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.

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.

1. **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.

1. **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.

1. **PRIVACY NOTICES - RIGHTS OF DATA SUBJECTS 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 United Kingdom 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. Refer to Annex A for Train’s privacy notices.

Learners upon enrolment will also receive the ESFA privacy notice and ILR privacy notice. These are available to view using the below links:

[https://www.gov.uk/government/publications/esfa-privacy-notice](https://www.gov.uk/government/publications/esfa-privacy-notice )

[https://guidance.submit-learner-data.service.gov.uk/22-23/ilr/ilrprivacynotice](https://guidance.submit-learner-data.service.gov.uk/22-23/ilr/ilrprivacynotice )

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.

1. **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 section 6 of this Policy.

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 breeches 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.

1. **STAFF GUIDELINES AND RESPONSIBILITIES FOR CONFIDENTIALITY, INTEGRITY, MAINTAINING AND HANDLING OF PERSONAL DATA**

Staff have access to both information passed to them and to knowledge which accumulates in the course of performing their roles and responsibilities. They have a duty to comply with the below measures:

1. treat all personal information with respect and in the best interests of whom it relates too
2. share with their line manager, when appropriate, information given to them in confidence
3. always consult their line manager or director if they are unclear with respect to any area concerning confidentiality, or when made privy to confidential information that may have legal and or criminal connotations, for example: if an individual confides that they have allegedly been submitted to sexual abuse by another individual
4. pass and receive confidential information to and from colleagues on occasions when they have to be replaced because of sickness, holidays or other reasons, in a responsible and respectful manner
5. only to pass confidential information to other agencies with the agreement of the individual it relates to (where possible), with the permission of their manager, or in emergency situations when it is clear that it is in the best interests of the individual or is urgently required for the protection of the individual or another person under the Public Interest Disclosure Act 1998
6. refer to confidential information in training or group supervision sessions with respect and caution and preferably in ways which conceal the identity of the related individual
7. never to gossip about an individual or to pass information to any other individual other than for professional reasons
8. never to gossip about any individual
9. ensure all personal data that is collected is
10. ensure all information requested by telephone should only be transmitted at the approval of the manager and only when the verification of the recipient has been obtained
11. when giving information to others, either in person or via telephone, ensure that confidential information is not able to be overheard
12. keep all electronic access secure i.e. ensuring user logins and passwords are secure and not shared
13. always log off or lock the computer before leaving
14. ensure emails are sent or forwarded to appropriate people only and that the ‘confidentiality’ footer is included

All staff will process data about learners on a regular basis when enrolling learners, producing ILP’s, carrying out initial assessments and marking attendance registers Train will ensure, through enrolment and course application procedures, that all learners are notified of the categories of processing, as required by the law. The information that staff deal with on a day-to-day basis will be ‘standard’ and will cover categories such as:

* general personal details such as name and address;
* details about course attendance and progress; and
* notes of personal supervision, including matters about behaviour discipline.

**Sensitive/Special Category Data**

Information about a learner’s physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive; this may only be processed with the learner’s consent or on the advice and approval of the Data Protection Officer. If staff need to record this information they should seek advice before processing the data.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in this Policy. In particular, staff must ensure that records are:

* accurate
* up-to-date
* fair
* kept and disposed of safely and securely and in accordance with this policy.

Staff should complete annual mandatory Data Protection and GDPR training.

Staff shall not disclose personal data to any other staff member, except with the authorisation in line with this Policy or the agreement of the Data Protection Officer.

Before processing any personal data, all staff should consider the below checklist.

***Staff Checklist for Recording Data***

* Do you really need to record the information?
* Is the information ‘standard’ or is it ‘sensitive’/’special category’
* If it is ‘sensitive’/’special category’, do you have the data subject’s express consent?
* Has the learner been told that this type of data will be processed?
* Are you authorised to collect/store/process the data?
* If yes, have you checked with the data subject that the data is accurate?
* Are you sure that the data is secure?
* If you do not have the data subject’s consent to process, have you sought advice that there is a legal reason to process the data?

The Data Protection Office should be advised of any new collections of sensitive/special category data prior to the data processing starting.

1. **MANAGEMENT AND ADMINISTRATIVE RESPONSIBILITIES**

Confidential information may be occasionally seen by staff other than the staff delivering learning. It is therefore the responsibility of managers to ensure that information is maintained, stored and handled in ways that limit access to those who have a need to know, and to provide the following arrangements in particular:

1. To provide lockable filing cabinets to hold learners’ and staff records and ensure that records are kept secure at all times.
2. To arrange for information held on computers to be accessed only by appropriate personnel, and password encrypted.
3. To locate office machinery and provide appropriate shielding so that screens displaying personal data are hidden from general view.
4. **TECHNICAL FACILITIES AND MEASURES FOR PERSONAL 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 immediatelyto 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.
* Back-ups of Personal Data must be scheduled daily and securely using authorised encrypted Cloud-based Servers, based in the United Kingdom. In the event of corruption or accidental deletion of data, Personal Data must be restored in a timely manner.
* 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.
* Password protection using encryption to AES-256 Security Standards on personal information files must be adhered to by all staff.
* Pseudonymisation of data should be used to replace any personable identifiable data.
* Password protected encryption 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.

**Firewalls**

* All premises that have an office network must have boundary Firewalls in place. Routers installed at sites must meet industry requirements e.g. Draytek.
* Windows Firewall must be enabled on all desktop and laptops used by home-based workers.
* Internet router and hardware firewall devices must have their default passwords changed in line with this security policy i.e. minimum password length of 12 characters and no maximum length restriction. IT Support must action this when installing new routers or Firewall devices.
* Boundary firewalls must be configured to block all services from inside the network from being accessed from the internet.
* Boundary Firewalls are configured (IP locked and non-standard port) to allow access to their configuration settings over the internet. The business case for this is to allow out IT Support Company external access to support and configure any change on the routers and perform maintenance.
* If a user leaves TRN or longer requires access to a system listed in section 5.4, the service/account must be disabled. Services must be reviewed at least on an annual basis to ensure users who no longer require access have it removed.
* Software Firewalls must be enabled on all ICT devices and servers.

**User Access Control and Secure Configuration**

* Access to the network, and any equipment, applications, cloud-based services or other ICT resource must be by individual login, i.e. unique user name and password.
* TRN provides ICT equipment such as desktops, laptops and mobile phones for business use, which are built for compatibility with the TRN’s network and internet connection. TRNs equipment must not be connected to other networks or internet services, except for where employees work from home and therefore must be able to use their own internet services.
* Non-organisation computing equipment must not be used to access TRN’s network resources unless authorised.
* All external use of the network and cloud-based services must be by named individuals only, authorised by the Managing Director.
* The creation of new user accounts is carried out by TRNs authorised IT Support Company. Administrator accounts for carrying out administrative tasks e.g. installing software and User accounts must be separate. IT Support must only use local administrator accounts for configuring new ICT devices.
* Each individual who is authorised to access TRNs network or cloud-based services must have a user profile which limits their access to data, files and software via user privileges and access levels.
* Privileges and access levels must be authorised by a director and set by what the user requires access to do their job role.
* Staff who leave the company, the Managing Director must contact the IT Support Company to remove all access privileges.
* Any staff member who requires Administrator access to ICT systems, a written request must be submitted to a Company director. Approved requests will then be submitted to IT Support for action, however such approval must only be made on a temporary basis and recorded by IT Support with their CRM database.

As soon as Administrator access is no longer required, IT Support must be contacted immediately by a Company director to disable the access and the responsible person must be notified.

* All users must only access, or attempt to access, what is permitted by their profile. If there is any difficulty in accessing files or programmes, IT Support must be informed as soon as possible.
* Where a computer is shared by a number of users, it is essential for all users to log off the computer before leaving it. A user is responsible for all work carried out on a computer using their login details, including internet access and email use, whether or not that user was actually using the computer themselves.
* Administrator Access must be reviewed at least on an annual basis to ensure users who no longer require administrative access to carry out their role have it removed.

**Passwords**

* Passwords must be used in order to access computers, applications, systems and all other networked resources. Company mobile phones must protected using a PIN as a device locking mechanism.
* User account and administrative account passwords must be strong and unique and must be alpha-numeric, and contain a minimum of twelve characters and no maximum length restriction, of which at least one character must be a numeric digit and a special character.
* Passwords must not be common or discoverable, such as birth dates, pet’s names or common key board patterns. Network login / user names must not be used in any form (reversed, capitalised, or doubled as a password) nor any other information easily obtained about the User (such as pet names, car registration numbers, telephone numbers etc.).
* The same password must not be used for more than one application, system, device or service. Passwords cannot be re-used within 24 password changes.
* User account and administrative account passwords are protected against brute-force password guessing. Account Lockout Policy is configured to lockout accounts after 3 unsuccessful attempts within a 5-minute window.
* Our IT support company’s monitoring service alerts engineers on failed logon attempts. If the threshold is met, an engineer will then investigate to see if the issue was a failed attempt to logon by a legitimate user, or if it came from an unknown source. Relevant steps are taken to investigate the attempted breach and security measures put in place to block the brute force attack i.e. block IP address of incoming brute force.

In summary:

**Strong** **Password Do’s and don’ts**

|  |  |
| --- | --- |
| **DO** | **DON’T** |
| Use a password with mixed-case letters | Use a network login ID in any form |
| Use a password that contains alphanumeric characters, and include at least one numeric digit and special characters e.g. ~`! @#$%^&\*()\_-+={[}]|\:;"'<,>.?/ | Use your first, middle or last name or anyone else’s in any form.  Don’t use your initials, nickname, or anyone else’s |
| Minimum of twelve characters and no maximum length restriction | Use information easily obtainable about you - phone numbers, car registration plate, pet names etc. |
| Use a seemingly random selection of letters, numbers and special characters | Use a password of all numbers, dates or a combination |
| Use a password that can be typed quickly without having to look at the keyboard | Use a sample or a default password |

* If a software package comes installed with a default password, that password must be changed immediately after installation.
* Passwords must not be posted in a location accessible by others (such as a note stuck to the monitor, under the keyboard or even in a desk drawer). A password manager can be used to store multiple passwords securely.
* Passwords must NEVER be divulged to or shared with anyone else. There are NO exceptions to this, and if a password is disclosed, and therefore compromised the Information Security Officer must be informed.
* An ICT device must not be left unattended while logged onto a system unless the password protected screen saver has been activated or the device has been locked. Automatic password-protected screensavers will be remotely applied across desktops and laptops, following a period of inactivity of 10 minutes.
* Where files or data need to be shared between individuals the data must be held in a networked, restricted shared folder or other secure environment and password protected.
* Users must remember that they are at all times responsible for anything undertaken with their user ID and password.
* Passwords must be changed promptly by the user if the user suspects their password, account or access to an external service has been compromised. Should the user not be able to change their password, IT Support must be contacted immediately for assistance.
* In all events where a user suspects their password or account has been compromised, IT Support must be contacted so they can perform the necessary vulnerability checks on the user’s suspected ICT devices and accounts.
* Firewall passwords must be changed if they have been compromised or suspected of being compromised. IT Support must be notified immediately to change the respective passwords.
* Multi-factor authentication with a minimum password length of 8 characters and no maximum length restriction must be used when accessing external services e.g. cloud-based software.

**Security Update Management**

* Operating systems must be updated with any high-risk or critical security updates within 14 days of release. Installed operating systems must be fully supported for security updates.
* Auto updates must be enabled on all operating systems. In the event of a failed auto update, IT Support must be contacted immediately to manually install the update.
* High-risk or critical security updates for applications must be installed within 14 days of release.
* Auto updates must be enabled on all Applications. In the event of a failed auto update, IT Support must be contacted immediately to manually install the update.
* Unsupported operating systems or Applications must be removed and replaced with newer supported versions.

**Physical Security**

* All desktop devices, e.g. PC, printer and scanner, must have adequate precautions taken to protect them against theft and accidental damage in addition to environmental threats and hazards. All manufacturer and supplier instructions and advice must be followed.
* Security precautions should, in the first instance, concentrate on adequate building security and sitting of the device in the office, and then may extend to simple lock down devices attached to a desk.
* All ICT hardware purchasing must be coordinated through Commercial Director. This ensures that equipment in use across TRN is consistent, meets appropriate standards and is compatible with existing equipment and network resources. All desktop computer equipment should be turned off when not being used for an extended period of time.
* Equipment will be protected centrally by an Uninterruptible Power Supply (UPS) and where necessary controls must be in place to ensure a clean power supply by eliminating the impact of power spikes.

Portable devices /Removable Media

* When not in use all portable devices such as laptop computers must be retained in a secure environment. This may include a lockable store cupboard with controlled access, or lockable metal cabinets in larger alarmed offices, but again with controlled access.
* When portable devices are taken off premises all Users must ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times, e.g. not left visible but locked away.
* No portable devices must be left in an unattended vehicle at any time.
* The Managing Director must make users aware of insurance arrangements and the user’s obligations before allowing the device to be taken off the premises.
* Users who travel with TRN laptops must make regular backups of data contained on the laptop.
* Laptop computers must not be connected to the network unless anti-virus and malware software has been updated.
* Records must be maintained within the department or service which detail their portable devices including type, serial number and software available, and include provision for signing out and return.
* Portable devices must only be used in connection with authorised business use on behalf of TRN.
* Portable devices must never contain any more data than is the absolute minimum required.
* All computer consumables must be retained in a secure environment wherever possible and issued only for TRN’s business. Consumables must not be used for private purposes.

**Installation of Software**

* Only software for which TRN is licensed may be installed upon any company ICT device. It is the responsibility of each user to ensure that the correct licensing arrangements are followed when installing software. However, this is assumed to be correct when installation is arranged through IT support, who will retain records relating to current licences and software packages in use. Unused software, bloatware and unnecessary Apps must be removed.
* Administrator accounts must be used to install software and not standard user accounts, as these must be separate. IT Support must only use local administrator accounts for configuring new ICT devices.
* Appropriate action will be taken against any user found to have installed software that is not properly licensed or if the software is being used contrary to its license agreement.
* Modifications to existing software are generally discouraged, and in any case must be progressed through IT support and where appropriate be subject to Change Control procedures.

**Testing of technical facilities and measures**

* Train holds Cyber Essentials Plus accreditation and regularly tests its technical facilities and measures to ensure Personal Data is stored securely, is accessible only to authorised personnel and can be accessed and restored in a timely manner from backup facilities in the event of an incident.

1. **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
* Regularly tests, assesses and evaluates the effectiveness of technical facilities and measures
* 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 UK 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.

1. **RIGHTS OF DATA SUBJECTS 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 immediatelyto 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.

1. **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.

**13. 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.

**14. MAINTAIN RECORDS OF DATA PROCESSING ACTIVITIES**

Records of data processing activities, covering areas such as processing purposes, data sharing and retention must be maintained and available for review and audit. Specifically, records must contain the below information which is a GDPR legal requirement:

* The name and organisation contact details (including where applicable, other data controllers, organisation representative and organisation data protection officer).
* Subject matter of the Processing.
* Duration of the Processing.
* The nature and purposes of Data Processing.
* Type of personal data to be collected.
* A description of the categories of individuals and categories of personal data.
* Details of any transfers outside the UK and/or to third countries including documenting the transfer mechanism safeguards in place (if applicable).
* Retention and destruction schedules.
* A description of technical and organisational security measures.

**15. DATA SHARING, THIRD PARTY PROCESSING AND TRANSFER OF PERSONAL DATA OUTSIDE THE UNITED KINGDOM OR TO AN INTERNATIONAL ORGANISATION**

Where personal data including special category personal data is shared with a third party organisation based in the United Kingdom, legal safeguards are in place to share such information in the form of a data sharing agreement and/or appropriate wording written into Contractual clauses.

Although no personal data is transferred outside the United Kingdom or to an international organisation, the same legal safeguards plus additional checking of UK ‘adequacy regulations’ and appropriate safeguards such as IDTA or Binding Corporate Rules and risk assessments are in place, should there be a requirement to do so for a restricted transfer of data in the future.

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

**16. DATA SUBJECT CONSENT**

Train can only process personal data with the active, informed consent of the individual. This includes personal data that is sensitive, as express informed consent must be obtained for 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.

All consents must be accurately recorded and retained securely for audit purposes. This applies to both paper-based and electronic records.

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.

**17. 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.

**18. 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](mailto:gdpr@trainltd.org)

**19. MAINTAIN RECORDS OF PERSONAL DATA PROCESSING ACTIVITIES, 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 maintained and 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 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.

**20. 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/>

**Annex A**

**PRIVACY NOTICE - LEARNERS**

**BACKGROUND**

TRN (Train) Ltd. understands that the personal data that you share with us and your privacy is important to you. We genuinely do care about the privacy of all our learners, customers, employees, subscribers to our newsletters and website visitors and will only collect and use personal data in ways that are described in this privacy notice, and in a way that is consistent with our legal obligations and your rights under the law. This privacy notice explains who we are, what personal data is collected from you, how we use, hold and process your personal data and who we might share your data with. It also explains your rights under the law relating to your personal data.

**WHO WE ARE?**

TRN (Train) Ltd is a private independent training provider based in Gateshead, Tyne and Wear, delivering a wide range of short courses, accredited qualifications, apprenticeships and traineeship programmes.

Our head office address is: TRN (Train) Ltd, Endeavour House, Colmet Court, Queensway South, Team Valley Trading Estate, Gateshead, Tyne and Wear, NE11 0EF. Our main telephone number is: 0191 477 0840.

Our data protection representative and Data Protection Officer Contact details are:

Mark Hewitt

0191 477 0840

gdpr@trainltd.org

**WHAT IS PERSONAL DATA?**

Personal data is defined by the General Data Protection Regulation (GDPR) as ‘any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier’. Personal data is, in simpler terms, any information about you that enables you to be identified, for example, your name, address and contact details.

**WHAT PERSONAL DATA DO WE COLLECT?**

We may collect some or all of the following data:

Title, forename, surname, previous surnames, address, date of birth, age, NI number, time at address, employer name, employer address, telephone number, mobile number, email address, learning disabilities, learning difficulties, prior qualifications, no. of contractual hours worked, employment status, emergency contact details, initial assessment scores for English and maths, length of employment, residency status, job role, ethnicity, gender, shoe size, health problems, disabilities/health problems, religion/belief, sexual orientation, previous experience, skills and knowledge and career aim / ambitions.

Leaners whom are currently unemployed, in addition to the above we also collect the following data: benefit type, job centre office, personal advisor name and contact number, no. of month’s unemployed and household information.

Financial information - bank details.

**HOW DO WE USE YOUR PERSONAL DATA?**

Your personal data will primarily be used for purposes relating to you enrolling and studying towards one of our courses/learning programmes. We also collect your personal data for the following purposes:

* Processing applications, enrolments and individual learning plans
* Maintaining learner records
* Registration, examinations, achievement and certification
* E-portfolio and paper-based portfolios for qualifications studied
* Funding claims
* Safeguarding
* Health and Safety
* Equality and Diversity monitoring
* Learner support
* Sharing information, news, and offers about our services.
* To contact individuals in response to a specific enquiry
* To improve the services offered and delivered to individuals
* Sharing your contact details with the Office for Standards in Education, Children’s Services and Skills (Ofsted) and Awarding Organisations including External Quality Assurers for the purpose of interviewing / feedback in relation to our teaching, learning and assessment delivery to you.
* To contact individuals after they leave their course/learning programme to gather information about their destination
* Provision of information, advice and guidance to learners and clients
* Processing of personal data also includes the use of CCTV in order to monitor and maintain the security of the premises and for the prevention or detection of crime.

**WHO MIGHT WE SHARE YOUR DATA WITH?**

There are occasions when it is necessary for TRN (Train) Ltd. to share your personal data with other organisations or people. Where consent is required we will ask you for this, except where exemptions apply. We do not need your consent to share your personal data with the below list of organisations, because we lawfully have either a legitimate interest, contractual obligation or legal obligation to do so, where required.

* 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

**LAWFUL BASIS FOR PROCESSING PERSONAL DATA**

Our lawful basis for processing your personal data as set out in Article 6 of the GDPR is:

* For processing enquiries, application forms and enrolments, the lawful basis is a legitimate interest
* For SMS text reminders sent to individuals to attend induction days and SMS text reminders sent to individuals to confirm course commencement, the lawful basis is a legitimate interest
* For updating learner referral partners on learner attendance at induction, whilst on course/learning programme and upon exit of their course/learning programme, the lawful basis is a legitimate interest
* For sharing your contact details with the Office for Standards in Education, Children’s Services and Skills (Ofsted) and Awarding Organisations including External Quality Assurers for the purpose of interviewing / feedback in relation to our teaching, learning and assessment delivery, our lawful basis is a legitimate interest and contract.
* For accessing individual personal learner records (PLR’s), maintaining learner records, processing CSCS waiver forms, individual learning plans and information relating to an individual’s course/learning programme, the lawful basis is legitimate interest and contract.
* For obtaining learners financial bank details for reimbursement of travel expenses and/or weekly attendance allowance, the lawful basis is legitimate interest and contract.
* For gathering information about the destination of an individual once they have left their course/learning programme, the lawful basis is legitimate interest and contract.

As set out in Article 9(1)(a), processing “special categories” of data where you have given consent, TRN (Train) Ltd., will process certain sensitive information about you with your consent.

**TRANSFER OF YOUR PERSONAL DATA OUTSIDE THE UNITED KINGDOM OR INTERNATIONAL ORGANISATIONS**

We do not transfer your personal data outside the United Kingdom or International organisations.

**HOW LONG WILL WE KEEP YOUR PERSONAL DATA?**

We won’t keep your personal data for any longer than is necessary in respect of the reason(s) for which it was first collected. Your personal data could be kept for a number of years to meet any legal, statutory and regulatory obligations.

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 our document retention policy and deleted/destroyed upon expiry of the relevant document retention requirements contained within our funding contract(s).

Data is retained for a period of 6 years from the end of the financial year in which we received the last funding payment for your programme. 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 2014-2020 programme - 31/12/2030

**YOUR RIGHTS**

Under the GDPR, you have various rights with respect to our use of your personal data:

**Right to Access** - you have the right to request a copy of the personal data that we hold about you. This is referred to as making a ‘Subject Access Request’.

**Right to rectification** - you have the right to correct personal data that we hold about you that is inaccurate or incomplete. Please let us know if any of your personal data is not accurate or changes, so that we can keep your personal data up-to-date.

**Right to erasure** - you have the right under certain circumstances to ask for your personal data that we hold to be erased from our records.

**Right to restrict processing** - In certain circumstances, you have the right to request that we restrict the further processing of your personal data.

**Right to data portability** - You have the right to have the personal data that we hold about you transferred to another organisation.

**Right to object** - you have the right to object to certain types of processing of your personal data.

Rights to not be subject to decisions based solely on automated processing including profiling - we do not carry out any automated processing leading to an automated decision based on your personal data.

Please note that the GDPR sets out exceptions to these rights.  If we are unable to comply with your request due to an exception we will explain this to you in our response.

**WHO CAN I CONTACT IF I HAVE ANY QUESTIONS OR CONCERNS?**

If you have any questions or queries which are not answered by this Privacy Notice, or have any potential concerns about how we may use the personal data we hold, please write to the Data Protection Officer at TRN (Train) Ltd, Endeavour House, Colmet Court, Queensway South, Team Valley Trading Estate, Gateshead, Tyne and Wear, NE11 0EF or email gdpr@trainltd.org.

If your complaint is not resolved to your satisfaction and you wish to make a formal complaint to the Information Commissioner’s Office (ICO), you can contact their helpline on 0303 123 1113 or report a concern online at <https://ico.org.uk/concerns/>

You also have the right to judicial remedy against a legally binding decision of the ICO where you consider that your rights under this regulation have been infringed as a result of the processing of your personal data. You have the right to appoint a third party to lodge the complaint on your behalf and exercise your right to seek compensation.

**PRIVACY NOTICE CHANGES**

This Privacy Notice is regularly reviewed to ensure that we continue to protect your personal data and privacy. We reserve the right at all times, to update, modify or amend this Notice. Any changes that we make will not significantly change how we use personal data that you have already given to us without your prior agreement.