Data Protection

Introduction and Scope

Inspiring Leaders Teacher Training (ILTT) operates under the data protection framework of Discovery Schools Academies Trust (DSAT), which acts as the **Data Controller** for the purposes of UK data protection law. DSAT's registered office is located at:
NSPCC Training Centre, 3 Gilmour Close, Leicester, LE4 1EZ.

This policy applies to all **staff and trainees** engaged with ILTT. It outlines how we collect, use, store, and share personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Under data protection law, individuals have the right to be informed about how their personal data is used. We meet this obligation through the provision of **privacy notices** (also known as fair processing notices), which are issued to individuals when their data is collected or processed.

ILTT follows the data protection and privacy policies of DSAT. A copy of the relevant Data Protection Policy and Privacy Notice will be provided to all trainees and staff. However, if you are placed in a school outside of the Discovery Trust, please consult your school-based Leaders to access that school's own data protection and privacy policies.

Trainees may have access to confidential pupil data. It is essential that all trainees understand their responsibilities under the **Code of Conduct** and **UK GDPR**. Personal data must not be shared unless there is a lawful basis for doing so, such as safeguarding concerns.
All

Contact Information

If you have any questions or concerns about how your data is handled, please contact:

- **Ben Jordan** – Operations Director at Inspiring Leaders.
  bjordan@iltoday.co.uk
- **Adam Lapidge** – Data Protection Officer at Discovery Schools Trust
  alapidge@discoverytrust.org | 0116 318 4066

If your concern is not resolved to your satisfaction, you may escalate it to the Information Commissioner's Office (ICO):

- Online: Report a concern
- By post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Lawful Bases for Processing Personal Data

We collect and use personal data only when the law allows us to. The lawful bases we rely on include:

- Contractual obligation – where processing is necessary to fulfil a contract with the individual.
- Legal obligation – where we are required to comply with the law.
- Public task – where processing is necessary for us to perform a task in the public interest.
- Vital interests – to protect someone's life in exceptional circumstances.
- Consent – where the individual has given clear permission for us to process their data for a specific purpose.

Where consent is used, individuals have the right to withdraw it at any time. We will always explain how to do this when consent is requested.

Categories of Personal Data Collected

We may collect, use, store, and share the following types of personal data:

- General personal data: contact details, date of birth, gender, next of kin, bank details, recruitment information, qualifications, employment history, performance data, absence records, ID documents, photographs, and usage of IT systems.
- Special category data: racial or ethnic origin, religious beliefs, sexual orientation, health and medical conditions, and disability information.
- Other data: Data collected through secure communication systems.

Data Subject Rights

Under UK GDPR, individuals have rights over their personal data. These include the right to:

- Be informed about how their data is used
- Access their data
- Correct inaccurate data
- Request deletion or restriction of their data
- Object to certain uses
- Receive their data in a portable format

Requests to exercise these rights should be directed to the Data Protection Officer.

Data Retention and Disposal

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, regulatory, or reporting requirements.

- **Retention Periods:** Specific retention periods are defined in our data retention schedule.
- **Secure Disposal:** When data is no longer required, it is securely deleted or destroyed. Paper records are shredded, and digital records are permanently deleted using secure methods.

Data Breach Procedure

In the event of a personal data breach, we follow a simple but compliant process:

1. **Identification:** Any member of staff or trainee who suspects a data breach must report it immediately to the Data Protection Officer (DPO).
2. **Recording:** The DPO logs the breach in a secure Excel-based incident log, including:
   - Date and time of breach
   - Nature of the breach
   - Categories of data and individuals affected
   - Actions taken
3. **Assessment:** The DPO assesses the risk to individuals' rights and freedoms.
4. **Notification:**
   - If the breach is likely to result in a risk to individuals, the DPO notifies the Information Commissioner's Office (ICO) within 72 hours.
   - If there is a high risk to individuals, those affected will also be informed without undue delay.
5. **Review:** The breach is reviewed to identify lessons learned and improve future practices.

Training and Awareness

All staff and trainees must complete mandatory training on data protection and UK GDPR. Completion dates are recorded in a central Excel log maintained by the Operations Team. Refresher training is provided annually or when significant changes occur.

Data Sharing

We may share personal data with third parties where legally required or where it is necessary to fulfil our duties. These include:

- Through secure government systems (e.g., DfE portals)
- With trusted partner organisations with whom we have an established relationship
- Where there is a lawful basis for doing so

Data Security Measures

We are committed to protecting personal data through appropriate technical and organisational measures, including:

- Access Controls: Only authorised personnel have access to personal data, based on role and necessity.
- Password Protection: All systems are protected by strong passwords, which are changed regularly.
- Device Security: All devices used for processing personal data are encrypted and protected by antivirus software.
- Secure Storage: Paper records are stored in locked cabinets. Digital records are stored on secure, access-controlled systems.
- Data Transmission: Personal data is only shared via secure, encrypted channels (e.g., government portals, secure email). Transferring personal data to different IT systems (eg. Different email addresses, Microsoft Teams) is **not** appropriate. This includes data of children. Also refer to our Acceptable Use Policy.
- Regular Backups: Data is backed up regularly and stored securely to prevent loss.
- Incident Response: We maintain a breach log and follow a defined procedure for managing data breaches.
- Training: All staff and trainees receive mandatory data protection training, with completion tracked centrally.

These measures are reviewed annually to ensure ongoing compliance and effectiveness.

Policy Review
This policy is reviewed annually by the Operations Director and the Data Protection Officer to ensure it remains compliant with current legislation and best practice.

Appendix: Data Retention Schedule

This schedule outlines how long different categories of personal data are retained by Inspiring Leaders Teacher Training and the rationale behind each retention period. All data is securely disposed of once the retention period has expired.

Data Type	Retention Period	Reason / Legal Basis
Trainee Records	6 years after completion of training	DfE funding audit requirements and legal claims limitation
Application and Recruitment Data	1 year after recruitment cycle ends	Legitimate interest and safeguarding
Training and Assessment Records	6 years after completion	DfE audit and quality assurance
Safeguarding Records	25 years from date of birth (or longer if required)	In line with statutory guidance (e.g., Keeping Children Safe in Education)
Staff Employment Records	6 years after employment ends	Legal claims limitation and HR best practice
Financial Records (e.g., invoices)	6 years from end of financial year	HMRC requirements
Emails and Correspondence	2 years (unless part of a formal record)	Operational necessity
Complaints and Investigations	6 years after resolution	Legal claims limitation

Secure Disposal Methods:

- **Paper records**: Shredded using cross-cut shredders
- **Digital records**: Permanently deleted using secure deletion tools
- **Third-party disposal**: Proof of destruction is obtained where applicable