Accapita
accountants and
business advisors

DATA PROTECTION POLICY

Personal data may consist of data kept on paper, computer or other electronic media. We take the security and privacy of all personal data seriously. We gather, store and process personal data whilst carrying out our business activities and use this to manage our relationships with our current, past and prospective employees, clients, suppliers and other individuals, third parties and other organisations with whom we have dealings.

This policy aims to assist us in complying with the requirements of data protection legislation and to minimise any risk to our business by setting out clear guidelines relating to the processing, storage and disposal of personal data. It explains how we will hold and process personal data, outlines the rights of data subjects, as well as the obligations placed on all individuals when obtaining, handling, processing, storing or disposing of personal data in the course of working for, or on behalf of, our business.

Failure to comply with data protection legislation could have serious consequences for our reputation or our business. We therefore require all employees, workers and contractors to read this policy carefully and ask if they have any questions.

This policy is not contractual and may be amended or updated at any time. If any conflict arises between this policy and the 2018 Act and the GDPR laws, we intend to comply with the latter. Where appropriate, we will notify data subjects of any changes that apply to them personally by mail or email.

Who is covered by this policy

This policy applies to current, former and prospective employees, workers, apprentices and consultants, in particular those who handle personal data, whether this relates to their colleagues, our clients, or anyone else (such as potential clients to whom we send marketing or sales information). It should be read in conjunction with any contract of employment, contract for services and any other notice we issue from time to time in relation to personal data.

CONTENTS

Data protection policy

1. Definitions

We aim to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act'), the EU General Data Protection Regulation ('GDPR') and any codes of practice or advisory notes issued by the Information Commissioner (ICO). These restrict and control the way we process personal data and how others process data on our behalf. They also grant rights to the individuals whose data is processed.

Personal data
'Personal data' is information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession (such as name, ID, number, date of birth, online identifier (such as an IP address or "cookie") or location data, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that person). It includes any expression of opinion about the person, their actions or behaviour and any indication of the intentions of us or others, in respect of that person.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials. It includes documents, emails, data in electronic databases, messages, telephone logs or recordings, cctv footage, security records, records of internet, email and telephone usage, vehicle trackers and any other such activities. Information about individual contacts at companies, or gained via platforms such as LinkedIn or Facebook, is also personal data.

Personal data may relate to our current, past and prospective employees, clients, suppliers and other individuals with whom we have dealings.

Personal data might be provided to us by the individual, or someone else (such as a former employer, their doctor, or a credit reference agency), or it could be created by a manager or colleague. Personal data relating to employees, workers or contractors could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination.

Personal data does not include anonymised data. Information on deceased persons is not protected, but should still be treated with sensitivity.

Special categories data
'Special categories data' is personal data consisting of information regarding an individual's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data (where processed to uniquely identify a natural person)
- physical or mental health or condition
- sex life and sexual orientation and
- any criminal proceedings or convictions.

All the general compliance requirements apply to special categories data in the same way as to any other personal data, however, stricter conditions must be satisfied before special categories data can be processed.

Data processing
'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage
- adaption or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination and restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing. It also includes transferring personal data to third parties. However, this list is not exhaustive and therefore other forms of processing are possible.

Data controller
Accapita is a 'data controller'. This means that we determine the purpose and the manner in which, any personal data is processed.

We are responsible for ensuring and demonstrating compliance with the GDPR, for promptly notifying and updating the Information Commissioner (and data subjects where necessary) of any serious breaches of data protection, and for the monitoring and implementation of this policy. We are also responsible for implementing appropriate technical and organisational measures to ensure and to demonstrate compliance with data protection legislation.

We will ensure that, both in the planning and implementation phases of processing activities, data protection principles and appropriate safeguards are addressed and implemented and that records of processing activity are kept. A Privacy Impact Assessment will be carried out before we undertake any "high risk" processing activities.

Data processors
A 'data processor' is a natural or legal person, public authority, agency or any other body that is not a data user and which processes personal data on behalf of our business and on our instructions. Employees of data controllers are excluded from this definition.

Data protection legislation places obligations on data processors. This applies whether the personal data is collected directly from the data subjects, or from another source.

Data users
'Data users' are those employees, workers or contractors whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy and any applicable data security procedures at all times.

Data subjects
A 'data subject' is any living individual whose personal data is held by us. It includes not only employees, workers and contractors but also anyone who gives us their personal data to enable us to sell to them, provide services to them, process financial transactions or market to them by sending information by email, post or text. Data subjects do not have to be a UK national or resident.

2. Data protection principles

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purposes and shall not be further processed in any manner incompatible with that purpose
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
- not be kept for longer than is necessary for the purposes for which it is processed
- be processed securely and be protected against unauthorised or unlawful processing, loss, damage or destruction by using appropriate technical and organisational measures.

These principles apply to obtaining, handling, processing, transporting and storing personal data. We are accountable for these principles and must be able to show that we are compliant. Employees, workers and contractors who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.

3. Conditions for processing data

The processing of **personal data** will only be lawful if it satisfies at least one of the following conditions:

- with consent of the data subject
- necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract
- necessary for compliance with a legal obligation to which the data controller is subject
- necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- necessary for the purposes of the legitimate interest of the data controller or the party to whom the data is disclosed.

Any processing of **special categories data** must satisfy at least one of the following conditions:

- explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement
- necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent
- processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim, provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- data manifestly made public by the data subject

- necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- necessary for reasons of substantial public interest on the basis of EU or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures
- necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional
- necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

The obligations on data processors and data users apply whether the personal data is collected directly from the data subjects themselves (for example, by completing a form or by corresponding with us by mail, phone, email or otherwise), or whether we collect it from another source (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for specific purposes as permitted by legislation and in a manner that is compatible with those purposes. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

4. Responsibilities

Data Protection Manager
Our Data Protection Manager is responsible for reviewing this policy and updating the Directors on our data protection responsibilities and any risks in relation to the processing of data.

IT Manager
Our IT Manager is responsible for reviewing our systems, equipment and electronic storage and for ensuring that all data users are provided with equipment and software that sufficiently protects our data. The IT Manager should advise the Directors on any risks in relation to the processing of data.

HR Manager
Our HR Manager is responsible for ensuring that our HR and payroll records are compliant, and for ensuring that all data users (including new employees) are adequately trained. The HR Manager should advise the Directors on any risks in relation to the processing of data.

Payroll Manager
Our Payroll Manager is responsible for ensuring that our client payroll records are compliant, and for ensuring that all data users are adequately trained. The Payroll Manager should advise the Directors on any risks in relation to the processing of data.

Employees, workers and contractors
All employees, workers and contractors must ensure that, in carrying out their duties for us (or providing services to Accapita), they comply with our obligations under the 2018 Act. In addition, each individual is responsible for:

- checking that any personal data that they provide to us is accurate and up to date

- informing us of any changes to information previously provided, eg change of home or email address or phone number, marital status or civil partnership, bank details etc

- checking any information that we may send out from time to time, giving details of information that is being kept and processed

- ensuring that if, as part of their responsibilities, they collect information about other people or about other employees, they comply with this policy. This includes ensuring that information is processed in accordance with the 2018 Act, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

Employees are required to comply with our rules on IT security, as set out in our IT policy and other instructions from time to time. Settings that are designed to minimise the risk of a data breach (such as screensavers, automatic locking, password protection etc) must not be tampered with, changed or removed.

The 2018 Act applies not only to records relating to our employees, but also to the records of any client. Personal data should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or saved electronically (for example in emails, current or deleted) are potentially disclosable in the event of a subject access request (see below).

5. The rights of data subjects

Data subjects have the right to:

- have information about what personal data we process, how and on what basis as set out in this policy.
- access their own personal data by way of a subject access request (see below) and correct or remove any inaccuracies in their personal data, by contacting the Data Protection Manager.
- request that we erase their personal data where we were not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected, or it was processed in breach of the GDPR. To do so they should contact the Data Protection Manager. Data subjects who request that their personal data is corrected or erased or who are contesting the lawfulness of our processing, can apply for its use to be restricted while the application is made. To do so they should contact the Data Protection Manager.
- object to data processing where we are relying on a legitimate interest to do so and they think that their rights and interests outweigh our own and they wish us to stop.

- object if we process their personal data for the purposes of direct marketing.
- receive a copy of their personal data and to transfer their personal data to another data controller. We will not charge for this and will in most cases aim to provide this within one month.
- be notified of a data security breach concerning their personal data.

With some exceptions, they have the right not to be subjected to automated decision-making for the purposes of evaluating matters relating to them, such as conduct or performance, and which will significantly affect them.

In most situations we will not rely on consent as a lawful ground to process personal data. If we do however request consent to the processing of personal data for a specific purpose, the data subject has the right not to consent, or to withdraw their consent later. To withdraw consent, they should contact the Data Protection Manager.

Any data subject has the right to complain to the Information Commissioner if they have concerns about the way in which their data is being handled. They can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

6. Processing the personal data of our employees, workers and contractors

We collect and use the following types of personal data about our employees, workers and contractors:

- recruitment information such as an application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments
- name, home address, contact details and date of birth
- contact details for emergency contacts
- gender
- marital status or civil partnership and family details
- information about the contract of employment (or services) including start and end dates of employment; role and location; organisation charts; working hours; employment history including details of promotion/transfer/relocation/demotion; salary (including details of previous remuneration); pension; benefits and holiday entitlement
- bank or building society details and information in relation to tax status including national insurance number
- identification documents including visa (where applicable), passport and driving licence and information in relation to immigration status and right to work for us
- information relating to disciplinary or grievance investigations and proceedings involving the data subject (whether or not they were the main subject of those proceedings)
- information relating to performance and behaviour at work, including performance reviews and promotion prospects
- educational background, areas of expertise, training records
- electronic information in relation to use of our IT systems/swipe cards/telephone systems
- images (whether captured by photograph or video)

- records relating to holiday, sickness and other leave (including maternity, adoption, paternity, parental, shared parental leave, time off for dependants etc), working time records and other management records
- health and safety records
- correspondence between the individual and us
- any other category of personal data which we may notify the individual of from time to time.

We may receive and/or retain this information in various forms (whether in writing, electronically, verbally or otherwise).

The legal grounds on which we collect and process this data include:

- performing the contract of employment (or services) between us
- complying with any legal obligation or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if the interests and rights of the data subject do not override ours (or theirs). Data subjects have the right to challenge our legitimate interests and request that we stop this processing.

We may process personal data for the above purposes without the data subject's knowledge or consent. We will not use any personal data for an unrelated purpose without telling the data subject about this and the legal basis that we intend to rely on for processing it. Information about an individual will only be kept for the purpose for which it was originally provided. Employees and managers must not collect data that is simply "nice to have" nor use data for any purpose other than what it was provided for originally.

We process personal data in various situations during recruitment, employment (or engagement) and also following termination of employment (or engagement). This information is used for a variety of administration and management purposes, including payroll and benefits administration; facilitating the management of work and employees; performance and salary reviews; complying with record keeping and other legal obligations. For example, we use the above personal data:

- to decide whether to employ (or engage) you
- to decide how much to pay you, and the other terms of your contract with us
- to check you have the legal right to work for us
- to carry out the contract between us including where relevant, its termination
- to train you and review your performance
- to decide whether to promote you
- to decide whether and how to manage your performance, absence or conduct
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability
- to monitor diversity and equal opportunity
- to monitor and protect the security (including network security) of our business, of you, our other staff, clients and others
- to monitor and protect the health and safety of you, our other staff, customers and third parties
- to pay you and provide pension and other benefits in accordance with the contract between us
- to pay tax and national insurance
- to provide a reference upon request from another employer

  - to monitor compliance by you, us and others with our policies and our contractual obligations
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us
- to answer questions from insurers in respect of any insurance policies which relate to you
- to run our business and plan for the future
- to prevent and detect fraud or other criminal offences
- to defend our business in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure and
- for any other reason which we may notify you of from time to time.

We do not take automated decisions about a data subject using personal data or use profiling in relation to them.

Special categories data
Special categories data includes details such as physical or mental health or condition (this typically includes pre-employment health questionnaires; records of sickness absence and medical certificates (including self-certification of absence forms); night worker assessments; VDU assessments; noise assessments and any other medical reports) and any criminal proceedings or convictions.

We may hold and use any of these special categories data in accordance with the law. For example, we can do so if we have the individual's explicit consent. If we ask for consent to process any special categories data, we will explain the reasons for our request. Data subjects do not need to consent and can withdraw consent later if they choose by contacting our Data Protection Manager.

However, we do not need consent to process special categories data when we are processing it for the following purposes:

- where it is necessary for carrying out rights and obligations under employment law
- where it is necessary to protect the individual's vital interests or those of another person where either are physically or legally incapable of giving consent
- where the data has been made public
- where processing is necessary for the establishment, exercise or defence of legal claims and
- where processing is necessary for the purposes of occupational medicine or for the assessment of the individual's working capacity.

We may also store and process special categories data in relation to:

- sickness absence, health and medical conditions to monitor and manage absence, assess fitness for work, to pay benefits such as contractual and Statutory Sick Pay, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety

7. Processing the personal data of our clients

In supplying the professional services to you as our client we may collect the following data :

- Name
- Address
- Phone numbers
- Email address
- Date of birth
- Marital status
- Bank account details,
- Employee details - national insurance numbers, salary details

We keep the personal data of our clients for the following purposes :

- to enable us to supply professional services to you as our client
- to fulfil our obligations under relevant laws in force from time to time (e.g. the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLR 2017"))
- to comply with professional obligations to which we are subject as a member of the Association of Chartered Certified Accountants
- to use in the investigation and/or defence of potential complaints, disciplinary proceedings and legal proceedings
- to enable us to invoice you for our services and investigate/address any attendant fee disputes that may have arisen
- to contact you about other services we provide which may be of interest to you if you have consented to us doing so

8. Processing with consent (marketing and other data)

Through our marketing we will collect your name and e-mail address so that we can send you our newsletters, budget summaries and bulletins that you have requested.

In addition to the above, we also retain personal data relating to potential clients and suppliers. Where data is collected for marketing or purchasing purposes, this is done only with the data subject's specific, freely-given consent. At the time of collecting the data, the data subject will be informed of the use to which the data will be put and its retention period, via a privacy notice.

Such data subjects may withdraw their consent at any time and may ask to view their data, or to have it rectified or erased. Where a data subject requests correction, we will aim to comply with this promptly (within a month); where a data subject requests erasure, we will also comply with this promptly (within a month) provided there are no legitimate grounds for retaining it. This extends to back up copies and also to data which we have disclosed to third parties.

If we collect personal data directly from data subjects, we will inform them (via a "privacy notice") of:

- our identity and our contact details
- the purpose or purposes for which we intend to process that personal data and the legal basis of that processing
- the types of third parties, if any, with which we will share or to which we will disclose that personal data
- any countries outside the EEA to which we will transfer their personal data
- the period for which their personal data will be stored or the criteria for determining

that period
- their right to request access to and rectification or erasure of their personal data or to restrict or object to processing
- their right to data portability
- their right to withdraw any consent they have given at any time
- their right to lodge a complaint with a supervisory authority
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- the existence of automated decision-making and any profiling and the reasoning for it and the envisaged consequences of such processing for the data subject.

If we receive personal data about a data subject from other sources and we become a data controller in respect of that data, we will provide the data subject with this information as soon as possible thereafter.

We will also inform data subjects whose personal data we control that we are the Data Controller with regard to that data.

Records of consent will be kept to enable us to demonstrate evidence of this if required.

Generally, if we receive a request from any person that they wish to exercise any data protection right, the Data Protection Manager should be contacted in the first instance.

9. Handling personal data

We will, through appropriate management and the use of strict criteria and controls:

- fully observe the conditions concerning the fair collection and use of personal data
- specify the purpose for which the data is collected and processed
- collect and process data only to the extent that it is needed to fulfil our operational needs or legal requirements
- endeavour always to ensure the quality of data used and that it is accurate, including checking the accuracy of any personal data at the point of collection and at regular intervals afterwards
- not keep information for longer than required (operationally or legally) for the purpose or purposes for which it was collected – to do this, we will establish time limits to ensure we store data for the strict minimum and schedule periodic reviews and erasure of all data which is no longer required
- take all reasonable steps to correct any inaccurate or out of date data without delay
- always endeavour to safeguard personal data against unlawful or unauthorised access, loss or use, by the use of appropriate physical and technical means from the point of collection to the point of destruction (ie keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords which, where possible, are changed periodically, and ensuring that individual passwords are not easily compromised)
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised.

10. Sharing personal data

We may share personal data with group companies or our contractors and agents to carry out our obligations under our contract with our employees, workers and contractors or for our legitimate interests. We also have a legal obligation to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings (Protection of Employment) Regulations (TUPE). In addition, we may also disclose personal data to third parties in line with a proposed sale or transfer of part of all of the business.

References that disclose personal information will not be provided to any third party without the data subject's prior consent (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body). However, we may disclose or share personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, clients, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

We may also share personal data we hold with selected third parties for the following purposes: pension providers and our insurers.

Any data sharing with external parties will be carried out under a written agreement, setting out the scope and limits of the sharing and ensuring that the data processor has adequate data security measures in place. We require those parties to keep personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process such personal data for the lawful purpose for which it has been shared and in accordance with our instructions.

11. Transferring personal data to a country outside the EEA

We do not send personal data outside the European Economic Area.

12. Publication of personal data

Any individual who has good reason for wishing their details not to be included in information contained within externally circulated publications such as brochures and other sales and marketing literature, or included on our website, should contact the Data Protection Manager.

13. Updating personal data

From time to time we may ask our data subjects to review and update the personal information we hold about them. However we prefer that individuals do not wait until asked to update this information, but inform us immediately of any significant change(s).

Data retention periods are specified in our data retention policy, a copy of which is available on is available on request by e-mailing privacy@accapita.com.

14. Our rules regarding the processing of personal data

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. Access to personal data is strictly controlled and limited to those who are entitled to see it as part of their duties.

Everyone who works for, or on behalf of, Accapita has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and our data retention policy. All those who manage and handle personal data will be trained to do so and appropriately supervised.

Our rules on the processing of personal data include:

- Only people who are authorised to use the data may access it. Data users should only gather, store, access or process personal data covered by this policy if they need it for the work they do for, or on behalf of Accapita and only if they are authorised to do so. The data should only be used for the specified lawful purpose for which it was obtained, unless the individuals concerned are notified of any additional or different purposes to that carried on previously.
- Data users should not share personal data informally.
- Data users should not share personal data with unauthorised people. When receiving telephone enquiries for information, we will only disclose personal data we hold on our systems if the following conditions are met:
    - we will check the caller's identity to make sure that information is only given to a person who is entitled to it
    - we will suggest that the caller puts their request in writing if we are unsure about the caller’s identity or cannot check this.
- If disclosing personal data to a third party (for example employment references), data users should consider whether the data subject(s) should be informed of the disclosure, even if they have already given their prior consent to this. Where requested to disclose personal data to a third party and such disclosure is not a routine activity (eg disclosures to the police, to the press or to mortgage providers for reference purposes), the request should be forwarded to a Partner before making such disclosure, as in some cases it will be necessary to obtain the consent of the individual concerned.
- Data users should regularly review and update personal data which they have to deal with for work. If a data subject notifies them that some personal data is inaccurate, this should be amended if it is agreed that the data is inaccurate. If it is not agreed that the data is inaccurate then it should be left un-amended but a note of the data subject's views should be included with the data.
- Unnecessary copies of personal data should not be made and any copies should be kept and disposed of securely. This includes emails (either sent or received). Personal data which is excessive or irrelevant should not be retained.
- Managers should not to retain their own copies of personal data, but should use our central storage system. This is particularly important in terms of complying with subject access requests.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and with the prior authorisation of the Data Protection Manager, who will check that appropriate security precautions for the transfer of data are in place.
- Data on computers and in paper records should be maintained as accurately and securely as possible.

- Personal data should not be saved to data users' own personal computers or other devices.
- Data users should ask for help from our Data Protection Manager if they are unsure about data protection or if they notice any areas of data protection or security we can improve upon.
- A data user who receives any request or complaint from any individual in relation to the processing of their data should notify the Data Protection Manager immediately.
- Any rules, procedures or instructions which we may issue from time to time to ensure the security of information, and the safe destruction of such information, should be observed, in particular, the security procedures set out in our IT policy and in any other relevant policies or guidelines.

Any deliberate or negligent breach of this policy by employees may result in disciplinary action in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.

15. Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

We provide appropriate organisational, physical and technical security arrangements in relation to all personal data held on employees. The level of security used should be appropriate to the nature of the data and the harm that could result if it is used in an unauthorised manner.

All hard copy personnel files are kept in a locked cabinet in the HR Manager's office and are not to be removed from that location. Other information that is stored electronically has appropriate levels of authorisation which prevent unauthorised access.

Managers have access to the personnel records of the employees that report directly to them, but not to the files of other employees. Managers are required not to retain their own copies of personal data, but to use our central storage system.

Data stored on laptops, smartphones and any other electronic equipment that is removed from our offices must be password protected.

All employees and workers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Third party processors (such as our pension provider) will be required to provide sufficient guarantees for their data security measures and compliance with them. A written contract will be in place with each supplier which requires them to dispose of data securely and to provide suitable evidence of this. Checks will be made to ensure that secure data disposal facilities are in place and regular monitoring will take place.

In particular:

- Data on computers and in paper records should be maintained as accurately and

securely as possible.
- Our IT security procedures should be followed at all times. This includes ensuring that individual monitors or laptop screens do not show confidential information to passers-by and that users log off from their PCs (or lock their screens) when leaving them unattended. Laptops should never be left unattended unless shut down and locked in a secure cabinet.
- Computer discs, flashdrives and memory sticks and paper records should be properly secured at all times.
- Data users should use strong passwords. Computer passwords should not be disclosed to anybody other than the relevant authorised user.
- Where appropriate, we will consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Drawers, filing cabinets and cupboards should be locked if they contain confidential data of any sort.
- Paper with personal data should not be left lying about.
- All hard copy personnel files are kept in a locked cabinet in the HR Manager's office and are not to be removed from this location. Other information that is stored electronically has appropriate levels of authorisation which prevent unauthorised access.
- Personal data should not be taken away from our premises without authorisation from a manager or the Data Protection Manager. Data retained on laptops, smartphones and any other electronic equipment that is removed from our offices must be password protected.

Any employee who discovers personal or sensitive data in an inappropriate place (for example unknowingly sent to the wrong printer) should immediately pass this to a Partner, ensuring that its contents are not revealed to anyone else.

16. Subject access requests

All individuals who are the subject of personal data held by us are entitled to:

- be informed of what personal data we hold about them and why, whether it will be given to any other organisations or people (such as third party outsourcers) and for how long it will be retained
- be given details of the source of the data (where this is available and it was obtained from someone other than the data subject)
- be informed of how to gain access to it
- be informed of how to keep it up to date
- have inaccurate personal data corrected or removed.

The following procedure is in place to deal with any data access requests (internal or external) to ensure that such enquiries are dealt with promptly and courteously:

- All data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them and to get copies of that data. This request must be made in writing to the Data Protection Manager, indicating the information or processing activities to which the request relates.
- If you receive such a request (whether an employee or a third party, and whether by letter or email) you should forward it (together with all information in your possession as to the nature and circumstances of the request, including the date it was made) immediately to the Data Protection Manager who will coordinate a response. You should not respond directly to the individual concerned, other than to thank them for their request and to confirm that their

request is being dealt with. Copies of personnel files or other personal data should not be provided.

- We aim to comply with requests for access to personal information as quickly as possible, but we must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months. In such cases, the reason for the delay will be explained in writing to the individual making the request.
- If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party. We may also withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others'.
- Where possible, data subjects will be given access to the source of the personal data.
- A copy of the personal data that is being processed will normally be provided in the same format as the request was made.
- At the time of providing the information, we will confirm that the personal data is being processed; together with details of the recipients of the data (including data transfers); the data categories; where the personal data is being processed; the purpose of the processing, any automated decision-making; the envisioned consequences of the processing and the data subject's rights regarding rectification, erasure, restriction and how to make a complaint.
- There is no fee for making a SAR. However, if the request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to the request.
- If personal details are inaccurate, they will be amended promptly upon request.
- Unless we are under a legal obligation to release data, or the individual has given us permission, personal information will only be released to the individual to whom it relates.
- Any employee, worker or contractor who is in doubt regarding a subject access request should check with the Data Protection Manager.

17. Retention and destruction of personal data

Personal data will be kept in line with our document retention policy, a copy of which is available on our website. This aims to ensure the timely, secure and effective disposal of personal data and records, in all formats, once legislative and business use has been concluded, and also to ensure that it is safe from unauthorised access or accidental destruction. All employees, workers and contractors are responsible for ensuring that information is not kept for longer than necessary shredded or disposed of securely once it is no longer required for the purpose for which it was originally collected. Any personal data relating to any pending or actual litigation, claim, investigation, negotiation, audit, Data Protection or Freedom of Information enquiry must be retained until the issue is resolved, even if the retention period has expired.

Documents containing any personal data will be disposed of securely. Paper copies will be cross-shredded (not disposed of directly into a normal bin or recycling bin). Electronic data may be deleted automatically, or may be encrypted and stored in a form that no longer identifies the individual.

All backup copies, security copies, preservation copies and duplicate copies of all records authorised for destruction should be destroyed at the same time or as soon as practical afterwards.

Records of automated destruction of data will be kept indefinitely for audit, evidential and accountability purposes. This will state the dates the records were created and closed, the volume of data, the format, the reason for destruction, the method of destructions and the destruction date.

Information stored on obsolete electronic equipment (desktops, laptops and other devices) or on equipment that is to be reallocated to someone else will be erased prior to the equipment being sold, disposed of or reallocated to other employees.

18. Monitoring compliance

A copy of this policy also be given to any third parties to whom we outsource any data processing.

We will maintain appropriate documentation relating to how personal data is collected, processed, retained and destroyed to provide evidence that we are complying with our duties under the GDPR.

Periodic audits of files, systems and processes (including security measures) will take place on a regular basis to identify any areas of risk and appropriate actions.

Managers should be aware that whenever they record or use personal data (including emails, performance reviews, interview notes, disciplinary investigations, witness statements or personal information and contact lists), the material recorded may have to be disclosed to the individuals to which it relates if a subject access request is made. They should therefore ensure that all data is recorded in a business-like manner and does not include comments that could be considered offensive or inappropriate.

Any breach of this policy on the part of an employee will be taken seriously and may result in disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with a partner.

19. Training and equipment

Appropriate training will be provided to all data users to ensure firstly, that they are aware of their obligations under the GDPR and of our own policies and procedures for ensuring compliance with this, and secondly to ensure an ongoing high level of awareness of data protection issues.

All data users will be trained on the risks of inadvertent breaches of security and of our data security procedures.

Equipment will also be checked on a regular basis to ensure that security software is installed and up to date, and all other software is up to date and data backed up appropriately.

20. Data security breaches

All organisations are required to report any data security breach to the Information Commissioner's Office without undue delay and at the latest within 72 hours of detection, unless it is unlikely to result in a risk to the rights and freedoms of the data

subjects affected. A serious data security breach is described as one

- that could cause significant threat of harm to individuals
- where large volumes of data are involved (generally 1,000 people)
- where sensitive data is involved, such as financial or medical records or unencrypted personal data.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also have to notify those concerned directly in most cases –for example, this would apply if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Therefore, if you are aware of a confirmed or suspected data security breach you must contact a partner immediately and keep any evidence you have in relation to the breach.

Our Data Protection Manager is responsible for deciding whether a breach should be notified, and for making such notification if applicable.

All breached must be recorded, including those where there was no obligation to notify the ICO.

21. Related policies and documents

We also have the following related policies and documents: data access request form; data retention policy; IT and computer use policy; privacy notices in place in respect of job applicants, clients, suppliers and other categories of data subject.

22. Review of this policy

This policy will take effect from 25 May 2018. It will be reviewed on a regular basis following its implementation and may be changed from time to time.

Any queries or comments about this policy should be addressed to a partner.