Data Protection Policy

This policy applies to all employees of the Group. For the purposes of this policy the definition of employee/employees is as follows:

‘Any director, salaried staff member, zero hours worker, personal service company providing a contractor for a service offered by the Group, any sole trader providing a service offered by the Group, and any other individual who is authorised by the Group to access and use data records (paper or electronic) controlled by the Group.’

Purpose

The purpose of this policy is to reduce the risk to the Group, the employees, customers, clients, and others, of the Group accidentally disclosing personal data, or it being used for any purpose without suitable authorisation.

Background

The UK Data Protection Act of 2018 and the UK General Data Protection Regulation (UKDPA and GDPR) are the laws and regulations that govern the collection, access, and use of personal data.

Personal data is defined by the Information Commissioner’s Office (ICO), that enforces the rules and regulations surrounding personal data, as:

Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Anyone processing personal data MUST comply with the six lawful bases for processing and recognise the eight rights of data subjects. Both the bases and rights are explained in the appendices to this document.

Data Protection Policy

Aims and Objectives

By enforcing this policy, the Group aims to reduce the risk that personal data of any person is used inappropriately or illegally, and that the risks of 'attacks' on the Group by malicious third parties wishing to access/steal/amend/delete/ransom personal data held by the Group are minimised.

However, the Group's overriding aim and objective is to ensure that personal data that it collects on behalf of data subjects is managed, stored, deleted (or retained), and accessed only in line with the UK laws and Group policies relating to personal data, and that the risks of accidental or malicious leakage of data is minimised (realising that it is not possible to totally eradicate this risk).

Responsibilities

As part of its commitment to the protection of personal data, the Group has appointed a dedicated Data Protection Officer (DPO) whose responsibilities are to ensure that data is protected, that employees have suitable training, and that potential risks are minimised wherever possible.

The DPO takes the lead in sourcing and managing suitable training, with the support of the People & Culture team. This training is mandatory for all on an annual basis, except the sole traders and personal service company appointed contractors (who, due to legislation under HMRC rule IR35 are responsible for their own training, however the DPO will offer training – potentially in 2025 for a small fee to be agreed – if they are unable to provide adequate evidence of valid training elsewhere).

All existing eligible employees will be expected to take and pass their training during the month of May or can expect to have their access to systems removed on 1 June if they have not complied, and do not have mitigating circumstances that may be considered.

Employees have responsibilities to use, manage, delete (or retain where relevant) data and some examples are listed below (this is not an exhaustive list):

- Always adhere to the lawful bases and data subject rights as detailed in the appendices
- Only access the data required to do their jobs
- Only use Group approved resources and systems (laptops, portable storage, security software etc.) to process personal data. There are further rules explained elsewhere for those who use their own device for work purposes (the **Bring Your Own Device – BYOD – policy**)
- Never share personal data informally
- Always keep personal data secure, taking sensible precautions, and following the Group's **Information Security policy**
- Always use strong passwords and change them regularly, and never share them with anyone else, and follow the guidance in the **Password policy**
- Never disclose personal data (internally or externally) about a data subject, without have the correct authorisation to do so
- Always keep personal data up to date, and if found to be out of date, or no longer needed, follow the guidance in the **Data Retention and Deletion policy**
- When in any doubt, always request help from the DPO
- Always be aware that there are eight data subject rights that data subjects can request to use – and if a request is made it must be passed immediately to the DPO
- If there is a data breach (or a suspected one) this must be reported to the DPO for further investigation, following the guidance laid out in the **Data Breach Process**

PECR Compliance

Marketing communications must comply with the Privacy and Electronic Communications Regulations (PECR), including obtaining explicit consent for electronic marketing (emails, texts, calls etc.).

The use of cookies and similar technology must comply with PECR, including the provision of clear information, and obtaining consent where required.

Data Protection Policy

Security measures must be in place to protect the privacy of customers using electronic communications services, including traffic and location data, itemized billing, and directory listings.

Additional guidance has been issued to Marketing regarding the collection of images (photographs and video – individual or group) which must also be adhered to in addition to PECR compliance

Failure to adhere to this policy, or any of the policies highlighted above, may lead to disciplinary action, which could result in dismissal

Version Control

Version	Date	Authors	Approver	Comments
Version 0.1	09/02/2022	JS		Original Draft
Version 1.0	09/03/2022	JS	Michael Hall	FINAL PUBLISHED
ANNUAL REVIEW	15/02/2023	JS		NO CHANGES
ANNUAL REVIEW	12/02/2024	JS		NO CHANGES
V2.0	16/07/2024	JS		Interim review – changes to reflect business and other grammatical and term changes
Version 3.0	14/02/2025	JS		FULL REWRITE
Version 3.0				Executive Sign Off

Version 3.0 was created in February 2025, and will be reviewed again in February 2026, or sooner if legislation, regulations, or guidance change in the interim.

This document was created in February 2025. Please note that the new Data Use and Access Act received Royal Assent on 19 June 2025, and the contents of this document may change before the annual review date, once all aspects of the new Act have been assessed by the ICO and communicated to our Compliance and Data Protection Manager.

Data Protection Policy

The two appendices below contain information on 1) data protection principles and 2) good practice guidance.

APPENDICES

APPENDIX 1 – DATA PROTECTION PRINCIPLES

Personal Data falls into two categories:

Personal Data: which means any information relating to a living person who can be directly, or indirectly, identified, by an identifier.

The personal data definition provides for a wide range of identifiers which make up personal data, and include (not a full list) name, date of birth, location data (such as postcode or address) or online identifier (such as a unique learner reference number), reflecting changes in technology and the way organisations collect information about people.

DPA2018 and UKGDPR apply to both automated (online) personal data and to manual data such as paper filing systems which may include sets of manual records stored in date order that contain personal data.

Personal data that has been pseudonymised can fall within the scope of DPA2018 and UKGDPR depending on how difficult it is to attribute the pseudonym to a particular person.

Sensitive Personal Data: also known as 'special categories of personal data.' The special categories specifically include genetic data, and biometric data that identify a specific person because of its unique markers. It also includes any information relating to a person's racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, health, and sex life/orientation. Some of this type of data will regularly be collected (sometimes by accident, sometimes as a requirement of operational processes) during day-to-day operations. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards are in place for processing this type of data.

1. **The Lawful Bases for Processing:**

   There are six lawful bases under which the Group can process personal data. Any, or all, of the six must apply to a particular circumstance to allow the Group to collect the data:

   - **Consent:** the person has given their clear and explicit consent for the Group to process their personal data for a specific purpose.
   - **Contract:** the processing is necessary for a contract the Group has with the person, or because they have asked the Group to take specific steps before entering into a contract.
   - **Legal Obligation:** the processing is necessary for the Group to comply with the law (not including any contractual obligations).
   - **Vital Interests:** the processing is necessary to protect a person's life.
   - **Public Task:** the processing is necessary for the Group to perform a task in the public interest or for its official functions; and the task or function has a clear basis in law.
   - **Legitimate Interests:** the processing is necessary for the Group's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the person's personal data which overrides the legitimate interests.

2. **The Individual Rights of Data Subjects:**

   A living person has eight rights under DPA2018 and UKGDPR in respect of what they can ask the Group to do with their data:

   - **The right to be informed:** a living person has the right to be informed about the collection and use of their personal data. The Group must provide information that includes the purpose for processing, retention periods, and who the data will be shared with. This right is managed by the Group through its Privacy Statements, which are accessed through the Group's various websites.

- **The right of access:** a living person has the right to access their personal data and supplementary information, and to be made aware of, and verify, the lawfulness of the processing. This is commonly referred to as a Data Subject Access Request (DSAR) and is managed by the DPO.
- **The right to rectification:** a living person has the right to have inaccurate personal data rectified (amended) or completed (if incomplete) - e.g., employees can do this for a student who tells the employee that the Group has spelt their surname wrong on the Group's electronic records.
- **The right to erasure:** a living person has the right to have personal data erased (commonly known as the right to be forgotten). This right is not guaranteed and only applies in certain circumstances controlled by the Group's DPO.
- **The right to restrict processing:** a living person has the right to request for the restriction or suppression of personal data. Where restricted the Group can store the personal data but cannot use it. As with erasure this is not a guaranteed right and only applies in certain circumstances controlled by the Group's DPO.
- **The right to data portability**: a living person has the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move or copy or transfer personal data easily from the systems of one company to the systems of another (e.g., it may become possible in the future to ask for car insurance black box data to be transferred from one insurance company to another). All data must be provided in a structured, commonly used, and machine-readable format.
- **The right to object:** a living person has the right to object to processing based on legitimate interests, profiling, or the performance of tasks in the public interest. It also allows people to object (opt-out) to direct marketing and processing for statistical, historical, or scientific research.

- **Rights in relation to automated decision making and profiling**: a living person has the right to appeal against any Group decision to provide (or not) goods and services where the decision has been made by automated means. Any objection could lead to the decision being reviewed manually; but does not guarantee that the original decision will be overturned.

All requests and objections under DPA2018 and UKGDPR must be referred to the Group's DPO in the first instance.
No charges are normally levied by the Group against a person who is exercising their rights and all requests/objections from people must be actioned within one month of receipt.

3. Security

A key principle of DPA2018 and UKGDPR is that the Group processes personal data securely by means of 'appropriate, technical, and organisational measures'. This requires the Group to consider risk analysis, policies, completion of data protection impact assessments (DPIA), and physical and technical measures. Where appropriate the Group will consider pseudonymisation.
Measures must ensure the confidentiality, integrity and availability of systems and services including (but not restricted to) being able to restore access and availability to personal data promptly following a technical or physical incident; and the ability to test the effectiveness of measures and to undertake improvement actions because of the test.

4. International Transfers

Data cannot be transferred outside the European Economic Area (EEA) without referral and confirmation from the Group's DPO.

5. Data Protection Breaches

ALL data protection breaches (or suspected breaches) MUST be reported to the Group's DPO as soon as they are identified (and at the latest within 24 hours of finding the actual or suspected breach).

The DPO handles reporting to the ICO within 72 hours of a breach being identified where there has been material damage regardless of the number of people affected.

APPENDIX 2 – GOOD PRACTICE SUGGESTIONS (not exhaustive):

- Employees should make sure that paper documents and other manual records that contain personal data are stored in locked cabinets. If employees are struggling to find suitable cabinets/drawers, then their line manager must sort out additional suitable storage.
- Employees should always follow the Group's **2025 Clear Desk Policy.**
- Employees should make sure that computerised records are password protected.
- Employees should make sure that computer monitors are sited so that they are not visible except to authorised personnel – if employees are an employee and are concerned there are special computer privacy screens that can be ordered for employees.
- Monitors should not be left unattended and should routinely be locked when employees are away from their desk.
- Both manual and electronic records that contain personal data must only be kept for as long as they are needed and when personal data is no longer needed it should be disposed of securely (See the **2025 Data Retention and Deletion Policy**).
- Do not remove hardcopy information containing personal data from the office, and if unavoidable then the data needs to be treated with the same care and attention as data within the office.
- Where personal data is being sent to a third party, ensure that the receiving party treats the data in accordance with DPA2018 and UKGDPR.

- When entering into contracts with third parties always ensure that the Group's contract terms or those of the third party include specific clauses relating to the DPA2018 and UKGDPR obligations of both parties.