GDPR Policy Handbook

Cantel Computer Services Ltd

Cantel Computer Services Ltd,

Brunel Drive, Northern Road Industrial Estate,
Newark, Nottinghamshire, NG24 2EG

Registration: 01940170

DATA PROTECTION PRIVACY NOTICE (RECRUITMENT)

This notice explains what personal data (information) we will hold about you, how we collect it, and how we will use and may share information about you during the application process. We are required to notify you of this information, under data protection legislation. Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

Who collects the information

CANTEL COMPUTER SERVCIES LTD ('Company') is a 'data controller' and gathers and uses certain information about you.

Data protection principles

We will comply with the data protection principles when gathering and using personal information, as set out in our *data protection (employment) policy*.

About the information we collect and hold

The table below summarises the information we collect and hold up to and including the shortlisting stage of the recruitment process, how and why we do so, how we use it and with whom it may be shared.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any changes to information we collect or to the purposes for which we collect and process it.

Where information may be held

Information may be held at our offices.

How long we keep your information

We keep the personal information that we obtain about you during the recruitment process for no longer than is necessary for the purposes for which it is processed. How long we keep your information will depend on whether your application is successful and you become employed by us, the nature of the information concerned and the purposes for which it is processed.

We will keep recruitment information (including interview notes) for no longer than is reasonable, taking into account the limitation periods for potential claims such as race or sex discrimination (as extended to take account of early conciliation), after which they will be destroyed. If there is a clear business reason for keeping recruitment records for longer than the recruitment period, we may do so but will first consider whether the records can be pseudonymised, and the longer period for which they will be kept.

If your application is successful, we will keep only the recruitment information that is necessary in relation to your employment. For further information, see our data protection privacy notice (employment).

Further details on our approach to information retention and destruction are available in our Records Retention Schedule.

Your right to object to us processing your information

Where our processing of your information is based solely on our legitimate interests (or those of a third party), you have the right to object to that processing if you give us specific reasons why you are objecting, which are based on your particular situation. If you object, we can no longer process your information unless we can demonstrate legitimate grounds for the processing, which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

Please contact **Richard Cusworth,** Data Protection Officer (DPO), who can be contacted if you wish to object in this way.

Your rights to correct and access your information and to ask for it to be erased

Please contact our Data Protection Officer (DPO), if in accordance with applicable law you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask our Data Protection Officer for some but not all of the information we hold and process to be erased (the 'right to be forgotten') in certain circumstances. Our Data Protection Officer will provide you with further information about the right to be forgotten, if you ask for it.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain

We hope that our Data Protection Officer can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at https://ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

ABOUT THE INFORMATION WE COLLECT AND HOLD

Up to and including the shortlisting stage

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
Your name and contact details (ie address, home and mobile phone numbers, email address)	From you	Legitimate interest: to carry out a fair recruitment process Legitimate interest: to progress your application, arrange interviews and inform you of the outcome at all stages	To enable the DPO or the manager to contact you to progress your application, arrange interviews and inform you of the outcome To inform the relevant manager or department of your application
Details of your qualifications, experience, employment history (including job titles, salary and working hours) and interests	From you, in the completed application form and interview notes (if relevant)	Legitimate interest: to carry out a fair recruitment process Legitimate interest: to make an informed decision to shortlist for interview and (if relevant) to recruit	To make an informed recruitment decision
Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs	From you, in a completed anonymised equal opportunities monitoring form	To comply with our legal obligations and for reasons of substantial public interest (equality of opportunity or treatment)	To comply with our equal opportunities monitoring obligations and to follow our equality and other policies For further information, see * below
Information regarding your criminal record	From you, in your completed application form	To comply with our legal obligations	To make an informed recruitment decision

		For reasons of substantial public interest.	To carry out statutory checks Information shared with DBS, GOC and other regulatory authorities as required For further information, see * below
Details of your referees	From your completed application form	Legitimate interest: to carry out a fair recruitment process In the regulated sector, to comply with our legal obligations to obtain regulatory references	To carry out a fair recruitment process To comply with legal/regulatory obligations Information shared with relevant managers, HR personnel and the referee

Before making a final decision to recruit

The information we collect	**How we collect the information**	**Why we collect the information**	**How we use and may share the information**
Information about your previous academic and/or employment history, including details of any conduct, grievance or performance issues, appraisals, time and attendance, from references obtained about you from previous employers and/or education providers ☐	From your referees (details of whom you will have provided)	Legitimate interest: to make an informed decision to recruit To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance	To obtain the relevant reference about you To comply with legal/regulatory obligations Information shared with relevant managers and HR personnel

		obligations and good employment practice	
Information regarding your academic and professional qualifications ☐	From you, from your education provider from the relevant professional body	Legitimate interest: to verify the qualifications information provided by you	To make an informed recruitment decision
Information regarding your criminal record, in criminal records certificates (CRCs) and enhanced criminal records certificates (ECRCs) ☐	From you and from the Disclosure and Barring Service (DBS) and the General Optical Council	To perform the employment contract; To comply with our legal obligations Legitimate interest: to verify the criminal records information provided by you	To make an informed recruitment decision To carry out statutory checks Information shared with DBS and other regulatory authorities as required For further information, see * below
Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information ☐	From you and, where necessary, the Home Office	To enter into/perform the employment contract To comply with our legal obligations Legitimate interest: to maintain employment records To carry out obligations and exercise rights in employment law	To carry out right to work checks Information may be shared with the Home Office

You are required (by law or in order to enter into your contract of employment) to provide the categories of information marked '☐' above to us to enable us to verify your right to work and suitability for the position.

***** Further details on how we handle sensitive personal information and information relating to criminal convictions and offences are set out in our Criminal Records Information Policy available in GDPR Policy Handbook.

DATA PROTECTION PRIVACY NOTICE (EMPLOYMENT)

This notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during your employment and after it ends. We are required to notify you of this information under data protection legislation. Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

Who collects the information

Cantel Computer Services Ltd ('Company') is a 'data controller' and gathers and uses certain information about you.

Data protection principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection (employment) policy.

About the information we collect and hold

The table set out in the schedule summarises the information we collect and hold, how and why we do so, how we use it and with whom it may be shared.

We may also need to share some of the categories of personal information set out in the schedule with other parties, such as external contractors and our professional advisers and potential purchasers of some or all of our business or on a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any changes to information we collect or to the purposes for which we collect and process it.

Where information may be held

Information may be held at our offices.

How long we keep your information

We keep your information during and after your employment for no longer than is necessary for the purposes for which the personal information is processed. Further details on this are available in our Record Retention Schedule.

Your right to object to us processing your information

Where our processing of your information is based solely on our legitimate interests (or those of a third party), you have the right to object to that processing if you give us specific reasons why you are

objecting, which are based on your particular situation. If you object, we can no longer process your information unless we can demonstrate legitimate grounds for the processing, which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

Please contact **Richard Cusworth,** Data Protection Officer (DPO) if you wish to object in this way.

Your rights to correct and access your information and to ask for it to be erased

Please contact our Data Protection Officer (DPO), who can be contacted (in accordance with applicable law) you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask our Data Protection Officer for some but not all of the information we hold and process to be erased (the 'right to be forgotten') in certain circumstances. Our Data Protection Officer will provide you with further information about the right to be forgotten, if you ask for it.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain

We hope that our Data Protection Officer can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

THE SCHEDULE
ABOUT THE INFORMATION WE COLLECT AND HOLD

The information we collect	**How we collect the information**	**Why we collect the information**	**How we use and may share the information**
Your name, contact details (ie address, home and mobile phone numbers, email address) and emergency contacts (ie name, relationship and home and mobile phone numbers) ☐	From you	To enter into/perform the employment contract Legitimate interest: to maintain employment records and good employment practice	To enter into/perform the employment contract
Details of salary and benefits, bank/building society, National Insurance and tax information, your age ☐	From you	To perform the employment contract including payment of salary and benefits Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	To ensure you receive the correct pay and benefits Information shared with our payroll administrators and with HM Revenue & Customs (HMRC)
Details of your spouse/partner and any dependants ☐	From you	To perform the employment contract including employment-related benefits, eg private medical	To ensure you receive the correct pay and benefits

		insurance, life assurance, pension and emergency contact details	Information shared with our payroll administrators and with HM Revenue & Customs (HMRC)
Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information ☐	From you and, where necessary, the Home Office	To enter into/perform the employment contract To comply with our legal obligations Legitimate interest: to maintain employment records	To carry out right to work checks Information may be shared with the Home Office
Details of your pension arrangements, and all information included in these and necessary to implement and administer them ☐	From you, from our pension administrators and (where necessary) from your own pension fund administrators	To perform the employment contract including employment-related benefits To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	To administer your pension benefits AND/OR To comply with our auto-enrolment pension obligations Information shared with our pension administrators and with HMRC

Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health) ☐	From you, from your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators	To perform the employment contract including employment-related benefits To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	To maintain employment records, to administer sick pay entitlement, to follow our policies and to facilitate employment-related health and sickness benefits To comply with our legal obligations to you as your employer Information shared with your doctors, with medical and occupational health professionals we engage and with our insurance benefit administrators and out-sourced HR Consultant For further information, see * below
Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs	From you	To comply with our legal obligations and for reasons of substantial public interest (equality of	To comply with our equal opportunities monitoring obligations and

		opportunity or treatment)	to follow our policies For further information, see * below
Criminal records information, including the results of Disclosure and Barring Service (DBS) checks ☐	From you and the DBS	To perform the employment contract To comply with our legal obligations	To carry out statutory checks Information shared with GOC, DBS and other regulatory authorities as required For further information, see * below
Information on grievances raised by or involving you	From you, from other employees and from consultants we may engage in relation to the grievance procedure	To perform the employment contract To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	For staff administration, to follow our policies and to deal with grievance matters Information shared with relevant managers, HR personnel, HR consultant and with other consultants we may engage
Information on conduct issues involving you	From you, from other employees and from consultants we may	To comply with our legal obligations	For staff administration and assessments, to

	engage in relation to the conduct procedure	Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	follow our policies, to monitor staff performance and conduct and to deal with disciplinary and grievance matters Information shared with relevant managers, HR personnel, HR consultant and with other consultants we may engage.
Details of your appraisals and performance reviews	From you, from other employees and from consultants we may engage in relation to the appraisal/performance review process	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	For staff administration and assessments, to follow our policies, to monitor staff performance and conduct and to deal with disciplinary and grievance matters Information shared with relevant managers, HR personnel, HR consultant and with other consultants we may engage.

Details of your performance management/improvement plans (if any)	From you, from other employees and from consultants we may engage in relation to the performance review process.	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	For staff administration and assessments, to follow our policies and to monitor staff performance Information shared with relevant managers, HR personnel, HR consultant and with other consultants we may engage.
Details of your time and attendance records	From you and from our company software records or application logs.	To perform the employment contract Legitimate interest: to monitor and manage staff access to our systems and facilities and to record staff absences	For payroll and staff administration and assessments, to follow our policies and to monitor staff performance and attendance Information shared with relevant managers, HR personnel, HR consultant and with other consultants we may engage and with our payroll administrators.
Information in applications you make for other	From you	To enter into/perform the	To process the application

positions within our organisation		employment contract To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	Information shared with relevant managers, HR personnel and with other consultants we may engage
Information about your use of our IT, communication and other systems	Automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, remote access systems, email and instant messaging systems, intranet and Internet facilities, telephones, voicemail, mobile phone records any other relevant systems such as data loss prevention tools, next-generation firewalls, unified threat management systems, transport layer security, eDiscovery technology, mobile device management systems	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage to ensure our business policies, such as those concerning security and internet use, are adhered to	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel and with other consultants we may engage For further information, see ** below

		for operational reasons, such as maintaining employment records, recording transactions, training and quality control to ensure that employees comply with the company's policies and procedures which is not limited to disciplinary/ grievance but all the company's policies to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with for security vetting, spot checks and investigating complaints and allegations of criminal offences	

		to prevent unauthorised access and modifications to our systems as part of investigations by regulatory bodies, or in connection with legal *proceedings or requests	
Your image, in photographic and video form	From you	Legitimate interests: to monitor and manage staff access to our premises, systems and facilities for marketing and business development purposes	To protect and carry out our legitimate interests (see adjacent column) Information shared with HR, IT and security personnel Information shared with marketing and business development personnel and with other consultants we may engage
Details of your use of business-related social media, such as LinkedIn	From relevant websites and applications	Legitimate interests: to monitor and manage staff access to our systems and facilities	To protect and carry out our legitimate interests (see adjacent column) Information shared with

		to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage to ensure our business policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions, training and quality control to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with	relevant managers, HR personnel and with other consultants we may engage For further information, see ** below

		for security vetting and investigating complaints and allegations of criminal offences as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	
Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur)	From relevant websites and applications	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage to ensure our business policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions,	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel and with other consultants we may engage For further information, see ** below

		training and quality control to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with for security vetting and investigating complaints and allegations of criminal offences as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	
Details in references about you that we give to others	From your personnel records, our other employees	To perform the employment contract To comply with our legal obligations Legitimate interests: to maintain	To provide you with the relevant reference To comply with legal/regulatory obligations Information shared with

		employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	relevant managers, HR personnel and the recipient(s) of the reference

You are required (by law or under the terms of your contract of employment, or in order to enter into your contract of employment) to provide the categories of information marked '☐' above to us to enable us to verify your right to work and suitability for the position, to pay you, to provide you with your contractual benefits, such as for example, contractual sick pay and to administer statutory payments such as statutory sick pay (SSP). If you do not provide this information, we may not be able to employ you, to make these payments or provide these benefits.

***** Further details on how we handle sensitive personal information and information relating to criminal convictions and offences are set out in this handbook.

****** Further information on the monitoring we undertake in the workplace and how we do this is available in this handbook, the employee handbook and the CCTV policy.

BRING YOUR OWN DEVICE

Purpose and scope

1.1 This bring your own device (**BYOD**) policy supplements the company's other policies and procedures, which together place obligations on staff to take appropriate measures to safeguard company information against unauthorised or unlawful use, accidental loss, destruction or damage, by extending and/or clarifying these obligations in relation to staff use of their own personal devices at work.

1.2 References in this policy to the **company** means CANTEL COMPUTER SERVCIES LTD. References to **you** or **your** means any person subject to this policy as identified below.

1.3 The main purpose of this policy is to protect the company's confidential and commercially sensitive information and to ensure the company can comply with our legal and regulatory obligations, including those regarding data protection, record retention and audit by setting out the circumstances in which the company may monitor your use of its systems; access, retrieve, remove and destroy data on your device; and the action the company may take if you fail to comply with the obligations contained within this policy. The company knows and expects that you will also use your device for personal use and, unless you are doing something that is against this policy or its spirit, unlawful or that could otherwise adversely impact on the company or another person, the company are not concerned about how you use your device in your own time.

1.4 Except where indicated, this policy does not form part of any employee's contract of employment and the company expressly reserves the right to amend or remove it at any time.

1.5 This policy applies to:

1.5.1 all company employees and to others such as agents, subcontractors, consultants, interns, casual workers, agency workers or other company representatives who will be subject to this policy (together **staff**);

1.5.2 all written, spoken and electronic information held, used or transmitted by or on behalf of the company, in whatever media. This includes information and data held on computer systems, hand-held devices, tablets or other portable or electronic devices and telephones and to paper records, and information transmitted orally. This information may, for example, relate both to the company's own business or that of our affiliates or customers, suppliers and other third parties with whom we engage or do business (together **company information**); and

1.5.3 all electronic devices, including laptops, tablets, personal digital assistants and other hand-held or portable devices, smartphones, and any other applications or technology that are used by you to access, store, create, copy or transmit company information and that are not owned or supplied by us or on our behalf (together this is **your device**).

1.6 This policy supplements our other policies and procedures from time to time, including without limitation the following policies: Data security policy, Data Protection Policy, Records Retention Policy, Use of Electronic Communications Policy, Electronic Communications Monitoring Policy.

2 Obligations regarding information security

2.1 It is in the interests of the company and its staff for staff to be able to do their work flexibly and effectively, and the company recognises that this may extend to you using a personal electronic or communications device for work purposes. In permitting you to use such a device for work purposes, the company requires you to exercise all necessary care, take certain precautions and be responsible when using your device to connect to the company's IT systems and/or to access company information.

2.2 In order to protect company information, you are required to comply with the obligations set out below at all times, both during or outside of office hours and whether or not you are at your normal place of work.

2.3 If you do not comply with this policy, the company may revoke its permission for you to use your device for work purposes and may take other appropriate action (see paragraph 19 (Failure to comply with this policy) below).

2.4 If you have any questions about this policy, please contact Richard Cusworth at Unit 12 Pavilion Business Park, Royds Hall Road, Leeds LS12 6AJ, telephone number: 0044 (0) 7545 128107

3 Company information

3.1 All company information should be considered to be commercially valuable and you must protect it from loss, theft, misuse, inappropriate access, modification or disclosure. You should exercise an even higher degree of caution when accessing or working with sensitive information, in respect of which the impact of loss or unauthorised access may be even more serious than would ordinarily be the case. Your attention is drawn to the definition of 'Confidential Information' in your contract of employment.

3.2 Your obligations concerning data security generally (including regarding technical security measures and organisational security measures) are detailed in this handbook. If in doubt about your obligations, contact the DPO for advice.

4 Approved devices and registering your device

4.1 The company will only consider permitting you to use your device in accordance with this policy if it is listed as supported below in paragraph 4.2. This list will be maintained and updated from time to time.

4.2 The following devices are supported:

4.2.1 iPhone;

4.2.2 iPad;

4.2.3 Blackberry;

4.2.4 Android;

4.2.5 Windows;

4.2.6 Other.

4.3 Before using your device at work to connect to the company's IT systems and/or to access company information in accordance with this policy, you must:

4.3.1 register your device with the company; and

4.3.2 present your device to the company for approval, provisioning and configuration (if required); and

4.4 You are not permitted to use any device other than a device which has been registered and approved by the company to connect to the company's IT systems and/or to access company information. The company reserves the right to refuse or remove approval for your device to connect to its IT systems and/or access company information where it is of the reasonable opinion that the device is or may be capable of being used in a way that may breach this policy.

5 Acceptable use

5.1 The company defines acceptable business use as activities that directly or indirectly support the business of the company.

5.2 Staff are blocked from accessing certain websites that the company considers inappropriate while connected to the company's IT network.

5.3 The camera and/or video capabilities of your device must not be used while on-site.

5.4 Your device may not be used at any time to:

5.4.1 engage in any activity that constitutes a breach of any of the company's policies (such as the company's internet, email and communications policy or social media policy;

5.4.2 store or transmit illicit materials;

5.4.3 store or transmit proprietary information;

5.4.4 harass, bully or unlawfully discriminate against others;

5.4.5 defame or criticise the company or its affiliates, customers, clients, suppliers, vendors and other stakeholders;

5.4.6 engage in outside business activities

5.4.7 breach any other laws or ethical standards; or

5.5 You may use your device to access the following company IT systems:

5.5.1 the company email system;

5.5.2 the customer relationship management (**CRM**) system;

5.5.3 the enterprise resource planning (**ERP**) system;

5.5.4 calendars;

5.5.5 contacts;

5.5.6 documents;

5.5.7 any other relevant systems.

5.6 The company has a zero-tolerance policy towards texting or emailing using your device while operating a company or personal vehicle. You must comply with any applicable law concerning the use of such devices in vehicles. In the UK, only hands-free talking is permitted while driving.

6 Security

6.1 In order to prevent unauthorised access, your device must be password or PIN protected using the features of the device. A strong password is required to access the company's IT network.

6.2 The device must lock itself with a password or PIN if idle for five minutes.

6.3 You must comply with the attached BYOD security protocols (**security protocols**), which form part of this policy, and take all other reasonable efforts to secure your 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, the use of encryption and an enforced prohibition on the use of your device by anyone other than you.

6.4 Staff are automatically prevented from downloading, installing and using any app that does not appear on the company's list of permitted apps (see paragraph 5 (Acceptable use) above).

6.5 Smartphones and tablets belonging to staff that are for personal use only are not allowed to connect to the company's IT network.

6.6 Staff access to company information is limited based on user profiles defined by the IT department and automatically enforced.

6.7 Data on your device may be remotely erased by the company in accordance with paragraph 11.3 below if:

6.7.1 there is a data breach or potential data breach involving company information relevant to your device;

6.7.2 your device is lost or stolen;

6.7.3 your password is lost or stolen;

6.7.4 you are suspended from work or placed on garden leave in accordance with your contract of employment;

6.7.5 you cease working for the company and/ or you have not complied with your relevant obligations under paragraph 18 (Staff departure) below

6.7.6 the IT department detects a virus, malware or other destructive program or code relevant to your device;

7 Company responsibilities

7.1 As a data controller, the company is responsible for ensuring that all processing of personal data which is under its control remains compliant with the Data Protection Act 1998.

7.2 The company is however mindful of the personal usage of approved devices and the privacy of staff. Technical and organisational measures taken by the company in relation to this policy will remain proportionate to the risks involved. The company will use reasonable endeavours not to access, use, copy or delete personal data (which is not also company information) held on your device unless it is absolutely necessary for legitimate business purposes.

8 Device detection and tracking

8.1 The company may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to the company's IT network. Such technology may, without limitation, monitor, intercept, access, inspect, erase, review, retrieve and report on the materials, data, communications and information that has been copied onto or accessed by such devices, including your device. In using your device on the company's IT network you agree to such detection and monitoring.

8.2 The company's use of such technology is only for the legitimate business purpose of ensuring the security of our IT systems and tracking our company information, not to monitor your personal use of your device or carry out general surveillance. It is, however, possible that your personal data may be inadvertently monitored, intercepted, reviewed or erased and you should therefore have a limited expectation of privacy in relation to any data on your device. Any monitoring the company undertakes will be carried out in accordance with the company's notice of monitoring IT communications systems and local legal requirements (as applicable).

9 Accessing and using company information

9.1 You are permitted to connect to or access only the following company IT systems from your device:

9.1.1 the company email system;

9.1.2 the CRM system;

9.1.3 the ERP system;

9.1.4 calendars;

9.1.5 contacts;

9.1.6 documents;

9.2 You must only use company information:

9.2.1 if you are an employee: for acceptable business uses;

9.2.2 if you are a supplier, subcontractor or consultant: to provide services to us; or

9.2.3 if you are a customer: to receive services from us; and

not for any other purpose.

9.3 You must only use company information:

9.3.1 in accordance with the security protocols; and

9.3.2 in accordance with the attached BYOD separation protocols, which form part of this policy (**separation protocols**).

9.4 Company information remains our property at all times, no matter what format it is in, where it is stored or how it is accessed.

9.5 In using your device for work purposes, you agree to give us access to any company information on your device immediately on our reasonable request. In this context, 'access' includes us being permitted to access, make copies of, recover or delete files (including all copies of files) containing company information from your device.

10 Regulatory reasons and audit

10.1 From time to time the company may need to access and/or audit your device (and the information and applications on it), in order pursue the following legitimate business purposes, (together the **regulatory reasons**):

10.1.1 to verify your compliance with this and other company policies;

10.1.2 to ensure that the company complies with its obligations to its regulators, the courts and other relevant official bodies (**regulators**);

10.1.3 to demonstrate to regulators that the company has been complying with its legal and regulatory obligations; and

10.1.4 to cooperate with any investigations, proceedings or other requests for information by the regulators.

10.2 In using your device as envisaged by the provisions of this policy, you authorise the company (or its authorised agents or representatives, such as auditors or regulators) to access and/or audit your device for regulatory reasons, as the company reasonably require from time to time. You agree to co-operate with and facilitate any such access and/or audit.

10.3 The company appreciates that your device will contain both company information and your personal information.

10.4 If you comply with the separation protocols and the security protocols, any intrusiveness or inconvenience to you of the company accessing and/or auditing your device is likely to be minimised.

11 Remote access by company

11.1 The rights set out in this section only apply where:

11.1.1 company information is locally stored on (rather than just accessed from) your device (whether such local copies are made automatically or by you); and

11.1.2 the company notifies you of the possibility of remote access by the company at the time when you register your device or later gives you written notice.

11.2 If you do not promptly give us access to company information in accordance with paragraph 9 (Accessing and using company information) and/or paragraph 10 (Regulatory reasons and audit) above, or unreasonably delay doing so, the company may use technology to remotely access your device to enable the company to access company information, subject to local legal requirements (as applicable). You authorise the company to do this, provided that in so doing it complies with paragraph 12 (Restrictions on company rights of access) below.

11.3 If the company considers it reasonably necessary to do so, the company may, subject to local legal requirements (as applicable), use technology to remotely access and delete data or company information in the dedicated company areas on your device (as separated in accordance with the separation protocols) stored on your device, if any of the following situations occur, (each a **company information risk**):

11.3.1 there is a data breach or potential data breach involving company information relevant to your device;

11.3.2 your device is lost or stolen;

11.3.3 your password is lost or stolen;

11.3.4 you are suspended from work or placed on garden leave in accordance with your contract of employment;

11.3.5 you cease working for the company and you have not complied with your relevant obligations under paragraph 18 (Staff departure) below;

11.3.6 the IT department detects a virus, malware or other destructive program or code relevant to your device;

11.4 If you comply with the separation protocols and the security protocols, any intrusiveness or inconvenience to you arising from the company accessing and/or deleting personal data from your device is likely to be minimised

11.5 The company may use technology that enables it to remotely backup company information on your device. If you comply with the separation protocols this should only require us to access the company information in the dedicated company areas on your device for this purpose. However, if the company detects or reasonably suspects company information is being stored in other areas in your device, the company may also remotely access those other areas for this purpose

12 Restrictions on company rights of access

When taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, the company will, where practicable:

12.1 weigh up whether such action is proportionate in light of the potential damage to the company, its customers or other affected persons as a result of the company information risk, regulatory reasons or other relevant reasons;

12.2 consider if the company information risk, regulatory reasons or other relevant reasons could reasonably and effectively be dealt with in some other way (but appreciating company information risks and regulatory reasons in particular often require quick, decisive and urgent action); and

12.3 take reasonable steps to minimise loss of your personal data on your device, but the company shall not be responsible for any such loss that may occur.

13 Services the company provides

The company reserve the right to (temporarily or permanently) disconnect, disable, restrict use of or modify at any time any services that it provides and that you access via your device at any time, for any reason and without prior notice.

14 Your responsibilities concerning your device

14.1 You are at all times solely responsible for:

14.1.1 purchasing your device paying all device and carrier service costs, bills and tariffs for your device, including but not limited to voice and data usage charges;

14.1.2 repairs to and maintenance of your device and the associated costs, including costs required to replace your device;

14.1.3 running backups of your own data on your device at least weekly;

14.1.4 ensuring periodic system/security upgrades are installed without delay when notified of their availability; and

14.2 You agree that you use your device at your own risk and that the company will not be responsible for any losses, damages or liability arising out of its use (to the extent permitted under applicable law).

15 Risks you accept

15.1 You acknowledge that there are specific risks associated with you using your device for work purposes in accordance with this policy. These risks include the threat of viruses, malware and other software and/or hardware failures or programming, operating system or other errors that may result in loss of data (yours and/or company information) or your device not working properly or at all.

15.2 However, in consideration of you being allowed to use your device for work purposes in accordance with this policy, as the user of your device, you agree to accept and assume full liability for these risks (except for any liability that we cannot by law exclude or limit).

16 Theft or loss of device

16.1 If your device is lost or stolen, you must inform the company by no later than the next working day.

16.2 The quicker you inform the company of this and cooperate by providing such information and assistance as the company request, the more effectively the company will able to assess and contain any potential data security breach risk and any other relevant risks. This will in turn impact the level of our response and the action the company needs to take.

17 Data security breach

17.1 If you become aware of a breach of security or believe that your device may have been accessed by an unauthorised person or otherwise compromised, you must inform the company as soon as possible and in any event by no later than close of business on the relevant day.

17.2 The quicker you inform the company of this and cooperate by providing such information and assistance as the company requests, the more effectively the company will able to assess and contain any potential data security breach risk and any other relevant risks. This will in turn impact the level of our response and the action we need to take.

18 Staff departure

18.1 On your exit from the company (regardless of the reason for your exit) and prior to commencing any period of garden leave:

18.1.1 your access to the company IT system, its applications and all company information will cease;

18.2 You are reminded that your obligations to keep company information confidential continue even after you cease working for the company.

18.3 Upon ceasing working for the company, as well as complying with all HR exit procedures, if the company request, you will sign a written declaration confirming your device contains no company information and/or allow us to inspect your device to confirm your device contains no company information. You will provide all necessary co-operation and assistance to the company in relation to this process.

19 Failure to comply with this policy

19.1 Failure to comply with this policy may result in disciplinary action including, where appropriate, revocation of access to company IT systems, suspension, dismissal and criminal prosecution in accordance with local laws. Disciplinary action may be taken whether the breach (or suspected breach) is committed during or outside of office hours and whether or not use of the device takes place at your normal place of work. As well as any specific rights the company has in this policy that apply where you breach particular provisions of this policy, your breach of your obligations under this policy will constitute a breach of your contract with the company and the company may exercise its rights under that contract. You will be required to co-operate with any investigation into suspected breaches of this policy, which may require you to provide the company with full access to your device and any relevant passwords and login details.

19.2 If you have reasonable grounds to suspect that someone else is in breach of this policy, you must inform the company immediately and in accordance with the company's Whistleblowing policy.

1 CRIMINAL RECORDS INFORMATION POLICY - INTRODUCTION

1.1 This policy supplements the Company's data protection policy (employment).

1.2 This document sets out the Company's policy on asking questions about a prospective (or existing) employee's criminal record, and carrying out Disclosure and Barring Service (DBS) checks.

1.3 This policy sets out our commitment to comply with the DBS Code of Practice and our data protection obligations, to treat prospective employees fairly and not to discriminate unfairly against any subject of a criminal record check on the basis of a conviction or other information revealed. Its purpose is to set out how we comply with our data protection obligations in respect of criminal records information and seek to protect such information, and to ensure that staff understand and comply with the rules governing the collection, use and deletion of criminal records information to which they may have access in the course of their work.

1.4 We are committed to complying with our data protection obligations and the DBS Code of Practice in relation to criminal records information, in particular:

1.4.1 in relation to the circumstances in which we seek criminal records information;

1.4.2 by being concise, clear and transparent about how we obtain and use such information, and how (and when) we delete it once it is no longer required; and

1.4.3 by ensuring the correct handling, use, storage, retention and disposal of DBS certificates and certificate information.

1.5 The Company's data protection officer, is responsible for informing and advising the Company and its staff on its data protection obligations, including in relation to criminal records information, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer.

2 Policy statement

2.1 Having a criminal record will not necessarily bar you from working with us. We will take into account the circumstances and background of any offences and whether they are relevant to the position in question, balancing the rights and interests of the individual, our employees, customers/clients, suppliers and the public.

2.2 We will treat all applicants, employees and volunteers fairly but reserve the right to withdraw an offer of employment if you do not disclose relevant information, or if a DBS check reveals information which we reasonably believe would make you unsuitable for the role.

3 Scope and definitions

3.1 This policy applies to criminal records information relating to job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

3.2 Staff should refer to the Company's data protection policy (employment) and, where appropriate, to its other relevant policies.

3.3 This policy has been drafted with the assistance of a representative group of employees to ensure that it is clear and easy to understand. We will review and update this policy *regularly* in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

3.4 The definitions set out in the Company's data protection policy (employment) apply to terms used in this policy.

4 Asking for criminal records information

4.1 Before recruiting for any post the HR department will, with advice from the data protection officer, assess whether it is justified in seeking criminal records information for that particular post (see paragraph 4.3 below) and, if so:

4.1.1 whether it is appropriate to limit the information sought to offences that have a direct bearing on suitability for the job in question; and

4.1.2 whether the information should be verified with the DBS.

4.2 If an assessment under paragraph 4.1 has been carried out for the same or a similar post within the last *12* months, the HR department may rely on that assessment.

4.3 The Company will be justified in obtaining criminal records information for a particular post if it is necessary:

4.3.1 for the performance of the employment contract for that post;

4.3.2 in order for the Company to comply with a legal obligation to which it is subject;

4.3.3 in order to protect the vital interests of *vulnerable service users*; and

4.3.4 for the purposes of the Company's legitimate interests.

4.4 The level of criminal records information and DBS check that the Company is entitled to request (ie a criminal records certificate (CRC) or enhanced criminal records certificate (ECRC)) will depend on the post for which the prospective employee's suitability is being assessed. Further details are set out in Appendix 1.

4.5 We will only ask an individual to provide criminal records information in relation to convictions and cautions that the Company would be legally entitled to see in a DBS check for the relevant post (see paragraph 4.4 above), i.e.:

4.5.1 if the Company is justified in seeking criminal records information for the post, and the post is not exempt from the Rehabilitation of Offenders Act 1974, we will ask applicants to complete the criminal records information form, please ask your manager, which states that applicants are not required to disclose convictions that are spent under the Rehabilitation of Offenders Act 1974; and

4.5.2 if the Company is justified in seeking criminal records information for the post, and the post is exempt from the Rehabilitation of Offenders Act 1974, we will ask applicants to complete the criminal records information form, please ask your manager, which asks applicants if they have any convictions, cautions, reprimands or final warnings which are not filtered (or 'protected' as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended)). For further information on filtering, see Appendix 1.

4.6 If the information sought can be limited to offences that have a direct bearing on suitability for the job in question, the HR department will amend the criminal records information form accordingly.

4.7 Where a DBS check is identified as necessary, all application forms, job adverts and recruitment briefs will contain a statement that an application for a DBS certificate will be submitted in the event of the individual being offered the position.

4.8 Applicants will only be asked to complete a criminal records information form before an offer of employment is made unconditional; they will not be asked to do so during the earlier short-listing, interview or decision-making stages.

4.9 Before an individual is asked to complete a criminal records information form, they will be provided with a copy of this policy.

4.10 If the Company is not justified in seeking criminal records information for the post, it will not ask an applicant for criminal records information.

4.11 If it is assessed that the Company should use the DBS to verify criminal records information, the Company will:

4.11.1 provide the individual concerned with a copy of the Company's data handling policy (set out in Appendix 2) before asking them to complete a DBS application form or asking for their consent to use their information to access the DBS update service;

4.11.2 make every subject of a DBS check aware of the existence of the DBS Code of Practice and makes a copy available on request. A copy is available here; and

4.11.3 comply with the DBS Code of Practice.

4.12 The Company will not rely on a previously-issued DBS certificate.

4.13 Once criminal records information has been verified through a DBS check, the Company will:

4.13.1 if inconsistencies emerge between the information provided by the individual and the information in the DBS certificate, give the applicant the opportunity to provide an explanation in accordance with paragraph 5;

4.13.2 record that a DBS check was completed and whether it yielded a satisfactory or unsatisfactory result; and

4.13.3 delete the DBS certificate and any record of the information contained in it unless, in exceptional circumstances, the data protection officer assesses that it is clearly relevant to the ongoing employment relationship*, to allow for consideration and resolution of any disputes or complaints*.

4.14 If, in accordance with paragraph 4.13.3, the data protection officer assesses that the information in the DBS certificate is relevant to the ongoing employment relationship, it (and any record of the information contained in it) will be kept securely for no longer than is necessary, and no more than six months.

4.15 The Company will not seek criminal records information from any source other than the individual concerned or the DBS.

4.16 DBS certificate information will be handled and kept in accordance with the Company's policy on handling DBS certificate information set out in Appendix 2.

5 Where an unprotected conviction or caution is disclosed

5.1 If the Company has concerns about the information that has been disclosed by the DBS, or the information is not as expected, the Company will discuss its concerns with the prospective employee and carry out a risk assessment.

5.2 The Company has a legal duty, when recruiting staff to work in regulated activity with children or vulnerable adults, to check whether they are on the relevant children's or adults' barred list. If a prospective employee's name does appear on the relevant barred list, it would be against the law for the Company to employ them to work or volunteer with the relevant group.

5.3 If a prospective employee is not barred from working with the relevant group, but nevertheless has a criminal record, it is up to the Company to decide on their suitability for the role. The Company will not refuse a prospective employee employment simply on the basis that they have a criminal record. Before making a decision, the Company will:

5.3.1 give the prospective employee the opportunity to address its concerns before making any decisions; and

5.3.2 carry out a risk assessment.

5.4 In carrying out a risk assessment, the Company will take account of:

5.4.1 the relevance of the conviction or other matter revealed to the position in question;

5.4.2 the seriousness of the offence or other matter revealed;

5.4.3 the circumstances of the offence;

5.4.4 the age of the offence;

5.4.5 whether there is a pattern of offending; and

5.4.6 whether circumstances have changed since the offending took place.

6 Training

The Company will ensure that all those within the organisation who are involved in the recruitment process:

6.1 have been suitably trained to identify and assess the relevance and circumstances of offences; and

6.2 have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders, eg the Rehabilitation of Offenders Act 1974.

APPENDIX 1
LEVEL OF DBS CHECK AND FILTERING

1 Requesting a DBS certificate

1.1 The level of DBS check that the Company is entitled to request will depend on the position for which the prospective employee's suitability is being assessed. The Company may request:

1.1.1 a criminal record certificate (CRC) if the position is protected by the Rehabilitation of Offenders Act 1974;

1.1.2 an enhanced criminal record certificate (ECRC) if the position is:

(a) excepted from the protections of the Rehabilitation of Offenders Act 1974 (ie included in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, as amended); and

(b) prescribed in the Police Act 1997 (Criminal Records) Regulations 2002. Or

1.1.3 in addition, a search of the children's OR adults' barred list if the position is:

(a) eligible for an ECRC; and

(b) prescribed in the Police Act 1997 (Criminal Records) Regulations 2009 as one for which the children's OR adults' barred list may be checked.

2 Filtering of protected convictions and cautions

2.1 Certain old and minor convictions and cautions are 'protected', which means:

2.1.1 they are filtered out of a DBS check;

2.1.2 they need not be disclosed by prospective employees to the Company; and

2.1.3 they will not be taken into account by the Company in making decisions about employing a prospective employee.

Certain 'listed offences' will never be filtered out (see here). https://www.gov.uk/government/publications/dbs-list-of-offences-that-will-never-be-filtered-from-a-criminal-record-check **The list includes offences which are particularly serious, relate to sexual or violent offending or are relevant in the context of safeguarding.**

2.2 A conviction will be a protected conviction (ie filtered) if:

2.2.1 the offence was not a listed offence;

2.2.2 it did not result in a custodial sentence (or sentence of service detention);

2.2.3 it is the individual's only conviction; and

2.2.4 where the individual was an adult at the time of conviction, 11 years or more have passed since the date of the conviction (or five years six months or more have passed since the date of conviction if the individual was under 18 at the time of conviction).

2.3 A caution will be a protected caution (ie filtered) if:

2.3.1 the offence was not a listed offence; and

2.3.2 where the individual was an adult at the time of the caution, six years or more have passed since the date of the caution (or two years or more have passed since the date of conviction if the individual was under 18 at the time of conviction).

2.4 As part of an ECRC, the police may also disclose information that they reasonably believe is relevant and ought to be included.

For further guidance on filtering, see the DBS filtering guidance. https://www.gov.uk/government/publications/dbs-filtering-guidance

APPENDIX 2
DATA HANDLING

1 Storage and access

The Company will ensure that DBS certificate information is kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

2 Handling

2.1 In accordance with section 124 of the Police Act 1997, the Company will ensure that certificate information is only passed to those who are authorised to receive it in the course of their duties. The Company maintains a record of all those to whom certificates or certificate information has been revealed. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

2.2 Once the DBS certificate has been inspected, it will be destroyed in accordance with the code of practice.

3 Usage

Certificate information must only be used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

4 Retention

4.1 Once a recruitment (or other relevant) decision has been made, the Company does not keep certificate information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints.

4.2 If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so.

4.3 Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

5 Disposal

5.1 Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, eg by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle (eg waste bin or confidential waste sack).

5.2 We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of

the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

6 DBS logo

The Company will not copy or use the DBS logo without prior approval of the DBS.

1 INFORMATION SECURITY POLICY - INTRODUCTION

1.1 The Company is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

1.2 In relation to personal information, under Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), the Company must:

1.2.1 use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

1.2.2 implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Company's data processing activities; and

1.2.3 be able to demonstrate that it has used or implemented such measures.

1.3 This purpose of this policy is to:

1.3.1 protect against potential breaches of confidentiality;

1.3.2 ensure all our information assets and IT facilities are protected against damage, loss or misuse;

1.3.3 support the Company's [*data protection policy*] in ensuring all staff are aware of and comply with UK law and the Company's procedures applying to the processing of personal information; and

1.3.4 increase awareness and understanding in the Company of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

2 Definitions

For the purposes of this Policy:

business information	means business-related information other than personal information regarding customers, clients, suppliers and other business contacts of the Company;
confidential information	means trade secrets or other confidential information (either belonging to the Company or to third parties) that is processed by the Company;

personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3 Roles and responsibilities

3.1 Information security is the responsibility of all staff. The Company's data protection officer (DPO) is in particular responsible for:

3.1.1 monitoring and implementing this policy;

3.1.2 monitoring potential and actual security breaches;

3.1.3 ensuring that staff are aware of their responsibilities; and

3.1.4 ensuring compliance with the requirements of Regulation (EU) 2016/679, GDPR and other relevant legislation and guidance.

4 Scope

4.1 The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Company, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

4.2 This policy applies to all staff, including employees, temporary and agency workers, other contractors, interns, volunteers and apprentices.

4.3 All staff must be familiar with this policy and comply with its terms.

4.4 The Company information covered by this policy may include:

4.4.1 personal information relating to staff, customers, clients, suppliers;

4.4.2 other business information; and

4.4.3 confidential information.

4.5 This policy supplements the Company's data protection policy (employment) and other policies and privacy notices relating to internet, email and communications, document retention and the contents of those policies must be taken into account, as well as this policy.

4.6 We will review and update this policy in accordance with our data protection and other obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy when it is adopted.

5 General principles

5.1 All Company information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

5.2 Personal information, and sensitive personal information, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

5.3 Staff should discuss with line managers the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information they access in the course of their work.

5.4 Company information (other than personal information) is owned by the Company and not by any individual or team.

5.5 Company information must be used only in connection with work being carried out for the Company and not for other commercial or personal purposes;

5.6 Personal information must be used only for the specified, explicit and legitimate purposes for which it is collected.

6 Information management

6.1 Personal information must be processed in accordance with:

6.1.1 the data protection principles, set out in the Company's data protection policy;

6.1.2 the Company's data protection policy generally; and

6.1.3 all other relevant policies.

6.2 In addition, all information collected, used and stored by the Company must be:

6.2.1 adequate, relevant and limited to what is necessary for the relevant purposes;

6.2.2 kept accurate and up to date;

6.3 The Company will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

6.3.1 pseudonymisation of personal information;

6.3.2 encryption of personal information;

6.4 Personal information and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with the Company's records retention policy.

7 Human resources information

7.1 Given the internal confidentiality of personnel files, access to such information is limited to DPO, and senior managers at Head Office. Except as provided in individual roles, other staff are not authorised to access that information.

7.2 Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

7.3 Staff may ask to see their personnel files and any other personal information in accordance with Regulation (EU) 2016/679, GDPR and other relevant legislation.

8 Access to offices and information

8.1 Office doors, keys and access codes must be kept secure at all times and keys or access codes must not be given or disclosed to any third party at any time.

8.2 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, eg through office windows.

8.3 Visitors must be required to sign in at reception, accompanied at all times and never left alone in areas where they could have access to confidential information.

8.4 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains Company information, then steps should be taken to ensure that no confidential information is visible.

8.5 At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

9 Computers and IT

9.1 Password protection and encryption must be used where available on Company systems in order to maintain confidentiality.

9.2 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or given to others.

9.3 Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.

9.4 Confidential information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/ thumb drive without the express written permission of the DPO and must be encrypted. Data held on any of these devices should be transferred to the Company's computer network as soon as possible in order for it to be backed up and then deleted from the device.

9.5 All electronic data must be securely backed up at the end of each working day. This happens automatically for all data stored on the Company's computer network.

9.6 Staff must ensure they do not introduce viruses or malicious code on to Company systems. Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact DPO or their Line Manager for guidance on appropriate steps to be taken to ensure compliance.

10 Communications and transfer of information

10.1 Staff must be careful about maintaining confidentiality when speaking in public places, eg when speaking on a mobile telephone.

10.2 Confidential information must be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the Company. Further details of how emailed information must be marked and protected are set out in the Company's internet, email and communications policy and in the rest of this section of the policy.

10.3 Confidential information must not be removed from the Company's offices unless required for authorised business purposes, and then only in accordance with paragraph 10.4 below.

10.4 Where confidential information is permitted to be removed from the Company's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

10.4.1 stored on an encrypted device with strong password protection, which is kept locked when not in use;

10.4.2 when in paper copy, not transported in see-through or other unsecured bags or cases;

10.4.3 not read in public places (eg waiting rooms, cafes, trains); and

10.4.4 not left unattended or in any place where it is at risk (eg in conference rooms, car boots, cafes).

10.5 Postal, document exchange (DX) and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

10.6 All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

11 Personal email and cloud storage accounts

11.1 Personal email accounts, such as yahoo, google or hotmail and cloud storage services, such as dropbox, icloud and onedrive are vulnerable to hacking. They do not provide the same level of security as the services provided by our own IT systems.

11.2 Do not use a personal email account or cloud storage account for work purposes.

11.3 If you need to transfer a large amount of data, contact Richard Cusworth for help.

12 Home working

12.1 Staff must not take Company information home unless required for authorised business purposes, and then only in accordance with paragraph 12.2 below.

12.2 Where staff are permitted to take Company information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

12.2.1 personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

12.2.2 all personal and confidential information must be retained and disposed of in accordance with paragraph 6.4 above.

12.3 Staff must not store confidential information on their home computers (PCs, laptops or tablets).

13 Transfer to third parties

13.1 Third parties should be used to process Company information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings.

Consideration must be given to whether the third parties will be processors for the purposes of Regulation (EU) 2016/679, GDPR.

13.2 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the DPO for more information.

14 Overseas transfer

14.1 There are restrictions on international transfers of personal information. Staff may only transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway, with the prior written authorisation of the DPO.

14.2 You should refer to the Company's data protection policy for further information on overseas transfers.

15 Training

15.1 Relevant staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every *two years* or whenever there is a substantial change in the law or our policy and procedure.

15.2 Training is provided via workshops.

15.3 Completion of training is compulsory.

15.4 The DPO will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our Information management and security policy or procedures, please contact the DPO.

16 Reporting breaches

16.1 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Company to:

16.1.1 investigate the failure and take remedial steps if necessary;

16.1.2 maintain a register of compliance failures; and

16.1.3 make any applicable notifications.

16.2 Please refer to our Personal data breach plan for our reporting procedure.

17 Consequences of failing to comply with this policy

17.1 The Company takes compliance with this policy very seriously. Failure to comply with it puts both staff and the Company at significant risk. The importance of this policy means that failure

to comply with any requirement of it may lead to disciplinary action, which may result in dismissal.

17.2 Staff with any questions or concerns about anything in this policy should not hesitate to contact the DPO.

1 INTERNET, EMAIL & COMMUNICATIONS POLICY

2 Introduction

2.1 This policy outlines the principles and standards the Company requires those using our internet, email and other communications systems to observe. It also explains when the Company will monitor the use of those systems and the action the Company will take if the terms of this policy are breached.

2.2 The Company expects all of its electronic and computer facilities to be used in an effective and professional manner and encourages all staff to develop the skills necessary to do so. These facilities are provided by the Company for its own business purposes to assist its staff in carrying out their duties effectively. It is the responsibility of all staff to ensure that this technology is used for proper business purposes and in a manner that does not compromise the Company or its workforce in any way.

2.3 Professional integrity is central to the Company and it must characterise all our dealings. All staff should think about how their own image or that of the Company may be affected by how they use the internet and other electronic communication systems. The same professional ethical obligations apply to conduct in online and offline environments.

2.4 This policy applies to the use of Company technology while at work and also when using Company technology from outside work eg when accessing our systems remotely, using a Company laptop or tablet when travelling and when using BlackBerries, smartphones or personal digital assistants (PDAs).

2.5 Misuse of the internet, email and/or other communication systems can expose both individuals and the Company to legal or financial liability. For example, an individual may enter into unintended contracts, breach copyright or licensing arrangements, incur liability for defamation or harassment or introduce viruses into the system. This policy is designed to safeguard both individuals and the Company from such liabilities. It is important that all staff read the policy carefully and ensure that all use of the internet, email and other communication systems is in accordance with its terms.

2.6 This policy applies to all employees of the Company, agency workers, volunteers, workers, consultants and other contractors who have access to Company computer and other communications systems. It also applies to personal use of the Company's equipment and technology in any way that reasonably allows others to identify any individual as associated with the Company.

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

2.8 Senior Management are responsible for the monitoring and implementation of this policy. Any questions about the content or application of this policy or other comments should be referred to your Line Manager.

3 Use of the Company's computer systems

3.1 Staff may use the Company's computer systems only to the extent that they are authorised to do so. Staff should not use the Company's computer equipment for any purpose that is not connected to the Company's business unless they have express permission to do so or they are making personal use of the system as permitted by this policy.

3.2 Use of the Company's systems for commercial purposes other than the business of the Company is strictly prohibited.

3.3 Any individual with access to the Company's network must adhere to strict access controls, to reduce the risk of virus infections, hacking and other unauthorised access attempts:

3.3.1 only authorised equipment is allowed to connect to the Company's network from any office location;

3.4 The Company licenses software from a number of sources. The Company does not own that software and must comply with any restrictions or limitations on use, in accordance with its licence agreements. All staff must adhere to the provisions of any software licence agreements to which the Company is party.

3.5 Staff must not use any software for any purpose outside the business of the Company without express written permission of senior management or as otherwise permitted by the terms of this policy.

3.6 Staff must not copy, download or install any software without first obtaining written permission from senior management.

4 Confidentiality

4.1 Staff should never assume that internal or external messages are necessarily private and confidential, even if marked as such. Email and the internet are not secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an email which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by email unless absolutely unavoidable and if so, should be clearly marked in the message header as highly confidential. The confidentiality of internal communications can only be ensured if they are sent by internal post, or delivered personally by hand or included in a password-protected or encrypted online document.

4.2 Email and internet messages should be treated as non-confidential. Anything sent through the internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way unless the messages are properly encrypted.

4.3 Staff should refer to their contract and the Staff Handbook for details of the types of information that the Company regards as confidential and which should be treated with particular care.

5 General rules regarding communications and email

5.1 All communications, including email, should reflect the highest professional standards at all times. In particular, all staff must:

5.1.1 keep messages brief and to the point;

5.1.2 ensure the spelling and grammar are carefully checked before sending;

5.1.3 ensure that all emails sent from the Company include the current disclaimer wording;

5.1.4 ensure that an appropriate heading is inserted in the subject field; and

5.1.5 double check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about the Company or a client/customer.

5.2 Staff must not send messages from another person's email address (unless authorised in the proper performance of their duties) or under an assumed name.

5.3 Staff must not send offensive, demeaning, disruptive or defamatory messages or images by any method. This includes, but is not limited to, messages or images inconsistent with the Company's Equal Opportunities Policy and Harassment and Bullying Policy and any sexist or racist material or any material which could be offensive on the grounds of a person's disability, age, sexual orientation, gender or religion or belief.

5.4 Staff must not place on the system or send any message or image which could be regarded as personal, potentially offensive or frivolous to any recipient or to any other person (even if not sent to them).

5.5 If any individual receives any communication containing material that is offensive or inappropriate to the office environment, the individual must delete it immediately. Under no circumstances should such communication be forwarded either internally or externally, other than internally to senior management at Head Office in order to report a breach of this policy.

5.6 Staff should not transmit anything in an email or other communication that they would not be comfortable writing (or someone else reading) in a letter. Emails leave a retrievable record and, even when deleted, can remain on both the individual's computer and on the Company's back-up system. Emails can be recovered and used as evidence in court proceedings and/or reviewed by regulators. Electronic messages are admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases.

5.7 Staff must not create congestion on the Company's systems by sending trivial messages or by unnecessary copying or forwarding of messages to recipients who do not need to receive them, or by sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.

5.8 Staff must use a Company email address for sending and receiving work-related emails and must not use their own personal email accounts to send or receive emails for the purposes of the Company's business. Staff must not send (inside or outside work) any message in the Company's name unless it is for an authorised, work-related purpose.

5.9 Staff must not send unsolicited commercial emails to persons with whom the individual does not have a prior relationship without the express permission of the relevant manager.

6 Passwords and security

6.1 Each individual is personally responsible for the security of all equipment allocated to or used by them. An individual must not allow equipment allocated to that person to be used by any other person other than in accordance with this policy.

6.2 Each individual must use passwords on all IT equipment allocated to them and must keep any password allocated to them confidential and must change their password regularly.

6.3 No individual may use another person's username and/or password to access the Company's systems, nor may any individual allow any other person to use their password(s). If it is anticipated that someone may need access to an individual's confidential files in their absence, that individual should arrange for the files to be copied to a network location that is properly secure where the other person can access them or give the person temporary access to the relevant personal folders.

6.4 All staff must log out of the Company's system or lock their computer when leaving their desk for any period of time. All staff must log out and shut down their computer at the end of the working day.

7 Contact lists

7.1 Lists of contacts compiled by staff during the course of their employment and stored on the Company's email system and/or other Company database(s) (irrespective of how they are accessed) belong to the Company. Such lists may not be copied or removed by staff for use outside their employment or after their employment ends.

8 Systems and data security

8.1 Be vigilant when using the Company's email system. Computer viruses are often sent by email and can cause significant damage to the Company's information systems. Be particularly cautious in relation to unsolicited email from unknown sources.

8.2 If any individual suspects that an email may contain a virus, they should not reply to it, open any attachments to it or click on any links in it and must contact senior management at Head Office immediately for advice.

8.3 No individual may download or install software from external sources without prior authorisation from senior management.

8.4 No personal computer, mobile phone, tablet computer, USB storage device or other device is permitted to be connected to the Company's systems or network without express prior written permission from senior management. Any permitted equipment must have up-to-date anti-virus software installed on it and the Company may inspect such equipment in order to verify this.

8.5 Staff must not run any '.exe' files, particularly those received via email, unless authorised to do so in writing by senior management. Unauthorised files should be deleted immediately upon receipt without being opened.

8.6 Staff must not access or attempt to access any password-protected or restricted parts of the Company's systems for which they are not an authorised user.

8.7 All staff must inform senior management immediately if they suspect their computer may have a virus and must not use the computer again until informed it is safe to do so.

8.8 All laptop, tablet, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

9 The internet

9.1 Access to the internet during working time is strictly limited to matters relating to your work duties and employment.

9.2 Any unauthorised use of the internet is strictly prohibited. Unauthorised use includes (but is not limited to):

9.2.1 creating, viewing, accessing any webpage or posting, transmitting or downloading any image, file or other information unrelated to your employment and, in particular, which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to the Company or to our clients/customers;

9.2.2 engaging in computer hacking and/or other related activities; and

9.2.3 attempting to disable or compromise security of information contained on the Company's systems or those of a third party.

9.3 Staff are reminded that such activity may also constitute a criminal offence.

9.4 Postings placed on the internet may display the Company's address. For this reason staff should make certain before posting information that the information reflects the standards and policies of the Company. Under no circumstances should information of a confidential or sensitive nature be placed on the internet. Staff must not use the Company's name in any internet posting (inside or outside work) unless it is for a work-related purpose.

9.5 Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the internet may be done only by express permission from the copyright holder. Staff must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer program.

9.6 Staff must not commit the Company to any form of contract through the internet.

9.7 Subscriptions to news groups, mailing lists and social networking websites are permitted only when the subscription is for a work-related purpose. Any other subscriptions are prohibited.

9.8 The Company may block or restrict access to any website at its discretion.

10 Monitoring

10.1 The Company's systems enable us to monitor telephone (including mobile telephone), email, voicemail, internet and other communications. Any individual's use (including personal use) of our systems may be monitored by automated software or otherwise, for business reasons, in order to carry out our obligations as an employer and in order to monitor compliance with the terms of this policy.

10.2 The Company reserves the right to monitor, intercept, retrieve and read the contents of any internal or external email or other communication to listen to or record any telephone conversation or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the Company's business, including for these purposes (the list is not exhaustive):

10.2.1 monitoring and record keeping to establish facts;

10.2.2 to establish compliance with regulatory or self-regulatory procedures;

10.2.3 to prevent, detect or investigate alleged crime or wrongdoing;

10.2.4 to investigate or detect the unauthorised use of the Company's systems or to ascertain compliance with the Company's policies, practices or procedures (including this policy);

10.2.5 to locate and retrieve lost messages or files;

10.2.6 to check whether communications are relevant to the business (for example when an individual is absent due to sickness or holiday); and/or

10.2.7 to comply with any legal obligation.

11 Prohibited use and breach of this policy

11.1 The Company considers this policy to be extremely important. Any breach of the policy will be dealt with under the Company's dismissal and disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in immediate termination

of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, the Company may withdraw an individual's internet and/or email access.

11.2 Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

11.2.1 unauthorised use of the internet as outlined in paragraph 9.2 above;

11.2.2 creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;

11.2.3 creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in the Company's Equal Opportunities Policy and our Harassment and Bullying Policy;

11.2.4 accessing, transmitting or downloading any confidential information about the Company and/or any of our staff and/or client or customers, except where authorised in the proper performance of your duties;

11.2.5 accessing, transmitting or downloading unauthorised software; and

11.2.6 viewing, accessing, transmitting or downloading any material in breach of copyright.

12 Review and training

12.1 The Company regularly monitors the effectiveness of this policy to ensure it is working in practice and will review and update this policy as and when necessary. The Company will provide information and/or training on any changes made.

12.2 Relevant staff will receive appropriate training on this policy, including training on any updates made to it.

1 POLICY GDPR DATA SUBJECT ACCESS REQUESTS

2 Introduction

2.1 The Company holds personal data (or information) about job applicants, employees, clients, customers, suppliers, business contacts and other individuals for a variety of business purposes.

2.2 Under Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), individuals (known as 'data subjects') have a general right to find out whether we hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request. The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that we are undertaking.

2.3 Our data protection officer, is responsible for ensuring:

2.3.1 that all data subject access requests are dealt with in accordance with the GDPR and other relevant legislation and guidance; and

2.3.2 that all staff have an understanding of the GDPR and other relevant legislation and guidance in relation to data subject access requests and their personal responsibilities in complying with the relevant aspects of the GDPR and other relevant legislation and guidance.

2.4 This policy provides guidance for staff members on how data subject access requests should be handled, and is intended for internal use. It is not a privacy policy or statement, and is not to be made routinely available to third parties.

2.5 This policy applies to all staff but much of it is aimed primarily at those members of staff who are authorised to handle data subject access requests. These sections are identified by the words '(authorised staff)' appearing in the section title. For other staff members, it provides guidance on:

2.5.1 what to do if you receive a data subject access request (see paragraph 4 below); and

2.5.2 how to decide whether a request for information is a data subject access request (see paragraph 3 below).

2.6 Failure to comply with the right of access under the GDPR puts both staff and the Company at potentially significant risk, and so the Company takes compliance with this policy very seriously. For further information on the consequences of failure to comply, see paragraph 16 below.

2.7 We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

2.8 If you have any questions regarding this policy, please contact the data protection officer senior management at Head Office.

3 How to recognise a data subject access request (all staff)

3.1 A data subject access request is a request from an individual (or from someone acting with the authority of an individual, eg a parent making a request in relation to information relating to their child):

3.1.1 for confirmation as to whether we process personal data about him or her and, if so

3.1.2 for access to that personal data

3.1.3 and certain other supplementary information

3.2 Such a request will typically be made in writing but may be made orally (eg during a telephone conversation). The request may refer to the GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a data subject access request and should be treated as such.

3.3 All data subject access requests should be immediately directed to the data protection officer in accordance with paragraph 4 below.

4 What to do when you receive a data subject access request (all staff)

4.1 If you receive a data subject access request and you are not authorised to handle it, you must immediately take the steps set out in paragraphs 4.3 (request received by email) or 4.4 (request received by letter or fax) There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

4.2 For information on what amounts to a data subject access request, see paragraph 3 above. If you are in any way unsure as to whether a request for information is a data subject access request, please contact the data protection officer.

4.3 If you receive a data subject access request by email, you must immediately forward the request to the data protection officer.

4.4 If you receive a data subject access request by letter you must:

4.4.1 scan the letter;

4.4.2 send the original to the data protection officer; and

4.5 If you receive a data subject access request orally, you must:

4.5.1 take the name and contact details of the individual;

4.5.2 inform the individual orally that you will notify the data protection officer and that the data protection officer will contact them in relation to the request;

4.5.3 immediately email the data protection officer and provide the individual's contact details and details of the oral request and the date on which it was received.

4.6 You will receive confirmation when the request (or your email concerning an oral request) has been received by the data protection officer. If you do not receive such confirmation within [*two*] working days of sending it, you should contact the data protection officer to confirm safe receipt.

4.7 You must not take any other action in relation to the data subject access request unless the data protection officer has authorised you to do so in advance and in writing.

5 Conditions for responding to a valid request (authorised staff)

5.1 Where we process a large quantity of information about an individual, we may need to ask the individual to specify the information or processing activities to which the request relates.

5.2 While it is not a requirement under Regulation (EU) 2016/679, GDPR that an individual must make a DSAR in writing, it is helpful for the Company if they do so. Individuals should therefore be encouraged to use the Data subject access request form set out in Appendix i.

5.3 We will not usually charge a fee for responding to a data subject access request. We may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

5.3.1 that is manifestly unfounded or excessive, eg repetitive; or

5.3.2 for further copies of the same information.

6 Identifying the data subject (authorised staff)

6.1 Before responding to a data subject access request, we will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward.

6.2 We will not retain personal data, eg relating to former employees for the sole purpose of being able to react to potential data subject access requests in the future.

6.3 If we have doubts as to the identity of the person making the data subject access request, we may ask for additional information to confirm his or her identity. The Data subject access request form contains examples of the type of documents that can be used to do this. Typically, we will request a copy of the individual's driving licence or passport to enable us to establish his or her identity and signature (which should be compared to the signature on the data subject

access request and any signature we already hold for the individual). We also ask for a recent utility bill (or equivalent) to verify the individual's identity and address.

6.4 If, having requested additional information, we are still not in a position to identify the data subject, we may refuse to act on a data subject access request (see paragraph [7] below).

7 Refusing to respond to a request (authorised staff)

7.1 We may refuse to act on a data subject access request where:

7.1.1 even after requesting additional information in accordance with paragraph 6.2, we are not in a position to identify the individual making the data subject access request;

7.1.2 requests from an individual are manifestly unfounded or excessive, eg because of their repetitive character or, in certain circumstances, where the request relates to large amounts of data.

7.2 If we intend to refuse to act on a data subject access request, we will inform the individual, no later than one month after receiving his or her request:

7.2.1 of the reason(s) why we are not taking action; and

7.2.2 that they have the right to complain to the ICO and seek a judicial remedy.

8 Time limit for responding to a request (authorised staff)

8.1 Once a data subject access request is received, the Company must provide the information requested without delay and at the latest within one month of receiving the request. You should therefore make a note of when request was received and when the time limit will end.

8.2 If a data subject access request is complex or the data subject has made numerous requests, the Company:

8.2.1 may extend the period of compliance by a further two months; and

8.2.2 must inform the individual of the extension within one month of the receipt of the request, and explain why the extension is necessary.

9 Information to be provided in response to a request (authorised staff)

9.1 The individual is entitled to receive access to the personal data we process about him or her and the following information:

9.1.1 the purposes for which we process the data;

9.1.2 the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;

9.1.3 where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;

9.1.4 the fact that the individual has the right:

(a) to request that the Company rectifies, erases or restricts the processing of his personal data; or

(b) to object to its processing;

(c) to lodge a complaint with the ICO;

9.1.5 where the personal data has not been collected from the individual, any information available regarding the source of the data;

9.1.6 any automated decision we have taken about him or her (see paragraph 10 below), together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

9.2 The information referred to in paragraph 9.1 should be provided using the Company's standard form response to data subject request—right of access:

9.2.1 in a way that is concise, transparent, easy to understand and easy to access;

9.2.2 using clear and plain language, with any technical terms, abbreviations or codes explained;

9.2.3 in writing using the Company's standard form Response to data subject request—right of access in Appendix ii, if the data subject access request was made in writing;

9.2.4 in a commonly-used electronic format, if the data subject access request was made electronically, unless otherwise requested by the individual; and

9.2.5 where possible, by providing remote access to a secure system which would provide the data subject with direct access to his or her personal data.

10 Automated decision-making

10.1 If the data subject access request specifically asks for information about the logic behind any automated decision that we have taken in relation to important matters relating to the individual (eg performance at work, creditworthiness, reliability or conduct), we must provide a description of the logic involved in that automated decision, subject to the following conditions:

10.1.1 the automated decision must have constituted the sole basis for the decision. (For example, an application for credit which is conducted without any human intervention, other than to complete the application form, could be a decision which is taken solely by automatic means. However, if there is any element of human discretion as to whether or not to grant the credit, the decision would cease to be wholly automated and the individual would not be entitled to a description of the logic**)**;

10.1.2 in providing a description of the logic we are not required to reveal any information which constitutes a trade secret (eg the algorithm behind a credit scoring system).

10.2 If the Company carries out automated decision-making in relation to an individual, the data subject access request may include a request:

10.2.1 for information relating to the automated decision;

10.2.2 for human intervention on the part of the Company, ie to ask that an individual with the authority and competence to change the decision should review the automated decision, considering all the available data;

10.2.3 to express his or her point of view on the automated decision; and/or

10.2.4 to contest the automated decision.

If such a request is received, the data protection officer or senior management will ensure that it is dealt with in accordance with the GDPR and other relevant legislation and guidance.

11 How to locate information (authorised staff)

11.1 The personal data we need to provide in response to a data subject access request may be located in several of our electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

11.2 Depending on the type of information requested, you may need to search all or some of the following:

11.2.1 electronic systems, eg databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;

11.2.2 manual filing systems in which personal data are accessible according to specific criteria, eg chronologically ordered sets of manual records containing personal data;

11.2.3 data systems held externally by our data processors, eg external payroll service providers;

11.2.4 occupational health records held by the HR department

11.2.5 pensions data held by pension administrator

11.2.6 insurance benefit information held by insurance benefit provider

11.2.7 data held by outsourced consultants engaged by the Company that may hold data, eg consultants engaged to provide assistance with performance management and/or disciplinary and grievance procedures

11.3 You should search these systems using the individual's name, employee number, customer account number or other personal identifier as a search determinant.

12 What is personal data? (authorised staff)

12.1 Once you have carried out the search and gathered the results, you will need to select the information to be supplied in response to the data subject access request. The individual is only entitled to receive information which constitutes his or her personal data.

12.2 Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, eg their name, identification number, location data or online identifier. It may also include personal data that has been pseudonymised (eg key-coded), depending on how difficult it is to attribute the pseudonym to a particular individual.

13 Requests made by third parties on behalf of the individual (authorised staff)

Occasionally we may receive a request for data subject access by a third party (an 'agent') acting on behalf of an individual. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that he or she is authorised to act on behalf of the individual. The Data subject access request form in Appendix i should be used for all such requests.

14 Exemptions to the right of subject access (authorised staff)

14.1 In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

14.2 **Crime detection and prevention:** We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to. For example, if the disclosure of the personal data could alert the individual to the fact that he or she is being investigated for an illegal activity (ie by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

14.3 **Protection of rights of others:** We do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information (or that information and any other information that we reasonably believe the data subject is likely to possess or obtain), unless:

14.3.1 that other individual has consented to the disclosure of the information to the individual making the request; or

14.3.2 it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:

(a) the type of information that would be disclosed;

(b) any duty of confidentiality owed to the other individual;

(c) any steps taken by the controller with a view to seeking the consent of the other individual;

(d) whether the other individual is capable of giving consent; and

(e) any express refusal of consent by the other individual.

14.4 **Confidential references:** We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

14.4.1 education, training or employment of the individual;

14.4.2 appointment of the individual to any office; or

14.4.3 provision by the individual of any service

This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (ie the person giving the reference), which means you must consider the rules regarding disclosure of third-party data set out in paragraph 13 before disclosing the reference.

14.5 **Legal professional privilege:** We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

14.5.1 'Advice privilege' covers confidential communications between the Company and our lawyers where the dominant purpose of the communication is the seeking or giving of legal advice;

14.5.2 'Litigation privilege' covers any document which was created with the dominant purpose of being used in actual or anticipated litigation (eg legal proceedings before a court or tribunal). Once a bona fide claim to litigation privilege ends, the documents in the file which were subject to litigation privilege become available if a data subject access request is received.

If you think the legal professional privilege exemption could apply to the personal data that have been requested, you should refer the matter to the DPO for further advice.

14.6 **Management forecasting:** We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions and demotions. This exemption must be considered on a case-by-case basis and must only be

applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

14.7 **Negotiations:** We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations. For example, if HR is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes a data subject access request, HR can legitimately withhold giving access to information which would prejudice those redundancy negotiations. The HR department must, however, disclose all other personal data relating to the individual unless those other personal data are also exempt from disclosure.

15 Deleting personal data in the normal course of business (authorised staff)

15.1 The information that we are required to supply in response to a data subject access request must be supplied by reference to the data in question at the time the request was received. However, as we have one month in which to respond and we are generally unlikely to respond on the same day as we receive the request, we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied if such amendment or deletion would have been made regardless of the receipt of the data subject access request.

15.2 We are, therefore, allowed to carry out regular housekeeping activities even if this means that we delete or amend personal data after the receipt of a data subject access request. What we are not allowed to do is amend or delete data because we do not want to supply the data.

16 Consequences of failing to comply with this policy (all staff)

16.1 The Company takes compliance with this policy very seriously. If we fail to comply with a subject access request or fail to provide access to all the personal data requested, or fail to respond within the one-month time period, we will be in breach of GDPR and other relevant legislation. This may have several consequences:

16.1.1 it may put at risk the individual(s) whose personal information is being processed;

16.1.2 the individual may complain to the ICO and this may lead the ICO to investigate the complaint. If we are found to be in breach, enforcement action could follow, which carries the risk of significant civil and criminal sanctions for the Company and, in some circumstances, for the individual responsible for the breach;

16.1.3 if an individual has suffered damage, or damage and distress, as a result of our breach of the GDPR or other relevant legislation, he or she may take us to court and claim damages from us; and

16.1.4 a court may order us to comply with the subject access request if we are found not to have complied with our obligations under the GDPR and other relevant legislation.

16.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

17 Contacts and responsibilities (all staff)

17.1 This Policy will be reviewed annually by the data protection officer.

17.2 Any questions regarding this Policy should be address to the data protection officer.

Appendix i Data Subject Access Form

Please complete this form if you wish to request access to your personal data. You do not have to use this form, but it will help us to deal with your request as quickly and effectively as possible if you do.

You can also use this form if you are requesting access to personal data on behalf of someone else. In that case, we will need you to confirm you have that person's authority to ask for access to their data.

If you have any questions about this form or your request, please contact [*insert contact details*] to discuss it further.

1 About you

A Please provide the following information. If you have an account number or other reference number, please provide it.

Full name	[*Details to be inserted here*]
Address	[*Details to be inserted here*]
Contact details	[*Details to be inserted here*]
Customer account number OR Client number OR National Insurance number	[*Details to be inserted here*]

B For security reasons, we cannot respond to a request unless we have confirmed your identity. Please provide:

C a certified copy driving licence or passport, plus a utility bill or other proof of address]

2 Whose personal data are you requesting?

D Please provide the following information. If you are making this request on behalf of someone else, we will need this information before we can supply you with the data you are asking for.

Are you requesting access to your own personal data?	☐ Yes, please go to section 3 below. ☐ No, please complete the rest of this section of the form.

2.1 If you are not requesting access to your own personal data, please provide the following information about the person on whose behalf you are making this request:

Full name	[*Details to be inserted here*]
Address	[*Details to be inserted here*]
Contact details	[*Details to be inserted here*]
Customer account number OR Client number OR National Insurance number	[*Details to be inserted here*]
Age (if under 16)	[*Details to be inserted here*]

E We cannot respond to your request until we also receive satisfactory confirmation of the identity of the person on whose behalf you are making this request. Please provide:

F a certified copy of their driving licence or passport, plus a utility bill or other proof of their address

2.2 Please provide a copy of your legal authority to make this request. This might be a signed letter of authority from the person on whose behalf you are making this request, a power of attorney, or confirmation that you are their legal representative.

3 What data are you requesting?

G Please describe what personal data and other information you are requesting, in particular if you are asking for specific documents or information.

Description of the personal data and information requested including details of any specific documents or information you asking for (where relevant)	[*Details to be inserted here*]

H Please give as much detail as possible about where the data might be located and any other relevant information. You do not have to provide this information, but doing so will help us to deal with your request as quickly and effectively as possible.

Location of data, eg any particular departments or parts of the organisation you have dealt with (if known)	[*Details to be inserted here*]
Relevant time periods, eg when we are likely to have obtained your data (if known)	[*Details to be inserted here*]

Dates of any particular correspondence, meetings or telephone calls (if known)	[*Details to be inserted here*]
The name(s) of people you have dealt with within our organisation (if known)	[*Details to be inserted here*]
Any other relevant information you can think of that might help us respond to your request	[*Details to be inserted here*]

4 Signature

I Please check the information you have provided and sign below.

Signed	[*Signature to be inserted here*]
Date	[*Date to be inserted here*]

J Please send this form and the documents we have asked you to provide to: Richard Cusworth Richard.cusworth@cantel.uk.com Unit 12 Pavilion Business Park, Royds Hall Road, Leeds LS12 6AJ

K If you are making this request by email, we will provide the information to you in an electronic format unless you ask us not to. If you wish to receive your information in a different format, eg hard copy please let us know in the box below.

[*Details to be inserted here*]

RECORDS RETENTION SCHEDULE

Introduction

This Record retention schedule accompanies and is incorporated into the Company's Record management policy. It sets out the time periods that different types of (employment-related) business records must be retained for business and legal purposes. This is a relatively lengthy document listing the many types of employment-related records used by the company and the applicable retention periods for each record type.

The retention periods are based on business needs and legal requirements. If you maintain any types of records that are not listed in this Schedule, and it is not clear from the existing record types in this Schedule what retention period should apply, please contact the data protection officer for guidance.

Any deviation from the retention periods in this Schedule must be approved in advance by the DPO.

1 Employment records

1.1 Personnel records

Record	Recommended retention period	Storage format	Reference
Rejected job applicant records, including: contact details application letters or forms CVs references certificates of good conduct interview notes assessment and psychological test results	Six months after applicant is notified of rejection	Paper or electronic	ICO Employment Practices Code para 1.7 Equality Act 2010, s 123
Application records of successful candidates, including:	Seven years after employment ceases	Paper or electronic	Limitation Act 1980 (LA 1980), s 5

Record	Recommended retention period	Storage format	Reference
application letters or forms copies of academic and other training received references correspondence concerning employment CVs interview notes and evaluation forms assessment and psychological test papers and results			
Criminal records information: criminal records requirement assessments for a particular post criminal records information forms the Disclosure and Barring Service (DBS) check forms DBS certificates	Criminal records requirement assessments for a particular post—12 months after the assessment was last used All other information in this category—as soon as practicable after the check has been completed and the outcome recorded (ie whether satisfactory or not) unless, in exceptional circumstances, the data protection officer assesses that it is clearly relevant to the ongoing employment relationship to allow for consideration and	Paper or electronic	DBS guidance for employers: Duration of criminal record check validity ICO Employment Practices Code Nov 2011, part 1.7.4

Record	Recommended retention period	Storage format	Reference
	resolution of any disputes or complaints in which case, six months If the data protection officer considers it necessary to keep the information for longer than six months, the DBS should be consulted		
Employment contracts, including: personnel and training records written particulars of employment changes to terms and conditions	Seven years after employment ceases, unless document executed as a deed, in which case 13 years after employment ceases	Paper or electronic	LA 1980, ss 5, 8
Directors' service contracts and any variations	Seven years from termination or expiry of the contract, unless executed as a deed, in which case 13 years from termination or expiry	Paper or electronic	LA 1980, ss 5, 8 Companies Act 2006, ss 227 and 228
Copies of identification documents (eg passports)	Not less than two years from date of termination of employment	Paper or electronic	Immigration (Restrictions on Employment) Order SI 2007/3290, Art 6(1)(b)
Identification documents of foreign	Two years and six months from date of	Paper or electronic	Immigration (Restrictions on Employment) Order

Record	Recommended retention period	Storage format	Reference
nationals (including right to work)	termination of employment		SI 2007/3290, art 6(1)(b)
Records concerning a temporary worker	Seven years after employment ceases	Paper or electronic	LA 1980, s 5
Employee performance and conduct records, including: probationary period reviews review meeting and assessment interviews appraisals and evaluations promotions and demotions **[**[For relevant organisations only] all information relevant to an assessment of the individual's fitness and propriety under the Senior Managers and Certification (SM&CR) regime or Senior Insurance Managers regime (SIMR)**]**	Seven years after employment ceases	Paper or electronic	LA 1980, s 5 See Practice Note: Regulatory references under the SM&CR and SIMR
Records relating to and/or showing compliance with Working Time Regulations 1998 including:	Two years from the date on which the record was made	Paper or electronic	Working Time Regulations 1998, SI 1998/1833, reg 9

Record	Recommended retention period	Storage format	Reference
registration of work and rest periods working time opt-out forms			
Redundancy records	Seven years from date of redundancy	Paper or electronic	LA 1980, s 5
Annual leave records	Seven years after the end of each tax year	Paper or electronic	LA 1980, s 5
Parental leave records	Seven years after the end of each tax year	Paper or electronic	LA 1980, s 5
Sickness records	Seven years after the end of each tax year	Paper or electronic	LA 1980, s 5
Records of return to work meetings following sickness, maternity etc	Seven years the end of each tax year	Paper or electronic	LA 1980, s 5

1.2 Payroll and salary records

Record	Recommended retention period	Storage format	Reference
Records for the purposes of tax returns including wage or salary records, records of overtime, bonuses and expenses	Seven years	Paper or electronic	Taxes Management Act, 1970 s 12B Finance Act 1998, Schedule 18, para 21
Pay As You Earn (PAYE) records, including:	Three years after the end of the tax year to which they relate	Paper or electronic	Income Tax (Pay As You Earn) Regulations 2003, SI 2003/2682, reg 97

Record	Recommended retention period	Storage format	Reference
wage sheets deductions working sheets calculations of the PAYE income of employees and relevant payments to them, the deduction of tax from, or accounting for tax in respect of, such payments all documents relating to any information which an employer is required to provide to HMRC under Form P11D (benefits in kind)			
Records demonstrating compliance with national minimum wage requirements, including hours worked	Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends	Paper or electronic	National Wage Act 1998, s 9 National Minimum Wage Regulations 2015, SI 2015/621, reg 59
Employee income tax and national insurance returns and associated HMRC correspondence	Three years from end of tax year to which they relate	Paper or electronic	Income Tax (Pay as You Earn) Regulations 2003, SI 2003/2682, reg 97
Statutory sick pay (SSP) records	Three years after the end of the tax year to which they relate	Paper or electronic	The requirement to maintain SSP records for three years after the end of the tax year to which they relate was revoked in 2014, but

Record	Recommended retention period	Storage format	Reference
			an employer may still be required by HMRC to produce such records as are in his possession or power which contain, or may contain, information relevant to satisfy HMRC that statutory sick pay has been and is being paid. The Statutory Sick Pay (General) Regulations 1982, SI 1982/894, reg 13(A)
Wage or salary records (including overtime, bonuses and expenses) and payments to consultants and independent contractors	Seven years	Paper or electronic	Taxes Management Act 1970, s 43
Statutory maternity, paternity and shared parental pay records, calculations, certificates or other evidence	Three years after the end of the tax year in which the period of statutory pay ends	Paper or electronic	Statutory Maternity Pay (General) Regulations 1986, SI 1986/1960, reg 26 (and other corresponding legislation)

2 Health and safety records

Record	Recommended retention period	Storage format	Reference
Records of reportable injuries, diseases or dangerous occurrences reportable incidents reportable diagnoses injury arising out of accident at work (including [*insert organisation's name*]'s accident book)	Three years from date of the entry	Paper or electronic	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR 2013), SI 2013/1471, reg 12
Lists or register of employees who have been exposed to asbestos dust, including health records of each employee	40 years from the date of the last entry made in the record	Paper or electronic	Control of Asbestos Regulations 2012, SI 2012/63, reg 22(1)
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry made in the record	Paper or electronic	The Control of Lead at Work Regulations 2002 (CLAW 2002), SI 2002/2676, reg 10
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record	Paper or electronic	The Control of Substances Hazardous to Health Regulations 2002 (COSHH 2002), SI 2002/2677, reg 11

Record	Recommended retention period	Storage format	Reference
Records of monitoring of exposures to hazardous substances (where exposure monitoring is required under COSHH)	Where the record is representative of the personal exposures of identifiable employee—40 years from the date of the last entry made in the record Otherwise, five years from the date of the last entry made in the record	Paper or electronic	COSHH 2002, reg 10(5)
Records of tests and examinations of control systems and protective equipment under COSHH	Five years from the date on which the record was made	Paper or electronic	COSHH 2002, reg 9

GDPR DATA PROTECTION POLICY

You must read this policy because it gives important information about:

- the data protection principles with which the Company must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, eg about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to the data protection officer.

1 GDPR DATA PROTECTION POLICY - INTRODUCTION

1.1 The Company obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices for a number specific lawful purposes, as set out in the Company's data protection privacy notices relating to recruitment and employment.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

1.4 The Company's data protection officer, is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer.

2 Scope

2.1 This policy applies to the personal information of job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

2.2 Staff should refer to the Company's data protection privacy notice and, where appropriate, to its other relevant policies including in relation to internet, email and communications, monitoring, social media, information security, data retention, bring your own device (BYOD) and criminal record information, which contain further information regarding the protection of personal information in those contexts.

2.3 We will review and update this policy regularly in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

3 Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal

	information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 The Company will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

4.1.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

(f) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

6 Sensitive personal information

6.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

6.2 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, eg it is necessary for the performance of the employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and

6.2.2 one of the special conditions for processing sensitive personal information applies, eg:

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.3 Before processing any sensitive personal information, staff must notify the data protection officer of the proposed processing, in order that the data protection officer may assess whether the processing complies with the criteria noted above.

6.4 Sensitive personal information will not be processed until:

6.4.1 the assessment referred to in paragraph 6.3 has taken place; and

6.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.5 The Company will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

6.6 The Company's data protection privacy notice sets out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

6.7 In relation to sensitive personal information, the Company will comply with the procedures set out in paragraphs 6.8 and 6.9 below to make sure that it complies with the data protection principles set out in paragraph 4 above.

6.8 **During the recruitment process**: the company, with guidance from HR and the data protection officer, will ensure that (except where the law permits otherwise):

6.8.1 during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, eg race or ethnic origin, trade union membership or health;

6.8.2 if sensitive personal information is received, eg the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

6.8.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

6.8.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

6.8.5 we will not ask health questions in connection with recruitment and only ask health questions once an offer of employment has been made.

6.9 **During employment**: the HR department, with guidance from the data protection officer, will process:

6.9.1 health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

6.9.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting.; and

6.9.3 (may process) trade union membership information for the purposes of staff administration and administering 'check off'.

7 Criminal records information

L Criminal records information will be processed in accordance with the Company's Criminal records information policy.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to an individual's data protection rights (eg where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to individuals; and

8.1.3 what measures can be put in place to address those risks and protect personal information.

8.2 Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer in order that a DPIA can be carried out.

8.3 During the course of any DPIA, the employer will seek the advice of the data protection officer.

9 Documentation and records

9.1 We will keep written records of processing activities which are high risk, ie which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

9.1.1 the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);

9.1.2 the purposes of the processing;

9.1.3 a description of the categories of individuals and categories of personal data;

9.1.4 categories of recipients of personal data;

9.1.5 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;

9.1.6 where possible, retention schedules; and

9.1.7 where possible, a description of technical and organisational security measures.

9.2 As part of our record of processing activities we document, or link to documentation, on:

9.2.1 information required for privacy notices;

9.2.2 records of consent;

9.2.3 controller-processor contracts;

9.2.4 the location of personal information;

9.2.5 DPIAs; and

9.2.6 records of data breaches.

9.3 If we process sensitive personal information or criminal records information, we will keep written records of:

9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

9.3.2 the lawful basis for our processing; and

9.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

9.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

9.4.1 carrying out information audits to find out what personal information the Company holds;

9.4.2 distributing questionnaires and talking to staff across the Company to get a more complete picture of our processing activities; and

9.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

10 Privacy notice

10.1 The Company will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11 Individual rights

11.1 You (in common with other data subjects) have the following rights in relation to your personal information:

11.1.1 to be informed about how, why and on what basis that information is processed—see the Company's data protection privacy notice;

11.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the Company's subject access request policy;

11.1.3 to have data corrected if it is inaccurate or incomplete;

11.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

11.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

11.2 If you wish to exercise any of the rights in paragraphs 11.1.3 to 11.1.6, please contact the data protection officer .

12 Individual obligations

12.1 Individuals are responsible for helping the Company keep their personal information up to date. You should let your Line Manager know if the information you have provided to the Company changes, for example if you move house or change details of the bank or building society account to which you are paid. Alternatively, you can update your own personal information on a secure basis via the Company's intranet.

12.2 You may have access to the personal information of other members of staff, suppliers and customers of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 11.1 above.

12.3 If you have access to personal information, you must:

12.3.1 only access the personal information that you have authority to access, and only for authorised purposes;

12.3.2 only allow other Company staff to access personal information if they have appropriate authorisation;

12.3.3 only allow individuals who are not Company staff to access personal information if you have specific authority to do so from the data protection officer;

12.3.4 keep personal information secure (eg by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's *information security policy*);

12.3.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

12.4 You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6.2.2 being met;

12.4.2 any data breach as set out in paragraph 15.1 below;

12.4.3 access to personal information without the proper authorisation;

12.4.4 personal information not kept or deleted securely;

12.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;

12.4.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

13 Information security

13.1 The Company will use appropriate technical and organisational measures in accordance with the Company's policies to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13.2 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

13.2.1 the organisation may act only on the written instructions of the Company;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-contractors are only engaged with the prior consent of the Company and under a written contract;

13.2.5 the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;

13.2.6 the organisation will assist the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organisation will delete or return all personal information to the Company as requested at the end of the contract; and

13.2.8 the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the data protection officer.

14 Storage and retention of personal information

14.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's information security policy.

14.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Company's records retention policy which set out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the data protection officer.

14.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal information is stored;

15.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

15.2 The Company will:

15.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

15.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16 International transfers

16.1 The Company may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) on the basis that that country, territory or organisation is designated as having an adequate level of protection.

17 Training

M The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under

this policy, will receive additional training to help them understand their duties and how to comply with them.

18 Consequences of failing to comply

18.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy:

18.1.1 puts at risk the individuals whose personal information is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

18.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.