systems and, where appropriate, remove any company data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from company data in all circumstances. You should therefore regularly backup any personal data contained on the device.

5.5 You consent to us, without further notice or permission, inspecting a device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using some or all of the data on or from a device for the legitimate business purposes set out above.

6. LOST OR STOLEN DEVICES AND UNAUTHORISED ACCESS

6.1 In the event of a lost or stolen device, or where a employee member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the employee member must report the incident to the HR immediately.

6.2 Appropriate steps will be taken to ensure that company data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all company data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature). Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from company data in all circumstances. You should therefore regularly backup all personal data stored on the device.

7. PROCEDURE ON TERMINATION OF EMPLOYMENT AND SELLING, TRANSFERRING OR REPLACING THE DEVICE

On your last day of work, or your last day before commencing a period of garden leave, or when you intend to sell or transfer your device to anyone else, or to sell it, all company data (including work e-mails), and any software applications provided by us for business purposes, will be removed from the device. You must provide all necessary co-operation and assistance in relation to this process. This Paragraph 7 of the policy is contractual.

8. PERSONAL DATA

8.1 We, and our clients, have a legitimate basis on which to access and protect company data stored or processed on your device, including the content of any communications sent or received from the device. However, we recognise the need to balance our obligation to process data for legitimate purposes, with your expectations of privacy in respect of your personal data. Therefore, when taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, we will, where practicable:

(a) consider whether the action is proportionate in light of the potential damage to the company, our customers or other people impacted by company data;

(b) consider if there is an alternative method of dealing with the potential risks to the company's interests (recognising that such decisions often require urgent action);

(c) take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur; and

(d) delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data which is also company data, including all personal emails sent or received using our email system).

8.2 To reduce the likelihood of the company inadvertently accessing your personal data, or the personal data of third parties, you must comply with the following steps to separate company data from your personal data on the device:

(a) organise files within the device specifically into designated folders that clearly distinguish between company data and personal data (for example, marking your own folders as "PERSONAL");

(b) do not use work e-mail for personal purposes, but if you do ensure that it is labelled appropriately in the subject line;

(c) keep the amount of third party personal data (e.g. in relation to family and friends) stored on the device to a minimum;

(d) regularly backup all personal data stored on the device.

9. APPROPRIATE USE

9.1 You must be aware of our, our clients and your obligations under the relevant data protection legislation when processing company data. You must ensure that company data is used only for the business purposes for which it was intended, and that you do not use it for a purpose different from that for which it was originally intended. For example, you should not use contact information gathered for business purposes for your own personal purposes. You should also minimise the amount of company data you retain on the device by accessing information remotely where possible, and deleting any data saved locally on your device as soon as it is no longer required. Your obligations as a processor of personal data are explained in more detail in our Data protection policy.

9.2 You should never access or use our, or our clients', systems or company data through a device in a way that breaches any of our other policies. For example, you must not use a device to:

(a) breach our obligations with respect to the rules of relevant regulatory bodies;

(b) breach any obligations that relevant regulatory bodies may have relating to confidentiality and privacy;

(c) breach our Disciplinary Rules;

(d) defame or criticise us or our affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;

(e) breach our, or our clients', Anti-harassment and bullying policy;

(f) breach The Equality Act 2010;

(g) breach our, or our clients', Data Protection Policy;

(h) breach any other laws or ethical standards (for example, by breaching copyright or licensing restrictions by unlawfully downloading software on to a device).

9.3 If you breach any of the above policies you may be subject to disciplinary action up to and including dismissal.

9.4 You must not talk, text, e-mail or otherwise use a device while operating a company vehicle or while operating a personal vehicle for business purposes. You must comply with any applicable law concerning the use of devices in vehicles. For your own safety and the safety of others, we recommend you should not use your device while operating vehicles of any kind.

9.5 Before using your device under this policy for the first time you must erase all information and software related to any previous employment. You must confirm to us that this has been done if asked to do so.

10. TECHNICAL SUPPORT

We do not provide technical support for devices. If you use a device for business purposes you are responsible for any repairs, maintenance or replacement costs and services.

11. COSTS AND REIMBURSEMENTS

You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. You acknowledge that you alone are responsible for all costs associated with the device and that you understand that your business usage of the device may increase your voice and data usage charges.

OTHER POLICIES

SCHEDULE 22 – WHISTLEBLOWING POLICY

1. ABOUT THIS POLICY

1.1 We are committed to conducting our business with honesty and integrity, and we expect all employee to maintain high standards in accordance with our Code of Conduct. However, all organisations face the risk of things going wrong from time to time, or of unknowingly harbouring illegal or unethical conduct. A culture of openness and accountability is essential in order to prevent such situations occurring and to address them when they do occur.

1.2 The aims of this policy are:

(a) To encourage employee to report suspected wrongdoing as soon as possible, in the knowledge that their concerns will be taken seriously and investigated as appropriate, and that their confidentiality will be respected.

(b) To provide employee with guidance as to how to raise those concerns.

(c) To reassure employee that they should be able to raise genuine concerns without fear of reprisals, even if they turn out to be mistaken.

1.3 This policy covers all employee.

1.4 This policy takes account of the Whistleblowing Arrangements Code of Practice issued by the British Standards Institute and Protect.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. WHAT IS WHISTLEBLOWING?

2.1 Whistleblowing is the disclosure of information which relates to suspected wrongdoing or dangers at work. This may include:

(a) criminal activity;

(b) failure to comply with any legal or professional obligation or regulatory requirements;

(c) miscarriages of justice;

(d) danger to health and safety;

(e) damage to the environment;

(f) bribery under our Anti-corruption and Bribery Policy;

(g) facilitating tax evasion contrary to our Anti-facilitation of Tax Evasion Policy;

(h) financial fraud or mismanagement;

(i) breach of our internal policies and procedures including our Code of Conduct;

(j) conduct likely to damage our reputation or financial wellbeing;

(k) unauthorised disclosure of confidential information;

(l) negligence;

(n) the deliberate concealment of any of the above matters.

2.2 A whistleblower is a person who raises a genuine concern relating to any of the above. If you have any genuine concerns related to suspected wrongdoing or danger affecting any of our activities (a whistleblowing concern) you should report it under this policy.

2.3 This policy should not be used for complaints relating to your own personal circumstances, such as the way you have been treated at work. In those cases you should use the Grievance Procedure or Anti-harassment and Bullying Policy as appropriate.

2.4 If you are uncertain whether something is within the scope of this policy you should seek advice from the Whistleblowing Officer, whose contact details are at the end of this policy.

3. RAISING A WHISTLEBLOWING CONCERN

3.1 We hope that in many cases you will be able to raise any concerns with HR. You may tell them in person or put the matter in writing if you prefer. They may be able to agree a way of resolving your concern quickly and effectively. In some cases they may refer the matter to the Whistleblowing Officer.

3.2 However, where the matter is more serious, or you feel that HR has not addressed your concern, or you prefer not to raise it with them for any reason, you should contact one of the following:

(a) The Whistleblowing Officer.

(b) HR.

Contact details are set out at the end of this policy.

3.3 We will arrange a meeting with you as soon as possible to discuss your concern. You may bring a colleague to any meetings under this policy. Your companion must respect the confidentiality of your disclosure and any subsequent investigation.

3.4 We will take down a written summary of your concern and provide you with a copy after the meeting. We will also aim to give you an indication of how we propose to deal with the matter.

4. CONFIDENTIALITY

4.1 We hope that employee will feel able to voice whistleblowing concerns openly under this policy. However, if you want to raise your concern confidentially, we will make every effort to keep your identity secret. If it is necessary for anyone investigating your concern to know your identity, we will discuss this with you.

4.2 We do not encourage employee to make disclosures anonymously. Proper investigation may be more difficult or impossible if we cannot obtain further information from you. It is also more difficult to establish whether any allegations are credible. Whistleblowers who are concerned about possible reprisals if their identity is revealed should come forward to the Whistleblowing Officer or one of the other contact points listed at the end of this policy and appropriate measures can then be taken to preserve confidentiality.

5. INVESTIGATION AND OUTCOME

5.1 Once you have raised a concern, we will carry out an initial assessment to determine the scope of any investigation. We will inform you of the outcome of our assessment. You may be required to attend additional meetings in order to provide further information.

5.2 In some cases we may appoint an investigator or team of investigators including employee with relevant experience of investigations or specialist knowledge of the subject matter. The investigator(s) may make recommendations for change to enable us to minimise the risk of future wrongdoing.

5.3 We will aim to keep you informed of the progress of the investigation and its likely timescale. However, sometimes the need for confidentiality may prevent us giving you specific details of the investigation or any disciplinary action taken as a result. You should treat any information about the investigation as confidential.

5.4 If we conclude that a whistleblower has made false allegations maliciously or with a view to personal gain, the whistleblower will be subject to disciplinary action.

6. IF YOU ARE NOT SATISFIED

6.1 While we cannot always guarantee the outcome you are seeking, we will try to deal with your concern fairly and in an appropriate way. By using this policy you can help us to achieve this.

6.2 If you are not happy with the way in which your concern has been handled, or if you believe it has not been acted upon, you can raise it with one of the senior management team. Alternatively you may contact the board of Managing Partners.

7. EXTERNAL DISCLOSURES

7.1 The aim of this policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases you should not find it necessary to alert anyone externally.

7.2 Where a whistleblowing report relates to our client's employees, customers or our client as a whole, we are under an obligation to report such matters to our client.

7.3 The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. It will very rarely if ever be appropriate to alert the media. We strongly encourage you to seek advice before reporting a concern to anyone external. The independent whistleblowing charity, Protect, operates a confidential helpline. They also have a list of prescribed regulators for reporting certain types of concern. Their contact details are at the end of this policy.

7.4 Whistleblowing concerns usually relate to the conduct of our employee, but they may sometimes relate to the actions of a third party, such as a customer, supplier or service provider. In some circumstances the law will protect you if you raise the matter with the third party directly. However, we encourage you to report such concerns internally first. You should contact HR or one of the other individuals set out at the end of this policy for guidance.

8. PROTECTION AND SUPPORT FOR WHISTLEBLOWERS

8.1 It is understandable that whistleblowers are sometimes worried about possible repercussions. We aim to encourage openness and will support employee who raise genuine concerns under this policy, even if they turn out to be mistaken.

8.2 Whistleblowers must not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the

Whistleblowing Officer immediately. If the matter is not remedied you should raise it formally using our Grievance Procedure.

8.3 You must not threaten or retaliate against whistleblowers in any way. If you are involved in such conduct you may be subject to disciplinary action. In some cases the whistleblower could have a right to sue you personally for compensation in an employment tribunal.

8.4 You can be put in touch with a confidential support and counselling support, upon request..

9. INFORMATION AND TRAINING

9.1 Whistleblowing will be included in Employee induction, and subsequent appropriate training will be provided annually.

SCHEDULE 23 – ENVIRONMENTAL POLICY

1. ABOUT THIS POLICY

1.1 We recognise the importance of environmental protection and are committed to operating our business responsibly and promoting sustainable business activities. Our objective is to carry out all measures reasonably practicable to meet, exceed or develop all necessary or desirable requirements, to protect the environment and to continually improve the Environmental Management System to enhance environmental performance.

1.2 This policy covers all employee.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time. We will continue to review this policy to ensure it is achieving its aims.

1.4 This policy is designed to ensure complete compliance with ISO14001.

2. ENVIRONMENTAL COMMITTMENTS

To minimise environmental impacts concerning our activities and services, we shall commit to the following:

(a) Prevent pollution, reduce the production of waste, and minimise energy wastage and the consumption of resources.

(b) Promote the use of recyclable and renewable materials.

(c) The assessment and revision of all processes in order to reduce environmental impact, with particular focus on paper elimination.

(d) Regularly re-assess the environmental effects of CWC's activities.

(e) Include the consideration of environmental issues in all business strategies and initiatives.

(f) Educate, train and motivate employees to carry out tasks in an environmentally responsible manner and ensure that a continuous professional development strategy remains core to our business goals.

(g) Investigate the feasibility of influencing our clients and third parties with consideration to environmental aspects of their activities.

(h) Comply with applicable legal requirements, and other requirements (including ISP 14001) to which CWC subscribes, which relate to its environmental aspect.

3. RESPONSIBILITY FOR ENVIRONMENTAL MATTERS

The Managing Partners of CWC demonstrate leadership and commitment to ensure that protection of the environment is firmly embedded in the company's culture, by:

(a) Taking accountability for the effectiveness of the Environmental Management System.

(b) Ensuring that this Environmental Policy is compatible with the strategic direction and the context of the organisation.

(c) Ensuring the integration of the Environmental Management System requirements into the organisation's business processes.

(d) Ensuring that the resources needed for the Environmental Management System are available.

(e) Communicating the importance of effective environmental management and of conforming to the Environmental Management System requirements.

(f) Ensuring that the Environmental Management System achieves its intended outcomes.

(g) Directing and supporting persons to contribute to the effectiveness of the Environmental Management System.

(h) Promoting continual improvement.

(i) Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

4. YOUR RESPONSIBILITIES

All employee share responsibility for protecting the environment. You should adhere to the following when carrying out your responsibilities:

(a) Reduce the use of energy and office supplies. In particular, minimise the use of paper in office activities.

(b) Dispose of waste responsibly. Recycle (recycling bins are provided in the office for this purpose) and reuse materials wherever practical.

(c) Reduce energy waste by ensuring heaters/lights are turned off when leaving the office.

(d) Consider carsharing where practicable.

(e) Be considerate of how your activities impact the environment; and

(f) Raise any concerns you may have regarding environmental issues to HR.

5. INFORMATION AND TRAINING

5.1 We will inform and update employee regarding environmental issues.

5.2 Environmental matters will be included in Employee's induction, and subsequent appropriate training will be provided ad hoc.

6. POLICY REVIEW

This policy will be reviewed on an annual basis.