Data Protection Policy

1. Introduction

The organisation takes the security and privacy of data subjects seriously. We need to gather and use information or 'data' about data subjects as part of our business and to manage our relationship with data subjects. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') in respect of data privacy and security. We have a duty to notify data subjects of the information contained in this policy.

This policy applies to customers, service users, job applicants, current and former employees, workers, volunteers, apprentices and consultants. If a person falls into one of these categories, then they are a 'data subject' for the purposes of this policy. Data subjects should read this policy alongside the contract of employment (or contract for services) and any other notice we issue to data subjects from time to time in relation to data.

The organisation will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from Senior Management Team. We will only hold data for as long as is necessary.

The organisation is a 'data controller' for the purposes of personal data. This means we determine the purpose and means of the processing of personal data.

This policy explains how the organisation will hold and process personal data information. It explains data subjects' rights and obligations when obtaining, handling, processing or storing personal data in the course of working for or on behalf of, the Organisation.

This policy does not form part of the contract of employment (or contract for services) and can be amended by the Organisation at any time. It is intended this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the organisation intends to comply with the 2018 Act and the GDPR.

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.
- 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.

The organisation is accountable for these principles and must be able to show we are compliant.

Reviewed Date: July 2024
Next Review: July 2027

3. Defining Personal Data

'Personal data' means information which relates to a living person who can be identified from the 'data subject' on its own or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of the person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

The personal data might be provided to us by data subjects or someone else (such as a former employer, medical professional or a credit reference agency) or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by a data subjects' manager or other colleagues.

We will collect and use the following types of personal data about data subjects:

- Recruitment information such as the application form, CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.
- Contact details and date of birth.
- Emergency contacts information.
- Gender.
- Marital status and family details.
- Information about the contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits, holiday entitlement, services provided and services received.
- Bank details and information in relation to tax status including National Insurance number.
- Identification documents including passport and driving licence and information in relation to immigration status and right to work in the UK.
- Information relating to disciplinary or grievance investigations and proceedings (whether or not the data subject was the main subject of those proceedings).
- Information relating to performance and behaviour at work.
- Training records.
- Electronic information in relation to use of IT systems/swipe cards/telephone systems.
- Images (whether captured on CCTV, by photograph or video).
- Any other types of personal data which data subjects hold for employees/workers/consultants.
- Any other category of personal data which we may notify data subjects of from time to time.

4. Defining Special Category Data

'Special category data' are types of personal data consisting of information as to:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade Union membership.
- Genetic or biometric data.
- Health.
- Sex life and sexual orientation.
- Criminal convictions and offences.

We may hold and use any of these special categories of personal data in accordance with the law.

5. Defining 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.
- Restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6. How the Organisation Will Process Personal Data

The organisation will process personal data (including special category personal data) in accordance with obligations under the 2018 Act.

We will use personal data for:

- Performing the contract of employment (or services) between us.
- Complying with any legal obligation.
- If it is necessary for legitimate interests (or for the legitimate interests of someone else). However, this can only be done if data subjects' interests and rights do not override the organisations (or theirs). Data subjects have the right to challenge legitimate interests and request we stop processing their data.

We can process personal data for these purposes without data subjects' knowledge or consent. We will not use personal data for an unrelated purpose without telling data subjects about it and the legal basis that we intend to rely on for processing it.

If data subjects choose not to provide us with certain personal data, they should be aware we may not be able to carry out certain parts of the contract between us. For example, if data subjects do not provide us with bank account details, we may not be able to pay them. It might also stop us from complying with certain legal obligations and duties which we have such as

to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability data subjects may suffer from.

7. Data Processing Examples

We have to process personal data in various situations during recruitment, employment (or engagement of contract for services) and following termination of data employment (or engagement).

For example:

- To decide whether to employ (or engage) someone or a contractor.
- To decide how much to pay and the other terms of contract.
- To check data subjects have the legal right to work in the UK.
- To carry out the contract between us including where relevant, its termination.
- Training and reviewing performance.
- To decide whether or not to promote someone.
- To decide whether and how to manage performance, absence or conduct.
- To carry out a disciplinary or grievance investigation or procedure in relation to data subjects or someone else.
- To determine whether we need to make reasonable adjustments to the workplace or role.
- To monitor diversity and equal opportunities.
- To monitor and protect the security (including network security) of the organisation, of every data subject.
- To monitor and protect the health and safety of every data subject.
- To pay data subjects and provide pension and other benefits in accordance with the contract.
- To pay tax and National Insurance.
- To provide a reference upon request from another employer.
- To pay trade union subscriptions.
- To monitor compliance by data subjects, us and others with our policies and contractual obligations.
- To comply with employment law, immigration law, health and safety law, tax law and other laws which affect the organisation.
- To answer questions from insurers in respect of any insurance policies which relate to data subjects.
- To running the business and planning for the future.
- The prevention and detection of fraud or other criminal offences.
- To defend the organisation in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure.
- For any other reason which we may notify data subjects of from time to time.

The organisation will only process special category data in certain situations and in accordance with the law. For example, with explicit consent. If required, the organisation will request consent to process special category data and explain the reasons for the request. Data subjects do not need to consent and can withdraw consent later if they choose.

Consent to process special category data is not required when it is processed for the following purposes:

- Where it is necessary for carrying out rights and obligations under employment law.

- Where it is necessary to protect data subjects' vital interests or those of another person where they are physically or legally incapable of giving consent.
- Where data subjects have made the data public.
- Where processing is necessary for the establishment, exercise or defence of legal claims.
- Where processing is necessary for the purposes of occupational health or for the assessment of working capacity.

The organisation may process special category in relation to:

- Race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities.
- Sickness absence, health and medical conditions to monitor absence, assess fitness for work, to pay benefits, to comply with legal obligations under employment law including to make reasonable adjustments and to support health, safety and wellbeing.
- Trade union membership to pay any subscriptions and to comply with legal obligations in respect of trade union members.

The organisation does not make automated decisions about data subjects using personal or special category data or use profiling.

8. Sharing Personal Data

The organisation may share personal data with group companies or contractors and agents to fulfil obligations under contract with data subjects or for legitimate interests.

We require those companies to keep data subjects' personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send personal data outside the European Economic Area. If this changes data subjects will be notified of this and the protections which are in place to protect the security of data will be explained.

9. How All Staff Should Process Personal Data

Everyone who works for, or on behalf of, the organisation has responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy.

The Data Protection Officer/Data Protection Manager is responsible for reviewing this policy and updating the Board on the organisation's data protection responsibilities and any risks in relation to the processing of data. Staff should direct any questions in relation to this policy or data protection to this person.

Staff should only access personal data covered by this policy if they need it for the work they do, or on behalf of the organisation and only if authorised to do so. Staff should only use the data for the specified lawful purpose for which it was obtained.

Staff must:-

- Not share personal data informally.

- Keep personal data secure and not share it with unauthorised people.
- Regularly review and update personal data which they deal with including deleting any personal data no longer required for work purposes.
- Not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- Use strong passwords as stipulated by external IT suppliers.
- Lock computer screens when not at their desk.
- Encrypt personal data before being transferred electronically to authorised external contacts.
- Anonymise data or use separate keys/codes so the data subject cannot be identified.
- Not save personal data to personal computers or other devices.
- Never transfer personal data outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.
- Lock drawers and filing cabinets.
- Not leave paper with personal data lying about.
- Take personal data away from organisation's premises without authorisation from their line manager or the Data Protection Officer.
- Shred and dispose of personal data securely when finished with it.
- Ask for help from the Data Protection Officer/Data Protection Manager if unsure about data protection or if staff notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken in accordance with the disciplinary procedure.

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

10. Homeworkers

For any member of staff who works from home for part or all of their contractual hours whether defined as a "homeworker" under the HSE definition or not, all terms of this policy remain and apply at all times. Any breach of this policy may result in the disciplinary procedure being instigated.

All devices including PCs, laptops, tablets, smart televisions and smart phones must be secured when not in use. If devices are accessible by other household members, access to any material, programme, application, website, document and any other data which may fall under the terms of this policy must be password protected.

In the circumstance of shared or sole access to devices, it remains essential no passwords are auto-filled, auto-completed or stored.

Physical information such as paperwork, files or otherwise containing personal data must be kept secure when not in use. A lockable case, cabinet, drawer, briefcase or otherwise should be utilised to ensure access to personal data cannot be obtained by any other member of the household or any potential visitor.

11. Dealing with Data Breaches

The organisation has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of data subjects or someone else) evidence of the breach must be taken and retained. If the breach is likely to result in a risk to the rights and freedoms of individuals then, the organisation must also notify the Information Commissioner's Office within 72 hours.

If staff become aware of a data breach, they must contact their line manager immediately and keep any evidence in relation to the breach.

12. Subject Access Requests

Data subjects can make a 'subject access request' ('SAR') to find out the information held about them. This request must be made in writing. If staff receive such a request data subjects should forward it immediately to their line manager who will coordinate a response.

If staff would like to make a SAR in relation to their own personal data, they should make this in writing to their line manager. The organisation must respond within 30days 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.

There is no fee for making a SAR. However, if the request is manifestly unfounded or excessive, the organisation may charge a reasonable administrative fee or refuse to respond to the request.

13. Data Subjects Rights

Data subjects have the right to information about what personal data we process, how and on what basis as set out in this policy.

Data subjects have the right to access their own personal data by way of a subject access request.

Data subjects can correct any inaccuracies in personal data. To do so, data subjects should contact their line manager.

Data subjects have the right to request the organisation erase 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. To do so, data subjects should contact their line manager.

While data subjects are requesting personal data is corrected or erased or are contesting the lawfulness of processing, data subjects can apply for its use to be restricted while the application is made. To do so, data subjects should contact their line manager.

Data subjects have the right to object to data processing where we are relying on a legitimate interest to do so and data subjects think their rights and interests outweigh our own and they wish us to stop.

Data subjects have the right to object if we process personal data for the purposes of direct marketing.

Data subjects have the right to receive a copy of their personal data and to transfer personal data to another data controller. We will not charge for this and will in most cases aim to do this within 30 days.

With some exceptions, data subjects have the right not to be subjected to automated decision-making.

Data subjects have the right to be notified of a data security breach concerning their personal data.

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, data subjects have the right not to consent or to withdraw consent later. To withdraw consent, data subjects should contact their line manager.

Data subjects have the right to complain to the Information Commissioner. Data subjects 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). This website has further information on data subjects' rights and our obligations.

DATA SECURITY

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means only those who are authorised to use the data can access it.
- Integrity means personal data should be accurate and suitable for the purpose for which it is processed and takes all reasonable steps to ensure inaccurate personal data is rectified or deleted without delay.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- Entry controls - Anyone not recognised in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

Methods of Disposal

Paper documents should be shredded. Electronic data stored on pen drives, CDs or otherwise should be destroyed when they are no longer required.

Equipment

Data users should ensure individual monitors do not show confidential information to passers-by and they log off from their PC whenever it is left unattended.

Retention Periods

Different types of data will be retained for different periods of time:

- Personal customer/supporter data: Personal data will be held for as long as the individual is a customer of the company plus 7 years for any financial information pertaining to this customer/supporter.
- Personal employee data: General employee data will be held for the duration of employment and then for 5 years after the last day of contractual employment. Employee contracts will be held for 5 years after last day of contractual employment.
- Personal tax payments will be held for 7 years.
- Records of leave will be held for 7 years.
- Recruitment details: Interview notes of unsuccessful applicants will be held for 1 years after interview. This personal data will then be destroyed.
- Health and Safety: 5 years for records of major accidents and dangerous occurrences.
- Operational data: Most company data will fall in this category. Operational data will be retained for 7 years.
- Critical data including Tax and VAT: Critical data must be retained for 7 years.