
	Policy BM 01	Version 13	Page 1 of 14	Last updated: 1 April 2025
	Authorised: M Hewitt  01/04/2025	Data protection		Review date: 1 April 2026
Business Management Framework				
Data Protection Policy				

1. PURPOSE AND SCOPE

This Policy defines the arrangements in place across TRN (Train) Ltd, hereinafter Train, that ensures compliance to the requirements of the Data Protection Act 2018 (the “DPA Act”) and the General Data Protection Regulation (the “GDPR”), as relevant to Train’s business interests.

This policy should be read in conjunction with related company policies. These include:

- E-safety & Acceptable Use of ICT - HS08
- Digital Communication and Devices at Work - BM17
- Security Policy - BM25
- Confidentiality Policy - BM02

All employees, Board Directors, self-employed staff and volunteers are required to handle and process data in any of Train’s records or systems in accordance with this policy and in accordance with other related policies concerning the handling or processing of data.

2. INTRODUCTION TO DATA PROTECTION

Both the DPA Act and the GDPR provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice and they set new standards for protecting general data, in accordance with the GDPR, giving people more control over use of their data.

With the GDPR, the definition of personal and sensitive data is:

Personal data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as “special categories of personal data”.

The special categories specifically include:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life; or
- sexual orientation.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

3. THE MAIN ELEMENTS OF THE DPA ACT AND PRINCIPLES OF DATA PROTECTION

The DPA Act contains four main elements that include:

- General Data Processing
- Law enforcement processing
- Intelligence services processing
- Regulation and enforcement processing

The data protection principles within Article 5 of the GDPR requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. PRIVACY NOTICES - RIGHT TO BE INFORMED

All learners, staff, employers and other individuals in receipt of Train's services are entitled to:

- Know what personal data Train collects, the reason for collecting it and how it is used;
- Know how long their personal data will be kept for;
- Know their rights: right to access, right to rectification, right to erasure, right to restrict processing, right to data portability and right to object;
- Know whether their personal data will be transferred outside the European Union, third countries or international organisations;
- Know who Train may share their data with; and
- Know whom to contact to make a complaint or report a concern.

Train will therefore provide all learners, staff, employers and other relevant users with privacy information via privacy notices.

Privacy notices will be included in the appropriate documentation such as course application and enrolment forms and staff recruitment documentation. This information will also be available on the Policies pages of Train's website <https://www.trainltd.org/policies> and on Train's internal network server within the 'Procedures' network drive.

5. RESPONSIBILITIES OF STAFF

Staff are responsible for complying with this policy as it relates to their own and other individual's personal data.

Staff must comply with the staff guidelines for data protection when collecting personal data from learners, employers and other individuals who utilise Train's services. The staff guidelines are located in Confidentiality Policy - BM02.

Staff should also complete the mandatory staff training on Data Protection and GDPR when asked to do so. Failure to do so may result in disciplinary action.

Staff are also responsible for:

- Checking that any information provided to Train in connection with their employment is accurate and up to date.
- Informing Train of any errors or changes with their personal data. Train cannot be held responsible for any errors unless the staff member has informed Train of them.

Staff Working from Home;

- Staff are provided with company laptops, all company equipment has comprehensive cyber security that is routinely updated installed on the devices
- All mobile devices have ESET mobile security to protect and encrypt the data held within the mobile device
- Staff should ensure that their environment is suitable for the work that they are undertaking and that data breaches don't occur due to the suitability of the environment, to this means staff have password protected phones and laptops and must not share these passwords with others within their own homes.
- When taking calls within the home environment staff must where reasonably possible move to a room within their home that is private.
- All personal data transferred within the company is password protected or transferred using internal server platforms.
- Training is provided to all staff on GDPR compliance whilst working remotely.

6. DATA SECURITY

All staff are responsible for ensuring that:

Any personal data has been collected and is being used in a fair and lawful manner.

- Any personal data which they hold is kept securely whether in paper or electronic format.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

- Personal data processed for one reason is not reused for another unrelated reason without seeking the consent of the individual.
- Data is accurate, up to date and is not kept longer than necessary.
- All personal data is treated with a high degree of sensitivity and disposed of by cross-cut shredding.
- Any breach of data security is reported immediately to the Data Protection Officer using the data breach reporting form, which can be located on Train's internal network 'Procedures' drive.

Train will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. All Train users must take reasonable responsibility to ensure the data is accurate and up to date, relevant and not excessive. Any unauthorised disclosure of personal data to a third party by any staff member may result in disciplinary or legal action being taken against them.

Failure to comply with Train's policies and procedures for handling personal data is a disciplinary offence which may be considered gross misconduct and may also involve personal criminal liability.

Paper-based storage

- Paper-based personal data should be kept in a locked room, lockable filing cabinet, drawer or other appropriate storage device.
- All staff should adopt a clean desk policy to ensure that personal data is not left visible on desks that could be viewed by an unauthorised third party.

Electronic storage

- The storage or use of any personal data processed by Train on local hard disk devices such as personal computers or mobile devices must be avoided unless absolutely necessary. The recommended mechanism for using such data is to keep the data on the Train secure network server. Staff must not save personal data to the desktop of their PC, Laptop or any other mobile device.
- All mobile devices containing stored personal data owned by Train must use an approved method to protect data. The definition of mobile devices includes laptops, tablets, smart phones and mobile phones.
- All portable storage devices containing stored personal data owned by Train must use an approved method of encryption to protect data. The use of portable storage devices and unencrypted file sharing mechanisms e.g. Dropbox, We Transfer is prohibited.
- Laptops must have a user name and password to gain access to the device.
- All mobile phones and tablets must be secured with a PIN code as a minimum. The PIN code must not be the factory default code set by the manufacturer.

- Use of personal devices for Train's business must be approved by the Data Protection Officer.
- The loss or theft of any mobile device or portable storage device containing Train data must be reported immediately to the Data Protection Officer and the staff members Line Manager.
- Staff should note that unauthorised disclosure of data or a failure to adequately secure data either paper-based or electronically will usually be a disciplinary matter and may be considered gross misconduct.
- Mandatory renewal of passwords set by Train must be adhered to by all staff.
- Password protection on personal information files must be adhered to by all staff.
- Password protected attachments for personal data and/or sensitive personal information sent by email must be used by all staff. Passwords to access protected attachments must not be disclosed within the same email containing the attachment being sent.

7. PERSONAL DATA BREACH PROCEDURE

Breach definition

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

A non-exhaustive list of potential incidents is shown below:

- Unauthorised use of, access to or modification of personal data or information systems
- Unauthorised disclosure of personal or sensitive data (either deliberate or through not following proper procedures and processes for the security of data)
- Improper sharing of data, or not taking appropriate steps to secure data when transmitting data within the organisation or to authorised agencies
- Loss or theft of confidential or sensitive data or equipment on which data is stored (e.g. USB pen drive, laptop, tablet, mobile phone)

- Attempts (successful or otherwise) to gain unauthorised access to information or IT systems
- Human error
- Unforeseen circumstances e.g. fire or flood – resulting in data loss
- Hacking attack

Train takes the following measures to mitigate any risk of data loss:

- Implements robust policies and procedures
- Ensures relevant training is undertaken by all staff
- The use of lockable cupboards (restricted access to keys)
- Password protection on personal information files
- Setting up computer systems to allow restricted access to certain areas
- Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick) without adequate safeguarding e.g. encryption
- Where personal data can be taken off site, instruction are provided on safe keeping
- Appropriate security data backup procedures are implemented and tested.
- Password protected attachments are used for the transmission of personal data sent by email
- Robust and reliable IT security features
- Robust secure on site IT storage facility
- Ensure robust data sharing agreements exist
- Ensure access controls are relevant to staffing needs and re assess where required
- Measures to ensure safe transfers of data outside of the EU/EEU where cross border sharing is necessary

Reporting an incident

All staff are responsible for reporting a data breach or an information security incident, or suspected incident. The incident must be reported immediately it is known or suspected to the person identified as holding the responsibilities of the Data Protection Officer (DPO). Incidents should also be reported by the individual to their line management or supervisor. If an incident occurs outside of normal working hours, it should be reported as soon as is practicable.

An incident report must be completed by the individual who reports the incident. An incident report form is located on Train's internal network 'Procedures' drive.

Containment and recovery

The DPO will first determine if a data breach has occurred and if the breach is still occurring. If a breach has occurred and is still occurring, then the appropriate steps will be taken to stop the breach immediately and to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with any relevant resources to establish the severity of the breach, assess the risk, and to determine who will take the lead in investigating the breach. This will depend on the nature of the breach. Reference may be made to the Disciplinary Policy if required.

An Investigating Officer (IO) will be appointed and will determine what can be done to contain the breach. The IO will establish who needs to be notified as part of the initial containment, informing relevant authorities which may include the police, supervisory authorities, and individuals depending on the severity of the breach and the level of risk to individuals.

The IO will work with relevant resources to determine the course of action to be taken to ensure a resolution to the incident

Investigation and risk assessment

An investigation will be undertaken by the IO immediately (supported by the DPO and other resources) and wherever possible within 24 hours of the breach being discovered/reported. The IO will investigate the breach and assess the risk associated with it. This will include the potential adverse consequences for individuals, how serious or substantial the risks are, and how likely they are to occur. The impact on Train should also be assessed.

The investigation should take account of the following:

- The type of data involved
- The sensitivity of the data
- The current protection in place
- How did the breach occur (e.g. was data lost or stolen)?
- How could the data be used by a third party (illegal or inappropriate use)?
- Who is affected, numbers involved, potential effects on these data subjects
- Impact on Train
- Wider consequences to the breach under GDPR
- Who to inform

Notification

The IO and/or the DPO, will determine who needs to be notified of the breach. A notifiable breach must be reported to the Information Commissioner's Office (ICO) within 72 hours of Train becoming aware of a breach.

Every incident should be assessed individually, but the following should be considered as part of the decision to notify:

- Whether there are any legal/contractual obligations to notify
- Whether notification would assist the affected individuals to mitigate their risks
- Whether notification would prevent further unlawful use of data

- Who needs to be notified
- How will notification help to protect Train?
- What details will be released in the notification

Where it is necessary to inform the ICO of a breach, Train will provide all relevant facts of the breach and fully document the incident including measures and safeguards in place and how systems and controls were breached. The Board of Directors must be notified in advance of the notification to the ICO.

Notification to the individuals whose personal data has been affected by an incident will include a description of how and when the breach occurred and the data that was involved. Individuals will be advised of actions that have been taken by Train to mitigate any risks. Individuals will be notified of how to contact Train for further information.

Consideration must be given to who should be notified based on the details of the incident. If potential illegal activity is known or is believed to have occurred or could occur as a result of the incident, then agencies such as the police and insurers could also be notified.

The IO and/or the DPO in discussion with the Board of Directors will determine what internal and external communications should take place.

All actions taken should be recorded in the log of the incident.

Evaluation and response

Once the initial incident is contained and any notifications made, Train will undertake a full review of the causes of the breach, the effectiveness of the response(s) to the breach, and whether any changes to systems, policies and procedures are required.

This may include:

- Where personal data is held and how it is stored
- Current identified risks, and potential weaknesses with current measures
- Transmission and transfer of data methods
- Staff awareness
- The evaluation and response process

Existing controls including privacy impact assessments, will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8. RIGHTS TO ACCESS INFORMATION/SUBJECT ACCESS REQUESTS

Staff, learners, employers and other individuals in receipt of Train's services have the right to access any personal data that is being kept about them.

Any person wishing to exercise their right to access their own personal data must make a Subject Access Request. Train has devised a "Subject Access Request" Form which can be completed and forwarded to Train's Data Protection Officer by email, post or by hand delivered. Subject Access Requests can also be made verbally, however further details may be required to enable the processing of the Subject Access Request. Any additional information requested will be fully documented on the Subject Access Request form.

Subject Access Requests may be made directly to the Data Protection Officer or to any staff member. Any member of staff receiving such a request should pass it immediately to the Data Protection Officer who will process the request and respond accordingly. All Subject Access Requests will be logged.

Subject Access Requests made on behalf of someone, including those aged under 18 must be made with the consent of the individual if they are over the age of 13. Proof of that consent will be required. Where Train determines that the individual is not able to give consent, for example, learners with profound and multiple learning difficulties, the information will be provided to the named individual on the learner's file.

There is no charge for Subject Access Requests, however, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, Train may either:

- Charge a reasonable fee taking into account the administrative costs for providing the information or communication or taking the action requested; or
- Refuse to act on the request.

Train aims to comply with requests for access to personal information without undue delay and within one month of receipt of the request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request and Train will agree an extended deadline of up to a further two months.

The requester will receive a copy of the personal data held about them in a concise, clear, transparent and easily accessible form, either in writing or in electronic format, or in another format requested by the requester.

9. RIGHT TO RECTIFICATION, ERASURE, RESTRICTION TO PROCESSING, DATA PORTABILITY AND OBJECTION.

All individuals have the right to request that data held about them be rectified, if it is incorrect or deleted in certain circumstances. Individuals also have the right to object to processing of their data or under certain circumstances restrict their data processing or request their personal data is transferred to another organisation or person.

Anyone seeking to have their data amended, rectified or deleted, or to request that their data not be processed should complete the Data Amendment/ Deletion form, which is available on Train's internal network server within the 'Procedures' network drive.

10. DATA PROTECTION IMPACT ASSESSMENTS

For all new data collections or systems which involve data processing, a data protection impact assessment (DPIA) will be conducted as part of the Project Implementation Document.

Guidance and forms to complete DPIA's are located on Train's internal network server within the 'Procedures' network drive.

11. DATA SHARING AND THIRD PARTY PROCESSING

Where personal data including special category personal data is shared with a third party organisation, this will be covered by a data sharing agreement and/or appropriate wording within contracts. Where Train is processing personal data and any special category personal data on behalf of a Data Controller, the processing of such data will be covered by a written Contract.

Where Train receives requests for personal data from third parties including parents, it will adopt its standard procedures for verifying the identity of the third party and seeking confirmation that the sharing of the data would be fair and lawful.

Data sharing identity verification guidelines are located on Train's internal network server within the 'Procedures' network drive. No data will be shared with a third party unless these assurances are received.

There are occasions when it is necessary for Train to share data with other organisations or people and where consent is required. In such cases Train will seek and gain consent from the Data Subject except where exemptions apply i.e.:

- In order to fulfil legal obligations
- In order to fulfil contractual obligations
- In the vital interests of the individual
- Job Centre Plus
- Learner referral partners
- Department for Education
- Education and Skills Funding Agency
- Office for Standards in Education, Children's Services and Skills (Ofsted)
- The Learner Registration Service
- The Student Loans Company
- Awarding Organisations and End-point assessment organisations
- Employers
- Local authorities
- Police
- HMRC
- UK Border Control
- Other educational bodies or institutions
- Connexions
- Organisations conducting external funding audits
- Prevent teams
- Disclosure and Barring Service
- Apprenticeship Certification England (ACE)
- Construction Skills Certification Scheme

12. SUBJECT CONSENT

In some cases Train can only process personal data with the consent of the individual. If the data is sensitive, express consent must be obtained for some processing. Agreement to Train processing some specified classes of special categories of personal data is a condition of acceptance of a learner onto any course and a condition of employment for staff. For staff, this is also the case for information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. Train has a duty under the Children Act and other enactments to ensure that staff are suitable for the job and learners for the courses offered. Train also has a duty of care to all staff and learners and must, therefore, make sure that employees and those who use Train facilities do not pose a threat or danger to other users.

Train will also ask for information about particular health needs, such as allergies to food or particular forms of medication, or any health conditions such as epilepsy, asthma or diabetes. Train will only use the information in the protection of the health and safety of the individual or for another legal reason.

In instances where consent is given as the primary lawful processing condition, individuals may choose to withdraw their consent. Requests must be submitted in writing using the consent withdrawal form located on Train's internal network server within the 'Procedures' network drive. However where Train has other lawful reasons for processing personal data, it will continue to do so.

13. PROCESSING SENSITIVE/SPECIAL CATEGORY INFORMATION

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender, sexual life or political views or beliefs. This may be to ensure Train is a safe place for everyone, or to operate other Train's policies such as the equality and diversity policy or safeguarding policy.

Due to the sensitive nature of such information, Train will obtain express consent prior to any sensitive data processing.

Due to legal and/or contractual obligations, offers of employment and/or course places may be withdrawn if an individual refuses to consent to this, without good reason.

14. THE DATA PROTECTION OFFICER

The first point of contact for enquirers is to contact Train's Data Protection Officer:

Mark Hewitt
0191 477 0840
gdpr@trainltd.org

15. RETENTION AND DISPOSAL OF DATA

Train won't keep personal data for any longer than is necessary in respect of the reason(s) for which it was first collected. Personal data is only held for as long as required in compliance with any legal, statutory, regulatory or funding contractual obligations for retention. Data is archived as per Train's document retention policy and deleted/destroyed upon expiry of the relevant document retention requirements contained within our funding contract(s).

For ESFA Funding Contracts, personal data is retained for a period of 6 years from the end of the financial year in which Train receives its last programme funding payment. Where funding programmes have been matched funded by the European Social Fund, data is retained for a longer period as detailed below:

ESF Social Fund 2007-2013 programme - 31/12/2022

ESF Social Fund 2014-2020 programme - 31/12/2030

When disposing of any document containing personal data, care should be taken to ensure that the document is shredded before consigning to the waste collection.

Under no circumstances should paper containing personal data be disposed of in waste bins or refuse collections without first being shredded using a cross-cut shredder. Failure to adhere to this, may result in disciplinary action being taken against the staff member.

16. COMPLAINTS PROCESS

Any complaints concerning the processing of personal data should in the first instance be addressed marked private and confidential to the Data Protection Officer at Train, who will investigate the complaint and make a response. The contact details are:

FAO: Data Protection Officer, Endeavour House, Colmet Court, Queensway South, Team Valley Trading Estate, Gateshead, Tyne and Wear, NE11 0EF or email gdpr@trainltd.org.

In the event that complaints are not resolved or properly addressed, a formal complaint can be made to the Information Commissioner's Office (ICO). They can be contacted via their helpline number 0303 123 1113 or can be reported online at <https://ico.org.uk/concerns/>