Data Protection Policy and Procedures

Version	*Edited by*	*Date*	*Review Date*
1	Zena Hardy	September 2025	September 2026

Policy Statement

We Believe You Achieve (hereinafter referred to as "the Company") recognises that, in order to deliver our services effectively, we must collect and process certain types of personal information. This includes information relating to employees, learners, parents/carers, suppliers, contractors, volunteers, and other stakeholders.

The personal information we collect may include, but is not limited to names, addresses, email addresses, dates of birth, IP addresses, ULN numbers, identification details, confidential records, medical information, sensitive data, and financial details such as bank or credit card information.

In addition to supporting our operational activities, we may also be required to collect and process personal information to comply with legal and regulatory obligations. We are fully committed to processing all personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all other relevant data protection legislation and codes of practice (collectively referred to as "data protection laws").

To uphold these obligations, the Company has implemented robust policies, procedures, and security measures designed to ensure ongoing compliance. This includes regular staff training, procedural documentation, audits, and data protection impact assessments. We adopt a 'Privacy by Design and Default' approach, meaning that data protection considerations are embedded into all our systems, processes, and decision-making from the outset. Maintaining the security and confidentiality of personal and sensitive data is a top priority.

Purpose

The purpose of this policy is to ensure that We Believe You Achieve meets its legal, statutory, and regulatory responsibilities under current data protection laws, and to guarantee that all personal and special category data is processed lawfully, fairly, and in the best interests of individuals.

Data protection laws emphasise accountability and good governance. Accordingly, the Company has implemented a comprehensive data protection framework to minimise the risk of data breaches and to uphold the rights of individuals.

This policy serves as a key reference document for staff, volunteers, contractors, and third parties, outlining their responsibilities when handling personal data and responding to data subject requests.

Scope

This policy applies to all individuals working for or on behalf of We Believe You Achieve, including:

- Permanent and temporary employees
- Fixed-term staff
- Volunteers and interns
- Agency workers and sub-contractors
- Third-party representatives and external partners (UK or overseas)

Compliance with this policy is **mandatory**, and any breach may lead to disciplinary action or termination of contract where appropriate.

Definitions

For the purpose of this policy, the following definitions apply:

- **Biometric Data:** Personal data resulting from specific technical processing relating to an individual's physical, physiological or behavioural characteristics (e.g. facial recognition or fingerprints) used for unique identification**.**
- **Binding Corporate Rules**: Internal data protection policies adhered to by the Company for the transfer of personal data to controllers or processors in third countries.
- **Consent**: Any freely given, specific, informed, and unambiguous indication of a data subject's wishes by which they signify agreement to the processing of their personal data.
- **Cross-Border Processing:** Processing of personal data in more than one Member State, or where it substantially affects data subjects in more than one Member State.
- **Data Controller:** The individual or organisation that determines the purposes and means of processing personal data.
- **Data Processor:** An individual or organisation that processes personal data on behalf of the controller.
- **Data Protection Laws:** Refers collectively to the UK GDPR, the Data Protection Act 2018, and any other relevant UK data protection legislation.

- **Data Subject:** The individual who is the subject of personal data.
- **GDPR:** The General Data Protection Regulation (EU) 2016/679, as incorporated into UK law.
- **Genetic Data:** Personal data relating to inherited or acquired genetic characteristics that provide unique information about a person's physiology or health.
- **Personal Data:** Any information relating to an identified or identifiable natural person, directly or indirectly.
- **Processing:** Any operation performed on personal data (e.g. collection, storage, use, disclosure, destruction).
- **Profiling:** Automated processing of personal data to analyse or predict personal aspects of an individual.
- **Recipient:** Any party to whom personal data is disclosed.
- **Supervisory Authority:** An independent public authority established by a Member State to oversee data protection compliance (e.g. the ICO in the UK).
- **Third Party:** Any person or organisation other than the data subject, controller, or processor, acting under the direct authority of the controller or processor.

National Data Protection Law

As We Believe You Achieve operates within the United Kingdom, we are bound by the requirements of the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, which implements the GDPR into UK law.

Our data protection policies, procedures, and practices are fully aligned with the provisions set out in both the GDPR and the Data Protection Act 2018. This ensures that all personal and special category data is collected, processed, stored, and disposed of lawfully and responsibly, in accordance with the rights of individuals and the expectations of our business operations.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (EU) 2016/679 was adopted by the European Commission in April 2016 and became enforceable in all EU Member States on 25 May 2018**.** As a **Regulation**, rather than a Directive, it applied directly to Member States, replacing their national data protection laws and repealing Directive 95/46/EC.

Although the UK has left the European Union, the core principles of the GDPR have been retained in UK law through the **UK GDPR**, ensuring a high and consistent standard of data protection.

As the Company collects and processes personal information relating to individuals ("data subjects"), we are legally obligated to handle such information in full compliance with GDPR principles. This includes ensuring that personal data is lawfully obtained, processed, stored, and destroyed, and that individuals' rights are respected throughout the data lifecycle.

Personal Data

Under GDPR, personal data is defined 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."

We Believe You Achieve applies particular care when processing **special categories of personal data** (previously referred to as sensitive personal data). This type of information carries a higher risk because it could be misused or cause harm or discrimination to the individual.

Special categories of personal data include, but are not limited to, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (used for identification), health data, and data concerning a person's sex life or sexual orientation.

Under Article 9 of the GDPR, the processing of these special categories is prohibited unless a specific legal condition applies, such as explicit consent, legal obligations, or safeguarding requirements.

The GDPR Principles

Article 5 of the GDPR sets out six fundamental principles for processing personal data, along with the principle of accountability. We Believe You Achieve fully adheres to these principles:

1) **Lawfulness, Fairness and Transparency**
Personal data must be processed lawfully, fairly and in a transparent manner, ensuring that individuals understand how their data is used.

2) **Purpose Limitation**

Data must be collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.

3) **Data Minimisation**

Data collected must be adequate, relevant, and limited to what is strictly necessary for the intended purpose.

4) **Accuracy**

Personal data must be accurate and, where necessary, kept up to date. Inaccurate data must be rectified or erased without delay.

5) **Storage Limitation**

Data must not be kept in a form that permits identification for longer than is necessary. Where data is retained for archiving, research or statistical purposes, appropriate safeguards must be in place.

6) **Integrity and Confidentiality (Security)**

Personal data must be processed securely, protecting it against unauthorised access, unlawful processing, accidental loss, destruction, or damage through appropriate technical and organisational measures.

Accountability

Under Article 5(2), the Company, as data controller, is responsible for demonstrating compliance with all the above principles. We maintain documented policies, procedures, training, and audit trails to evidence our compliance and ensure risks associated with processing personal data are effectively managed.

OBJECTIVES

We Believe You Achieve is fully committed to ensuring that all personal data is processed in line with the **UK GDPR**, the **Data Protection Act 2018**, and all other relevant legislation, regulations, and codes of practice. We are dedicated to maintaining the lawful, secure, transparent, and ethical processing of personal data, while upholding the rights and freedoms of all individuals whose information we hold.

The Company has established the following key objectives to ensure continued compliance and best practice in data protection:

- **Upholding Individual Rights**

  We protect the rights of individuals in relation to the processing of their personal data and ensure that they can exercise these rights effectively.

- **Comprehensive Policy Framework**

  We have developed, implemented, and maintained a robust Data Protection Policy, supporting procedures, an audit plan, and a training programme to ensure compliance with all data protection laws.

- **Monitoring Business Processes**

  Every business practice, process, and activity undertaken by the Company is monitored to ensure ongoing compliance with data protection principles and legal obligations.

- **Lawful Processing**

  Personal data is only processed when the lawful basis for doing so has been identified, recorded, and meets the requirements of data protection legislation.

- **Special Category Data**

  Any processing of special category data is carried out strictly in accordance with GDPR and the relevant conditions set out in Schedule 1 of the Data Protection Act 2018.

- **Consent Management**

  Consent is always recorded at the point it is obtained, and evidence of consent can be provided to the Supervisory Authority upon request.

- **Training and Competence**

  All staff receive regular, in-depth training on data protection laws, principles, and procedures relevant to their role, ensuring that they are fully aware of their responsibilities.

- **Building Trust with Individuals**

  We aim to foster a culture where individuals feel safe and confident when providing their personal information, knowing that it will be handled responsibly and in accordance with their legal rights.

- **Continuous Improvement**

  We maintain an ongoing programme of monitoring, review, and improvement to identify and address gaps or risks in compliance before they become issues.

- **Staying Up to Date**

  We actively monitor guidance and updates from the Information Commissioner's Office **(ICO)**, the European Data Protection Board **(EDPB)**, and relevant legal bodies to stay informed of changes or new requirements.

- **Incident and Complaint Handling**

  We have clear, documented procedures for identifying, investigating, reviewing, and reporting data protection complaints or breaches.

- **Data Protection Officer (DPO)**

  We have appointed a Data Protection Officer, responsible for the supervision, implementation, and ongoing compliance of our data protection framework, in line with Article 37 of the GDPR.

- **Auditing and Oversight**

  Our dedicated Audit & Monitoring Programme conducts regular checks on how personal data is collected, used, stored, and shared, to ensure adherence to legal and internal policy requirements.

- **Clear Reporting Lines**

  We maintain transparent reporting structures and lines of accountability regarding data protection matters.

- **Data Retention and Disposal**

  All personal information is stored and securely destroyed in line with our Data Retention Policy, which is based on legal, statutory, and regulatory timeframes.

- **Transparent Communication**

  Any information provided to individuals regarding their personal data is delivered in a clear, concise, and accessible format, using plain language.

- **Employee Rights**

  All employees are informed of their own rights under data protection law and are provided with Privacy Notices in accordance with Articles 13 and 14.

- **Record Keeping**

  Where applicable, we maintain Records of Processing Activities in line with Article 30 requirements.

- **Technical and Organisational Measures**

  We have implemented strong technical and organisational security measures to protect personal data, supported by a comprehensive Information Security Programme.

Governance Procedures

Accountability & Compliance

We Believe You Achieve recognises the importance of strong governance in ensuring full compliance with data protection legislation. Given the nature, scope, context, and purposes of the data we process, we conduct regular risk assessments and information audits to identify, assess, and monitor any potential impact of our data processing activities.

We have implemented robust technical and organisational measures to safeguard all personal data and can evidence compliance through clear documentation, training, and established working practices.

Our key governance objectives are to:

- **Educate** all staff and volunteers on data protection law, their responsibilities, and the risks of non-compliance.
- **Provide regular and role-specific training**, ensuring staff understand how data protection applies to their day-to-day work.
- **Allocate clear responsibility** for data protection compliance and ensure the designated lead has sufficient authority, resources, and support to fulfil their role effectively.
- **Establish clear reporting lines** within our governance structure to ensure transparency and accountability.

All governance measures, including those outlined below, are supported by internal Information Security Policies and procedures to ensure full compliance with GDPR, the Data Protection Act 2018, and relevant codes of conduct.

Privacy by Design

We adopt a Privacy by Design approach across all activities, meaning that privacy and data protection considerations are built into our systems and processes from the outset rather than added later.
We focus on risk prevention, minimising the data we collect and controlling access at every stage.

Data Minimisation

In line with GDPR Article 5(1)(c), we only collect, store, process, and share the minimum amount of personal data necessary to deliver our services or meet legal obligations.
Examples of how this is achieved:

- Online and paper forms are reviewed regularly to ensure they only request essential information.
- Telephone and face-to-face data collection uses predefined scripts to ensure only relevant data is captured.
- Service Level Agreements (SLAs) and data sharing agreements with third parties strictly limit the data shared to what is relevant and necessary.
- All collection tools and forms are reviewed at least every three months to ensure continued compliance.

Access Restriction

Access to personal data is strictly limited to those who need it for their role. Special category data (e.g. medical

information) can only be accessed by authorised Admin staff or First Aid Providers where necessary.

Hard Copy Data

Where paper records must be used:

- We always request data directly from the original controller first.
- We redact documents to remove unnecessary information before sharing.
- Where feasible, hard copy data is scanned, securely transferred using encryption, and originals are then securely destroyed.
- Any physical copies retained are kept in a locked safe, not in general storage, and are shredded as soon as they are no longer required.

Information Audit

To ensure full compliance, We Believe You Achieve Ltd has conducted a comprehensive information audit, recording all personal data we hold and process in our roles as both data controller and data processor.

The central information register includes:

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing
- The format(s) it is stored in
- Who is responsible for it internally
- Any disclosures or international transfers

This register supports our ability to meet GDPR Article 30 obligations and provides clear visibility of all data flows across the organisation.

Legal Basis for Processing *(Lawfulness)*

Before any personal data is collected or processed, the legal basis for processing is identified, documented, and verified against Article 6 of the GDPR. No processing activity is undertaken without a valid lawful basis.

Lawful bases used by the organisation include:

- **Consent** – freely given by the data subject for specific purposes.
- **Contractual necessity** – where processing is required prior to or during a contractual arrangement (e.g. payment details for service provision).
- **Legal obligation** – where processing is necessary to comply with the law.
- **Vital interests** – where processing is necessary to protect someone's life (e.g. emergency medical information).
- **Legitimate interests** – where processing is necessary for our legitimate organisational aims, provided these are not overridden by the individual's rights and freedoms, particularly in the case of children.

These lawful bases are clearly outlined in our Privacy Notices and recorded in the information audit.

Records of Processing Activities

As a small organisation with fewer than 250 employees, we are not required to maintain full Article 30 records for every processing activity. However, we continually review our size and processing activities. We will begin maintaining full records where:

1. We employ 250 or more staff.
2. Processing may pose risks to individuals' rights and freedoms.
3. Processing is not occasional.
4. We process special category or criminal offence data.

Where records are maintained, they will be in writing, easy to read, and available to the ICO upon request.

Data Retention & Disposal

We Believe You Achieve adheres to clearly defined retention periods, aligned with legal, contractual, and operational requirements. Personal data is never kept longer than necessary.

When data reaches the end of its retention period, it is securely destroyed to protect individuals' privacy, using methods such as:

- Shredding for paper records
- Secure confidential waste disposal

- Permanent electronic deletion from systems

Our retention procedures are reviewed regularly to ensure they meet current legal and operational standards.

1 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Individuals have the right to expect that their personal information will be treated with the highest levels of privacy and confidentiality while it is stored and processed by We Believe You Achieve**.**

We use a range of measures and tools to minimise data protection risks and potential breaches during everyday processing. Where proposed processing activities are likely to result in a high risk to the rights and freedoms of individuals (as defined in Article 35 GDPR), we will carry out a **Data Protection Impact Assessment (DPIA)** prior to commencing the activity.

Currently, the organisation does not conduct any processing activities that legally require a DPIA. However, we regularly monitor our operations against the GDPR criteria and have robust DPIA procedures ready to implement should the need arise. These procedures ensure that risks are identified early and that appropriate safeguards are built into any new systems, technologies, or processes.

DATA SUBJECT RIGHTS PROCEDURES

The GDPR and Data Protection Act 2018 provide individuals with specific legal rights over their personal data. We Believe You Achieve has implemented clear and practical procedures to enable individuals to exercise these rights quickly, transparently, and free of charge.

Consent & The Right to be Informed

As part of delivering our services, we collect personal and in some cases special category data. We have established controls to ensure that consent is always obtained and managed in line with GDPR standards.

Consent is defined as:

“Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they, by a statement or by clear affirmative action, signify agreement to the processing of personal data relating to them.”

We ensure that:

- Consent requests use plain, clear language avoiding legal jargon.
- Consent is freely given, specific, informed, and unambiguous, with positive opt-in only.
- Consent is separate from other agreements, never pre-ticked, and not a precondition of service (unless necessary).
- All third parties who rely on the consent are clearly named.
- Detailed records are kept, evidencing what was consented to, when, how, and what individuals were told.
- Withdrawing consent is as easy as giving it, and can be done verbally, in writing, or by email.
- Withdrawals are processed immediately and without detriment.
- Age-verification and parental consent checks are in place for children under 13.
- Consent is refreshed periodically for continuing data use.
- Special category data consent is always explicit and purpose specific.

Consent Controls

We keep strict, verifiable records of consent and ensure withdrawal processes are simple and documented. All consent wording is reviewed and approved by our Data Protection Lead before use.

Consent can be obtained through:

- Face-to-face conversations
- Telephone
- Written forms
- Email or SMS
- Electronic methods (e.g. web forms)

Privacy Notices accompany all consent collection to ensure transparency.

Child's Consent

Under the UK Data Protection Act 2018, the age of consent is set at 13 years. If a child is under 13, we only process their data with verified parental consent. We review consents annually and transfer control to the child once they reach 13.

Alternatives to Consent

We recognise that consent is not always the appropriate lawful basis. We only use consent where the individual genuinely has a choice. We do not rely on consent:

- Where processing would continue regardless of consent.
- As a precondition of service unless strictly necessary.
- In situations with an inherent power imbalance (e.g. employees).

Information Provisions

When we collect data directly, we provide individuals with a Privacy Notice that includes:

- Contact details for the Data Protection Lead
- Purpose and legal basis for processing
- Legitimate interests (if applicable)
- Recipients of the data
- Retention periods or criteria
- Rights of access, rectification, erasure, restriction, objection, and portability
- Withdrawal of consent rights
- Right to lodge a complaint

This information is provided at the time of collection, and consent records are kept for at least six years, unless legal requirements specify otherwise.

Privacy Notice

Definition

A Privacy Notice is the information we give to individuals at the point we collect their personal data (or at the earliest opportunity where data is obtained from another source). It explains how, why, and when we process personal data and sets out individuals' rights.

Content

Our Privacy Notices meet the requirements of **UK GDPR Articles 13 and/or 14** and include:

- Who we are and how to contact our Data Protection Lead
- The purposes and lawful bases for processing (including legitimate interests, where used)
- The categories of data (for indirect collection) and the source
- Recipients or categories of recipients
- Retention periods or the criteria used to set them
- Individuals' rights (access, rectification, erasure, restriction, objection, portability)
- The right to withdraw consent (where consent is used)
- How to raise a concern or complaint

Format & Accessibility

Privacy Notices are:

- Clear, concise, and jargon-free, using plain language
- Easily accessible in the format that fits the collection method, including:
    - Included in agreements, contracts, forms, and other written/face-to-face materials
        - Embedded in employee contracts and recruitment materials
        - Provided verbally where data is collected by phone or in person
        - Published on our website where appropriate

Quality Assurance & Testing

To ensure usability and comprehension, We Believe You Achieve:

1. Drafts Privacy Notices in line with data protection law and ICO guidance.
2. User-tests notices (in the formats we use) with a small sample of learners/parents/staff and gathers feedback on clarity, completeness, and confidence to consent.
3. Records feedback and make documented improvements.
4. Re-tests revised versions with a fresh sample for independent validation.
5. Conducts a final legal compliance check against current legislation and ICO guidance.
6. Approves the final notice via the appropriate senior sign-off (Director or Data Protection Lead).

When Consent Is the Lawful Basis

Where we rely on consent, we ensure that consent mechanisms are:

- Prominent and separate from other terms
- Positive opt-in
- Granular, allowing choice over different processing activities
- Informative, explaining each use clearly
- Simple to withdraw, with withdrawal routes as easy as giving consent

Employee Personal Data

We do not rely on consent as the lawful basis for processing employee data. Instead, lawful bases such as legal obligations and contractual necessity apply. All employees receive a Privacy Notice and guidance through the Staff Handbook on their data rights and how to exercise them.

The Right of Access

We provide all GDPR Article 15–22 information in a clear, transparent format, free of charge, within 30 calendar days. Extensions of up to 2 months are only used for complex cases and communicated in writing.

Subject Access Request

Under the UK GDPR and Data Protection Act 2018, individuals have the right to request confirmation of whether their personal data is being processed and, where applicable, access to that data. When a Subject Access Request (SAR) is received, We Believe You Achieve will provide the individual with the following information:

- The purpose(s) of the processing
- The categories of personal data concerned
- The recipients or categories of recipients to whom the personal data has been or will be disclosed
- Where possible, the envisaged retention period for the data, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data, restriction of processing, or to object to processing
- The right to lodge a complaint with the Information Commissioner's Office (ICO)
- Where the personal data has not been collected directly from the data subject, any available information regarding its source
- The existence of any automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and potential consequences of such processing for the data subject

All SARs are passed immediately to the Data Protection Lead, who records the request in the SAR log. The type of data held is then cross-checked against the organisation's Information Audit to determine:

- What data is held
- In what format it is stored
- Who has access to it
- Whether it has been shared with any third parties
- Applicable retention or access timeframes

We aim to respond to all SARs within **30 calendar days** from the date of receipt. This service is provided **free of charge**. Where the request is made electronically, the response will be provided in a commonly used electronic format (e.g. PDF), unless an alternative format is requested by the individual.

If the request is particularly complex or involves large volumes of data, we may extend the response period by a further **two months** in line with Article 12(3) of the UK GDPR. In such cases, the individual will be notified within the initial 30-day period and provided with a clear explanation for the delay.

For full guidance on how individuals can make a SAR and the steps the organisation takes to process requests, please refer to our **Subject Access Request Procedure** document.

Correcting Inaccurate or Incomplete Data

In line with **Article 5(d)** of the UK GDPR, We Believe You Achieve ensures that all personal data held and processed is accurate and, where necessary, kept up to date. We regularly review information and take every reasonable step to correct inaccuracies as soon as they are identified, either by us or by the data subject.

When a data subject notifies us of inaccurate or incomplete information, the Director (Zena Hardy) will be informed. He is responsible for validating the request, making the necessary amendments, and checking the information audit to ensure all relevant records are updated. Where applicable, a supplementary statement will also be added to clarify any changes made.

Corrections will be completed within **30 days** of receiving the request. If the inaccurate data has been shared with third parties (such as subcontractors, government bodies or public authorities), they will also be informed of the rectification. The data subject will receive written confirmation once the correction has been completed and, where relevant, details of any third parties notified.

If, for any reason, we are unable to comply with a rectification or completion request, the data subject will receive a clear written explanation. This will include information on their right to raise a complaint with the relevant supervisory authority.

The Right to Erasure

Also known as the **"Right to be Forgotten"**, We Believe You Achieve fully complies with **Article 5(e)** of the UK GDPR. We ensure that personal data which identifies an individual is not kept for longer than is **necessary** for the purposes for which it was originally collected and processed.

All personal data is reviewed as part of our information audit. Each category of data is assigned either a specific erasure date or is monitored to ensure it is securely deleted when it is no longer needed. This ensures we meet legal, regulatory, and operational requirements while protecting individuals' privacy.

For more details on how data is securely erased and how we meet the requirements of Article 17**,** please refer to our Data Retention and Erasure Policy.

Objections and Automated Decision Making

Individuals have the right to object to the processing of their personal data. This right is clearly explained in our Privacy Notices and at the point of first contact.

People can object to:

- Processing based on our legitimate interests or a legal/public task (including profiling).
- Direct marketing (including profiling).
- Processing for statistical purposes.

If someone objects to direct marketing, we will stop immediately. For other objections, we may continue if we can show strong legal grounds or if the processing is needed for legal claims. We respond to all objections within 30 days.

Automated Decision Making

We do not rely on fully automated decision-making to make significant decisions about individuals. If this ever changes, we will inform people, explain their rights, and ensure they can request human review of any automated decision.

8 Oversight Procedures

Security & Breach Management

We take the security of personal data very seriously. Regular information audits and risk assessments help us identify and reduce the risk of data breaches.

We use appropriate technical and organisational measures to protect data from loss, unauthorised access or disclosure. If a data breach occurs, we follow clear procedures to contain the breach, assess the impact, notify the Director (Zena), and inform affected individuals and authorities where required.

9 Data Sharing and information transfer

10 Audits & Monitoring

We carry out regular data protection audits to make sure our policies and security measures are effective. These audits check that:

- Policies and procedures are in place and followed.
- Risks are identified and addressed quickly.
- Staff are compliant with GDPR requirements.

The Data Protection Officer oversees all audits and reports outcomes to the team, along with any improvement plans.

11 Training

12 Penalties

We understand that failure to comply with data protection laws can result in significant fines and penalties, including:

- Up to 2% of annual turnover for certain breaches.
- Up to 4% of annual turnover for more serious breaches.

All staff are made aware of the seriousness of non-compliance.

13 Responsibilities

The Company has appointed a **Data Protection Lead** whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees to actively stay informed and up to date with all legislation and changes relating to data protection.

The DPL will work in conjunction with all processes, to ensure all systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPL has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent.