Data Protection (GDPR) Policy

This policy outlines how personal data should be collected, handled, and stored to ensure compliance with the company's data protection standards, in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

All employees, temporary staff, consultants, contractors, and third parties are responsible for protecting ITP data that they create, store, process, or transfer. This policy applies to both current and former employees, workers, volunteers, interns, apprentices, and consultants. If you belong to any of these groups, you are considered a "data subject" under this policy.

The Company has taken measures to safeguard your data and will inform all employees, temporary staff, consultants, contractors, and third parties of their responsibility to protect personal data. Data will only be retained for as long as necessary to fulfil the purposes for which it was collected.
This policy explains how the Company will handle and process your data, your rights as a data subject, and your responsibilities when collecting, handling, processing, or storing personal data.

Data Protection Principles

Personal data must be processed in accordance with Data Protection Principles;

- Personal data must be processed lawfully, fairly, and transparently in relation to the data subject, ensuring that the principles of lawfulness, fairness, and transparency are upheld.
- Data must be collected for specified, explicit, and legitimate purposes, and must not be further processed in a way that is incompatible with those purposes. However, processing for archiving in the public interest, scientific or historical research, or statistical purposes is considered compatible with the original purposes, as per Article 89(1) ('purpose limitation').
- Data must be adequate, relevant, and limited to what is necessary for the intended purposes of processing ('data minimisation').
- Data must be accurate and, when necessary, kept up to date. Every reasonable step should be taken to rectify or erase any inaccurate personal data without delay, based on the purposes for which they are processed ('accuracy').
- Data must be kept in a form that allows identification of data subjects for no longer than necessary for the purposes of processing. Personal data may be stored longer if it is solely for archiving purposes in the public interest, scientific or historical research, or statistical purposes, in line with Article 89(1), provided appropriate technical and organisational safeguards are in place to protect the rights and freedoms of the data subjects ('storage limitation').
- Data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing, as well as against accidental loss, destruction, or damage, through the use of appropriate technical or organisational measures ('integrity and confidentiality').

The controller (i.e. The ITP) shall be responsible for and be able to demonstrate compliance with these principles.

Definitions

'Personal data' refers to information about a living individual ('data subject') who can be identified either directly from the data or indirectly when combined with other information in our possession or likely to come into our possession. This includes expressions of opinion about the individual and indications of the intentions of us or others concerning that person.

This policy applies to all personal data, whether stored electronically, on paper, or other materials. Such data may be provided by the individual or others (e.g., former employers, doctors, or credit reference

agencies), or it may be created by us. It can arise during recruitment, throughout employment or service contracts, or even after termination, and may be generated by managers or colleagues.

Sensitive personal data refers to personal information about a data subject that includes details such as racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexuality, and information related to criminal offences.

Processing refers to obtaining, recording, holding, or performing any operation or series of operations on information or data. This includes activities such as collection, recording, organisation, structuring, or storage; adaptation or alteration; retrieval, consultation, or use; disclosure through transmission, dissemination, or other means; alignment or combination; and restriction, destruction, or erasure. It also covers the processing of personal data within a filing system and any automated processing.

A **data processor**, in relation to personal data, is any individual or entity (excluding an employee of the data controller) that processes data on behalf of the data controller.

Purpose

This document sets out clear guidelines for the collection, handling, storage, and processing of data within our organisation. It is designed to ensure compliance with applicable laws and regulations, such as data protection legislation, while protecting the confidentiality, integrity, and availability of sensitive information. By defining the rights of data subjects and the responsibilities of those handling data, this policy fosters transparency, accountability, and adherence to best practices in data protection.

It also aims to mitigate risks such as data breaches, misuse, or unauthorised access, reflecting the organisation's commitment to ethical data management.

The primary purpose of this document is to safeguard the personal information of employees, learners, and others whose data is collected or processed by The ITP, while ensuring they are aware of their rights under GDPR. Specifically, this policy aims to:

- Ensure good data protection practices across the organisation.
- Ensure compliance with GDPR and other relevant legislation governing personal data.

This document serves as an internal guide for data handling; however, it is subject to all laws, rules, and regulations that govern The ITP. Any discretion granted by this policy must be exercised in accordance with statutory obligations and must not contravene any legal, regulatory, or accounting requirements.

For more detailed information about how we collect, share, and use your personal data, please refer to the ITP Privacy Notice, available on our website or upon request.

Statement of Policy

The ITP is dedicated to protecting all data in line with its sensitivity and complying fully with applicable legal and regulatory standards.

For this document's purposes, ITP acts as a **Data Controller** when managing the personal data of learners, employees, and applicants. ITP may also act as a **Data Processor** when delivering services on behalf of third-party organisations such as awarding and assessment organisations.

This policy details the personal data held, how it is shared, how long it is retained, and the legal rights of data subjects (identifiable individuals) regarding their information.

Lawful Basis of Collecting and Processing Data

Under Article 6 of the GDPR, The ITP must ensure that processing personal data is lawful by meeting at least one of the following bases:

- **Consent:** The data subject has provided clear consent for their personal data to be processed for one or more specific purposes
- **Contractual necessity:** Processing is required to perform a contract to which the data subject is a party or to take steps at their request prior to entering into a contract.
- **Legal obligation:** Processing is necessary to comply with a legal obligation to which the data controller is subject.
- **Vital interests:** Processing is necessary to protect the vital interests of the data subject or another natural person.
- **Public interest or official authority:** Processing is necessary to carry out a task in the public interest or as part of the official authority vested in the controller.
- **Legitimate interests:** Processing is necessary for the legitimate interests pursued by the controller or a third party, provided these interests are not overridden by the rights and freedoms of the data subject, especially in cases where the data subject is a child.

Procedure

The ITP must protect sensitive personal data from being disclosed or shared with unauthorised individuals. Personal data will be processed lawfully, fairly, and transparently, and only where a valid lawful basis for processing applies.

The Data Protection Officer (DPO) ensures compliance with data protection laws through audits, guidance, risk mitigation, training, and cooperation with authorities. They report to senior management to prioritise data protection and operate independently. Additionally, the DPO responds to data-related inquiries, addresses staff and stakeholder concerns, reviews policies, organises GDPR training, and assists clients and employees in accessing information held about them by The ITP.

All ITP staff and contractors must complete GDPR training and comply with this policy at all times. Breaches may result in disciplinary action.

If you have any questions about this Privacy Notice or would like to contact us about any data protection matter, please use the following contact information.
Data Protection Officer: Hanna Bland
Email: DPO@theitp.org

Types of personal information we collect

Information that we may collect, store, and use include:

- Personal contact details (Name, title, addresses, telephone numbers, and personal email addresses)
- Date of birth
- Gender
- Next of kin/accompanying staff and emergency contact information
- Passport or other proof of identity details.
- Employment status and details
- Previous qualifications and experience
- Residency status in the UK
- If you are a care leaver or have an EHC Plan

"Special categories" of personal data

We will also collect, store, and use the following 'Special categories' of sensitive personal data such as but not limited to:

- Information about your race, religion, ethnicity, and sexual orientation
- Health information, including medical conditions or learning difficulties and disability status
- Criminal convictions and offences
- Household situation

Special category data requires additional conditions for lawful processing under Article 9 of the GDPR. In compliance with the law, we may collect and use such data under the following circumstances:

- The data subject has provided explicit consent for one or more specified purposes.
- Processing is necessary to fulfil obligations or exercise specific rights of the data controller or data subject under employment, social security, or social protection laws, including obligations under the Equality Act and employment law.
- Processing is essential to protect the vital interests of the data subject or another person when the data subject is unable to give consent, though this applies only in critical situations.
- Processing is required for reasons of substantial public interest.

In most instances, processing sensitive personal data will require the explicit consent of the data subject. Exceptions apply in extraordinary circumstances or when required by law, such as complying with health and safety regulations or safeguarding obligations. Consent must clearly outline the specific data involved, the purpose of processing, and any parties to whom the data will be disclosed.

How we use your information provided to us

- Personal information about learners is typically collected during the application or enrolment process.
- Relevant information about parents or guardians is collected from learners.
- Employer information is gathered during the application process.
- Additional personal information may be collected while organising and delivering the Programmes.

Information collected from others

- **Learning Records Service (LRS):** Used to verify prior qualifications, compare them to those declared on enrolment, confirm your Personal Learning Record (PLR), and add this to your evidence pack.
- **Employer:** Information is confirmed with your employer to verify eligibility for enrolment, including name spelling, employee number, workplace location, and branch details.
- **Cognassist:** Learners may undertake a Cognassist assessment to identify additional learning needs. This allows The ITP to provide tailored support, enhancing the learner's opportunity to complete their course. Assessment results are shared with learners for future educational use.
- **Levy Digital Account:** For Apprenticeship courses, information is collected from the Digital Apprenticeship Service account.
- **Criminal Convictions:** Details of criminal convictions are collected, and DBS checks are conducted for staff and certain visitors, such as contractors and volunteers, as required by law. This information is recorded and processed only when necessary.

When data might be used

- **Apprenticeship Matching:** Recruitment and initial candidate sifting.
- **Unique Learner Number (ULN):** Obtained from the Learner Records Service.
- **Enrolment Process:** Managed through Apprentice Learner Management System (LMS).
- **ILR Submission:** Information submitted to the Department for Education (DfE)
- **Teaching Staff:** Involvement of Development Coaches and key teaching and learning staff.
- **Change of Circumstances:** Includes transitions in relation to new providers, redundancy, new employers, or new line managers.
- **Assessment Organisation:** Coordination with relevant assessment bodies.
- **Certification:** Issuance of course completion certificates.
- **DfE funding and satisfaction surveys**
- **Auditors:** Engagement for compliance and quality assurance.

Your Rights regarding your Personal information

Under the GDPR, data subjects have the following rights:

- **Access:** Request access to and obtain a copy of their personal data.
- **Correction:** Request corrections to incorrect or incomplete data.
- **Informed:** You have the right to be informed about how we handle your personal information. This Privacy Notice is one of the ways we provide that information.
- **Restriction:** You have the right to request that we restrict or suppress your personal information. In this case, we would retain the data but not use it.
- **Erasure:** Request the deletion or cessation of data processing when the data is no longer needed for its original purpose. We will assess any deletion request on a case-by-case basis in some circumstances there may be reasons why we need to keep information about you.
- **Object:** You can object to receiving direct marketing from us and challenge how we handle your personal information.

If you would like to exercise any of your rights or have any other queries, please contact us on DPO@theitp.org

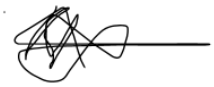
How we keep your personal information secure

We prioritise the security of personal information by implementing robust measures to prevent unauthorised access and ensure data integrity. Paper documents are stored in secure environments accessible only to authorised personnel, and they are securely destroyed when no longer needed. Data stored on computers is safeguarded with strong password protections and advanced security settings that are regularly assessed, updated, and enhanced for optimal security. All data is stored exclusively on secure, regulated company devices that undergo regular backups, and employees are prohibited from accessing company data on personal devices. Data is encrypted before any digital transfer, and sensitive information is never transmitted via email, ensuring maximum protection during communication.

We periodically review and update this Notice to ensure it remains accurate and reflective of our activities, incorporating improvements and addressing any regulatory changes. We encourage you to check it periodically, and if significant updates are made, we will make every effort to inform you directly.

Policy Review

This policy is reviewed annually or as needed.

Signed and Approved By	Charlotte Goodwill
Job Title	Chief Executive Officer
Signature	
Date Signed	22/01/2026

Document Management
Owner: Hanna Bland – Data Protection Officer
Last Review Date: 22/01/2026
Next Review Date: 22/01/2027

Version Control

Version	Date	Change
Version 01	11/12/2024	New document
Version 02	22/01/2026	Removal of all EPAO and ESFA terminology