General Data Protection Policy

This policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties. The below definitions apply to this policy:

- **Data Controller:** the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company and Personal Data used in our business for our own commercial purposes.
- **Data Protection Manager (DPM):** the person appointed by us with responsibility for data protection compliance. That person is [NAME].
- **Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data.
- **General Data Protection Regulation (GDPR):** the General Data Protection Regulation ((EU) 2016/679).
- **Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
- **Personal Data Breach:** any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
- **Processing or Process:** any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
- **Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

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

This policy applies to all staff. You must read, understand and comply with this policy when Processing Personal Data on our behalf. This policy sets out what we expect from you. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

Scope

In the course of your work you may come into contact with or use confidential information about employees, clients and customers, for example their names and home addresses. The GDPR contains principles affecting employees' and other personal records i.e. any information that identifies an individual. Information protected by GDPR includes not only personal data held on computer but also manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to

ensure that you do not breach GDPR. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the GDPR committee.
You should be aware that, under GDPR, you are personally accountable for your actions and can be held criminally liable if you knowingly, or recklessly, breach it. Any serious breach of data protection will also be regarded as misconduct and will be dealt with under the Company's disciplinary procedures. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

The GDPR principles

There are 7 key principles that are central to GDPR. All employees must comply with these principles at all times in information-handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data.
2. Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.
3. Adequate, relevant and not excessive. The Company will review personnel files on a regular basis to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.
4. Accurate and kept up-to-date. If your personal information changes, for example you change address, you must inform your Branch Manager as soon as practicable so that the Company's records can be updated. The Company cannot be held responsible for any errors unless you have notified the Company of the relevant change.
5. Not kept for longer than is necessary. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a period of time will be destroyed.
6. Processed in accordance with an individual's rights and consent.
7. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personnel files are confidential and are stored in locked filing cabinets. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on memory sticks, portable hard drives or other removable storage media will be kept in locked filing cabinets or locked drawers when not in use by authorised employees. Data held on computer will be stored confidentially by means of password protection, encryption or coding, and again only authorised employees have access to that data. The Company has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed.

Lawfulness and fairness

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

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

a) the Data Subject has given his or her consent;
b) the Processing is necessary for the performance of a contract with the Data Subject;
c) to meet our legal compliance obligations;
d) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

You must identify and document the legal ground being relied on for each Processing activity.

Transparency (notifying data subjects)

The GDPR requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.
Whenever we collect Personal Data directly from Data Subjects we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPM, how and why we will use, process, disclose, protect and retain that Personal Data through a notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

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

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

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

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

You may only collect Personal Data that you require for your job: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.
You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised.

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

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

Storage limitation

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

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

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

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

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

Protecting Personal Data

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

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

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

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

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

Data Breach

The GDPR requires us to notify Personal Data Breaches to the regulator and, in certain instances, the Data Subject. If at any time you suspect there has been a Personal Data Breach, then you must contact the DPM immediately and follow their instructions. You should preserve all evidence relating to the potential Personal Data Breach and

not attempt to investigate the matter yourself. Should the DPM not be available, please contact one of the GDPR Committee (see below) on 01558 824044.

- Ben Davies - Director
- Rachel Davies - Director
- Philip Evans - Finance Director
- Amanda Marouli - Human Resources Manager

Time is critical, so don't delay in reporting.

We will notify Data Subjects or any applicable regulator of any data breach where we are legally required to do so.

Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.
You are not permitted to transfer Personal Data outside the EEA and should you be required to do so as part of your job you should seek guidance first from the DPM.

Data Subject's rights and requests

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

a) withdraw consent to Processing at any time;
b) receive certain information about Processing activities;
c) request access to their Personal Data that we hold;
d) prevent our use of their Personal Data for direct marketing purposes;
e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
f) restrict Processing in specific circumstances;
g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and
k) make a complaint to the supervisory authority.

You must verify the identity of an individual requesting data under any of the rights listed above.
You must immediately forward any Data Subject request you receive to the DPM.

Accountability

As a Data Controller we must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

Record keeping

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

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' consents and procedures for obtaining consents.

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

Sharing Personal Data

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

You may only share the Personal Data we hold with another employee or agent if the recipient has a job-related need to know the information and the transfer complies with GDPR.

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

a) they have a need to know the information for the purposes of providing the contracted services;
b) sharing the Personal Data complies with the notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;
c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
d) the transfer complies with any applicable cross border transfer restrictions; and
e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Reviewed April 2023