Policy Date	January 2025
Review Date	January 2026
Responsible	Scott Kirkham

Data Management Policy

Introduction

Impact Training Academy needs to gather and use certain information about individuals. This can include pupils, commissioners, parents and carers, contacts, employees and other people the organisation has a relationship with or may need to contact. We regularly process and analysis pupil level data from schools and alternative provisions and this policy ensures we handle this sensitively, confidentially and carefully.

This policy describes how personal data must be collected, handled and stored to meet impact Training Academy data protection standards and to comply with the law.

This data management policy ensures Impact Training Academy:

- complies with data protection law and follows good practice
- protects the rights of clients, staff and partners
- is transparent about how it stores and processes individuals' data
- protects itself from the risks of a data breach

Data protection law

The UK General Data Protection Regulation (GDPR) applies in the UK. It outlines that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what's necessary in relation to the purposes for which they're processed.
4. Accurate and, where necessary, kept up to date.
5. Protected – every reasonable step must be taken to ensure that personal data that's inaccurate, having regard to the purposes for which they're processed, is erased or rectified without delay.
6. Kept in a form that permits identification of data subjects for no longer than is necessary, and for the purposes for which the personal data is processed (personal).
7. Stored for longer periods. For example, the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This will also be subject to implementation of the appropriate technical and organisational measures required by UK GDPR in order to safeguard the rights and freedoms of individuals.
8. Processed in a manner that ensures appropriate security of personal data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Policy Date	January 2025
Review Date	January 2026
Responsible	Scott Kirkham

9. Managed by a controller responsible for, and be able to demonstrate, compliance with the principles.

People and responsibilities

Everyone at Impact Training Academy contributes to compliance with UK GDPR. Key decision-makers must understand the requirements and accountability of the organisation to prioritise and support the implementation of compliance.

Scott Kirkham is the named person responsible for data protection in the organisation. They lead on compliance with the regulations, what training is required by whom, and how policy and procedural information is disseminated within the team.

These responsibilities include (but are not necessarily limited to):

1. Documenting, maintaining and developing the organisation's data protection policy and related procedures, in line with agreed schedule.
2. Embedding ongoing privacy measures into policies and day-to-day activities, throughout the organisation. The policies themselves will stand as proof of compliance.
3. Sharing the policy across the organisation, and arranging training and advice for staff.
4. Dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters.
5. Checking and approving contracts or agreements with third parties that may handle the organisation's sensitive data.
6. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
7. Performing regular checks and scans to ensure security hardware and software are functioning properly.
8. Evaluating any third party services the company is considering using to store or process data, to ensure their compliance with obligations under the regulations.
9. Developing privacy notices to reflect a lawful basis for fair processing, ensuring that intended uses are clearly articulated. This will also ensure that data subjects understand how they can give or withdraw consent, or exercise their rights in relation to the company's use of their data.
10. Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the UK GDPR principles.

Policy Date	January 2025
Review Date	January 2026
Responsible	Scott Kirkham

Data Protection Officer (DPO), the person responsible for fulfilling the tasks of the DPO in respect of Impact Training Academy, is Scott Kirkham.
The tasks of the DPO are to:

- inform and advise the organisation and its employees about their obligations to comply with UK GDPR and other data protection laws
- monitor compliance with UK GDPR and other data protection laws – including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, clients)

Scope of personal information to be processed

1. The scope of the data we process:
    - names of individuals
    - postal addresses of individuals
    - email addresses
    - telephone numbers
    - online identifiers
    - pupil level data including academic results, postcodes, safeguarding information, attendance and behaviour data.

Individual client data is collected from enquiries or from contracted projects. Pupil level data is provided by schools, parents and carers, alternative provisions or academy trusts. Any data is shared securely using XXXXXXXX to ensure data is not passed freely across email. Data is stored in encrypted files on XXXXXXX with two-factor authentication, access controls and individual file encryption to increase the security of the data and ensure GDPR compliance.

Any data collected to use in our provision will be limited to the minimum amount needed for a successful outcome for the students. It will be kept whilst the student is on role and for an appropriate time afterwards in line with retention protocols.

Uses for processing

Our data processing includes:

- Analysis of socio-economic and pupil level data to allow staff to understand potential barriers for students.
- Safeguarding information to ensure pupil wellbeing.
- Building knowledge of a students learning gaps and progress.
- Collection and communication with, a group of commissioners.

Policy Date	January 2025
Review Date	January 2026
Responsible	Scott Kirkham

Consent
Where we rely on consent as the lawful condition for processing, we have made sure that consent is freely and unambiguously given for specific purposes, and we can evidence an affirmative action on the part of the data subject to have indicated consent, we clearly show data subjects on mailing lists who is using their personal information, what information, and for what purposes, and using which communications channels. Our systems communicate an individual's right to withdraw consent at any time, and email communication supports the functionality to do this.

Data Sharing
No mailing list, subscriber or customer data will be shared outside the organisation. Pupil level data that allows individual identification will never be shared outside the immediate commissioner unless needed in a safeguarding referral to prevent harm to a pupil. Overall trends and learning from data will only be shared outside of a commissioner and paren/carer with the express, recorded, written permission of the parent/carer.

Security measures
We use xxxxxxx for secure file transfer. Data sent through xxxxxxxx is encrypted both in transit and on server. The accounts have two-factor authentication and files can be password protected. Files can also be shared using restricted access xxxxxxxx with two-factor authentication access and password protection.
Details should be documented here of the technical infrastructure considerations and measures put in place to leverage technology to require or ensure compliance, such as restricting and protecting access to the data to those people for whom it is necessary to perform the processing - such as measures like security software and firewalls, encryption, the use of secure Virtual Private Networks (VPN), log-in restricted access and two step authentications, etc.
Staff are trained in the handling of personal information and use this training in care over laptops and mobile devices. Paper copies of data are rarely used but are held securely when not used and shredded after use.

Subject access requests
All individuals who are the subject of data held by our organisation are entitled to:

- ask what information the company holds about them and why
- ask how to gain access to it
- be informed how to keep it up to date
- be informed how the company is meeting its data protection obligations

Subject Access Requests should be directed to Scott Kirkham and this policy is available for viewing online through our website:
XXXXXXXX

Policy Date	January 2025
Review Date	January 2026
Responsible	Scott Kirkham

The right to be forgotten
Subjects have the right to be deleted from our database. Where this is requested we will delete their details from all records. Where this request comes for pupil level data analysis key data such as exam results or attendance may be kept anonymously and analysed as part of an overall trend before being deleted at the end of the project.

Privacy notices
Impact Training Academy aims to ensure that individuals are aware that their data is being processed, and that they understand:

- who is processing their data
- what data is involved
- the purpose for processing that data
- the outcomes of data processing
- how to exercise their rights

Ongoing documentation of measures to ensure compliance
Meeting the obligations of the UK GDPR to ensure compliance will be an ongoing process we will ensure ongoing compliance by:

- maintaining documentation/evidence of the privacy measures implemented and records of compliance
- regularly testing the privacy measures implemented and maintain records of the testing and outcomes
- use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts
- keep records showing training of employees on privacy and data protection matters