Policy No: 225

GDPR - DATA PROTECTION AND CONFIDENTIALITY POLICY

Introduction and purpose

Steadfast Training Ltd is legally required to comply with the General Data Protection Regulation 2018 (GDPR) which replaces the Data Protection Act, 1998. In addition, it is Company Policy to ensure that every employee maintains the confidentiality of any personal and Company data held by The Company in whatever form. This requirement is covered within each employee's Contract of Employment, which they sign on commencement of employment.

This Policy defines the requirements of GDPR and The Company's philosophy and expectations of its staff pertaining to issues of Data Protection and Confidentiality as specifically relating to Learner, Employer, Personnel and Business data and information. A separate Policy No. 200 covers the Collection, Processing, Storage, Archiving and Retention of Learner records in more detail.

In addition, this Policy also provides guidance on what is or is not considered confidential, together with details of the processes in place for the keeping of all applicable records within The Company.

If there is any element of doubt then the information or situation should be treated as confidential until guidance is sought from a member of the Senior Management Team (SMT), Directors or Chief Executive Officer (CEO).

1. Responsibilities

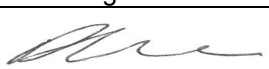
The purpose of this policy is to ensure that all employees of Steadfast Training Ltd are aware of their responsibilities with respect to data protection laws. Everyone within the organisation has a responsibility to protect the confidentiality and the integrity of all personal data we collect.

All staff and contractors must comply with this policy and:

Ensure that they keep all personal data that they collect store, use and come into contact with during the course of their duties confidential.

Not release or disclose any personal data to unauthorised personnel internally and externally to the organisation.

Take all necessary steps to ensure that there is no unauthorised access to personal data by other staff or by people outside of the organisation who are not authorised to do so.

Version	Owner	Author	Signature	Date	Changes made	Next Review
5	HR	Carole Parnell		Jan 2026	Removed the ESFA reference	Jan 2027

2. Purpose

The purpose of this policy personal data relates to all information collected and processed by Steadfast Training Ltd that relates to an identifiable individual.

The personal data we process will be for the following individuals (Data subjects)

Employees existing and former

Consultants/contractor existing and former

Apprentices/Learners existing and former

Recruitment candidates

Visitors

3. Data Controller and Data processer

Steadfast Training is both a data controller and a data processor:

Data controller as we hold and make decisions about the collection of use and data held by us about employees

Data processor as we collect and process data on behalf of the Education & Skills Funding Agency and the Department for Work and Pensions.

Information Commissioners Office

Steadfast training Ltd is registered with the (ICO) as follows registration number Z9666546

4. General Principles

Steadfast Training Ltd is required to keep certain information about its' employees, customers and suppliers for legal, financial and commercial reasons, to enable it to monitor performance, to ensure legal compliance and for health and safety purposes. In accordance with these legal requirements, it is Company Policy that information must only be collected and processed fairly, stored safely, not disclosed to any other person unlawfully and deleted securely when no longer required. All sensitive and personal data shared via email both internally and externally will be sent via secure technology, for example Encryptmail or similar secure encryption.

As set out in Article 6 of the GDPR we consider our main lawful bases for processing are:

a. Legal obligation – Processing is necessary to comply with the law.
b. Public Task – Processing is necessary to perform a task in the public interest or for an official function and the task or function has a clear basis in law.
c. Legitimate Interest – Processing is necessary for our legitimate interests or the legitimate interest of a third party.

Furthermore, The Company upholds the principles stipulated in the GDPR for the handling of personal information as identified in our Privacy Notice Policy P225a, and that such information will be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than is necessary
- processed in line with an employee's rights as applicable
- kept securely
- not transferred to countries outside the UK without adequate protection.

1. Information held by Steadfast Training Ltd

Information held by Steadfast Training Ltd generally falls into three categories:

1.1. That which relates to organisations or individuals which are supported or funded by the Department for Education and relates to, but is not exclusively concerning:

1.1.1. Information which is kept to enable The Company to prove learning and eligibility.

1.1.2. Information about learners and employers may be shared with specified partner organisations or statutory agencies, but is not disclosed to anyone else.

1.1.3. Information is kept for statistical analysis purposes e.g. ethnicity and disability of users and monitoring equal opportunities and reporting back to funders.

1.2. That which relates to employees:

1.2.1. H.R. records encompass a wide range of data relating to individuals who are employed by The Company, including but not limited to: pay details, absence levels, hours worked and holiday entitlement, next of kin, CRB (DBS) check, initial interview assessment, recruitment references, appraisal and performance reviews, job changes, promotions and pay rises, details of training undertaken and qualifications achieved, as well as any Disciplinary warnings, where relevant, and within the qualifying period for retention. (See Disciplinary Policy and Procedure No. 107 for details.)

1.2.2. The Company maintains an effective and secure system for storing HR data, both to ensure compliance with all relevant legislation (for example in respect of the minimum wage or working time regulations) as well as to support sound personnel administration and broader H.R. strategy.

1.3. That which relates to suppliers and associate companies with whom Steadfast Training Ltd does business.

2. Access to Information – Subject Access Request (SAR)

2.1. Information that is confidential to Steadfast Training Ltd as a Company, may be passed to colleagues, line managers or Directors to ensure efficient business operations and the best quality service for learners.

2.2. Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.

2.3. Learners and their employers have the right to access any personal information or records held in their name or that of their Organisation except when that information is pertaining to an issue of safeguarding. (See Policy P209 Safeguarding/PREVENT and 209a Safeguarding Code of Conduct Behaviour)

2.3.1. All requests for access to or copies of personal information will be dealt with within one calendar month of receiving the application verbally, via email or in writing, we will ask for this in writing but we will accept the former.

2.3.2. or authorised representative of an Organisation and sent as an attachment to our designated email: gdpr@steadfasttraining.co.uk

2.4. Employees have the right to know what personal information The Company holds about them and the purpose for which it is used. If an employee, for whatever reason,

wishes to see their personal file they must apply in writing to the Finance and HR Controller.

2.4.1. The Company will not remove information from an individual's file prior to their viewing it.

2.4.1.1. Information can only be withheld, however, if releasing it would make it more difficult to detect a crime or the information relates to national security.

2.5. Employees' requests will be processed by The Company who will arrange for the applicable access to the requested personal data within one calendar month of receiving the application verbally via email or in writing. Employees will be asked to do so in writing but we will accept the former. All requests relating to personal information whether from learners, employers or staff will follow the same process.

2.6. The GDPR applies equally to CCTV, email and internet monitoring of employees; for example to detect crime or excessive private use of e-mails, internet use etc.

2.6.1. Employees have all agreed to being monitored in this way by signing their Contract of Employment, in which it states that it is Steadfast Training Ltd's Policy to carry out this type of monitoring, and for what purposes.

2.6.2. If an employee feels that The Company has misused information or hasn't kept it secure they can raise a grievance under the Grievance or Anti-Harassment and Bullying Policies, as appropriate. If considered serious enough or satisfaction not achieved by this means, an individual may contact the Information Commissioner's Office.

2.7. CCTV is also used to monitor access to Steadfast Training Ltd's premises in order to ensure the safety of staff and learners. Appropriate warning and information notices about this are appropriately displayed.

2.8. If the Company is requested to provide personal information to a third party e.g. A Bank, Building Society, Landlord, etc. Whilst the request may be genuine, The Company will always seek the permission of the learner or employee concerned in writing before supplying the information.

3. Data Security

3.1. Steadfast Training Ltd will take all necessary steps and actions to ensure Data Security – as described within this Policy, and within the IT Computer Usage Policy No. 114.

3.2. The Company expects its' employees to protect Data security by ensuring that:

3.2.1. They do not withhold information from their line manager, when reasonably asked to provide it, unless it is purely personal and unrelated to the situation.

3.2.2. Any personal data that they hold, whether in electronic or paper format, is kept securely. (See IT Computer Usage Policy No. 114 for details)

3.2.3. Personal information is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.

3.2.4. Items that are marked 'personal' or 'private and confidential', or appear to be of a personal nature, are opened by the addressee only.

3.2.5. They do not use their office address, electronic or land address for matters that are not work related.

3.2.6. Confidential conversations regarding individuals or specific cases are conducted in a private location, that is one which offers privacy not to be overheard or interrupted by others

3.2.7. When photocopying or working on confidential documents, they take every precaution to ensure the privacy of such documents by using the secure printing access code allocated to individual's and ensure that they are not left where they can be seen by others.

3.2.7.1. This also applies to information on computer screens.

3.2.8. Sensitive or personal documents should not be left out when not in use or at the end of the working day, and duplicate documents must be destroyed by secure shredding unless they contain additional information which needs to be kept.

4. Storing Information

4.1. General non-confidential information about organisations is kept either in unlocked filing cabinets with open access to all staff or The Company's intranet.

4.2. Hard copy Information about all learners and other individuals is kept in locked filing cabinets by the Contracts and Compliance Department. These colleagues must ensure line managers know how to gain access. For further details relating to learner's records, please refer to Policy No. 200 Archiving and Retention of Learner Records.

4.3. Access to electronic Data will be restricted to necessary Job Roles within Contracts and Compliance and Delivery depending on the Data involved.

4.4. The GDPR applies to all personnel records, whether held in hardcopy or digital format.

4.4.1. Hard copy Employees' personnel information will be kept in locked filing cabinets by the Finance and H.R. Controller and will be accessible to them, the H.R. Representative and Managing Director, as well as members of the Senior Management Team on request to the Finance and HR Controller.

4.4.2. Electronic records will have restricted access by the Finance and HR Controller and HR representative.

4.5. In an emergency situation, the CEO may authorise access to files by Directors or members of the Senior Management Team.

4.6. In accordance with GDPR, data will only be kept for the length of time necessary for a particular purpose.

4.6.1. Certain documents such as employment contracts and personnel records, accident record books, the GDPR Access and Incident Log and other learner personal data and information would need to be produced in circumstances of legal action being taken against The Company. Consequently, the originals must either be available, or The Company would have to explain what happened to the original documents, backed up by what is known as a 'statement of truth'.

4.7. When Data reaches its expiry date, or at the request of the individual concerned, it is destroyed securely and effectively, by shredding or data cleansing of Computer records. The destruction of the data will be confirmed by Steadfast Training Ltd in writing.

5. Duty to Disclose

5.1. There is a legal duty to disclose some specific information including:

5.1.1. Issues of safeguarding. (Policy 209/209a)

5.1.2. Issues that would be deemed to be a criminal offence or breaking the law which The Company would be legally obliged to disclose to the police, such as Drug trafficking, money laundering, acts of terrorism/PREVENT or treason.

5.2. In addition, if employees believe that an illegal act has taken place, or that a colleague or learner is at risk of harming themselves or others, they must report this

to the designated person for Safeguarding who will report it to the appropriate authorities

5.3. Disclosure information is always kept separately from an employees personnel file or the learner's personal records, in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

6. Breach of Confidentiality

6.1. No employee shall, during or after their employment with Steadfast Training Ltd, disclose confidential information belonging to The Company.

6.2. Employees who are uncomfortable with the conduct or actions of other colleagues should raise this with their line manager in the first instance or invoke the Grievance procedure (see Policy No. 108) or Anti Harassment and Bullying Policy (see Policy No. 109) if necessary, and not discuss their dissatisfaction outside of this process.

6.3. Employees accessing unauthorised files without permission or breaching confidentially either deliberately or through negligence, will face disciplinary action and in certain circumstances may find themselves subject to a criminal prosecution. Ex-employees breaching confidentiality may face legal action.

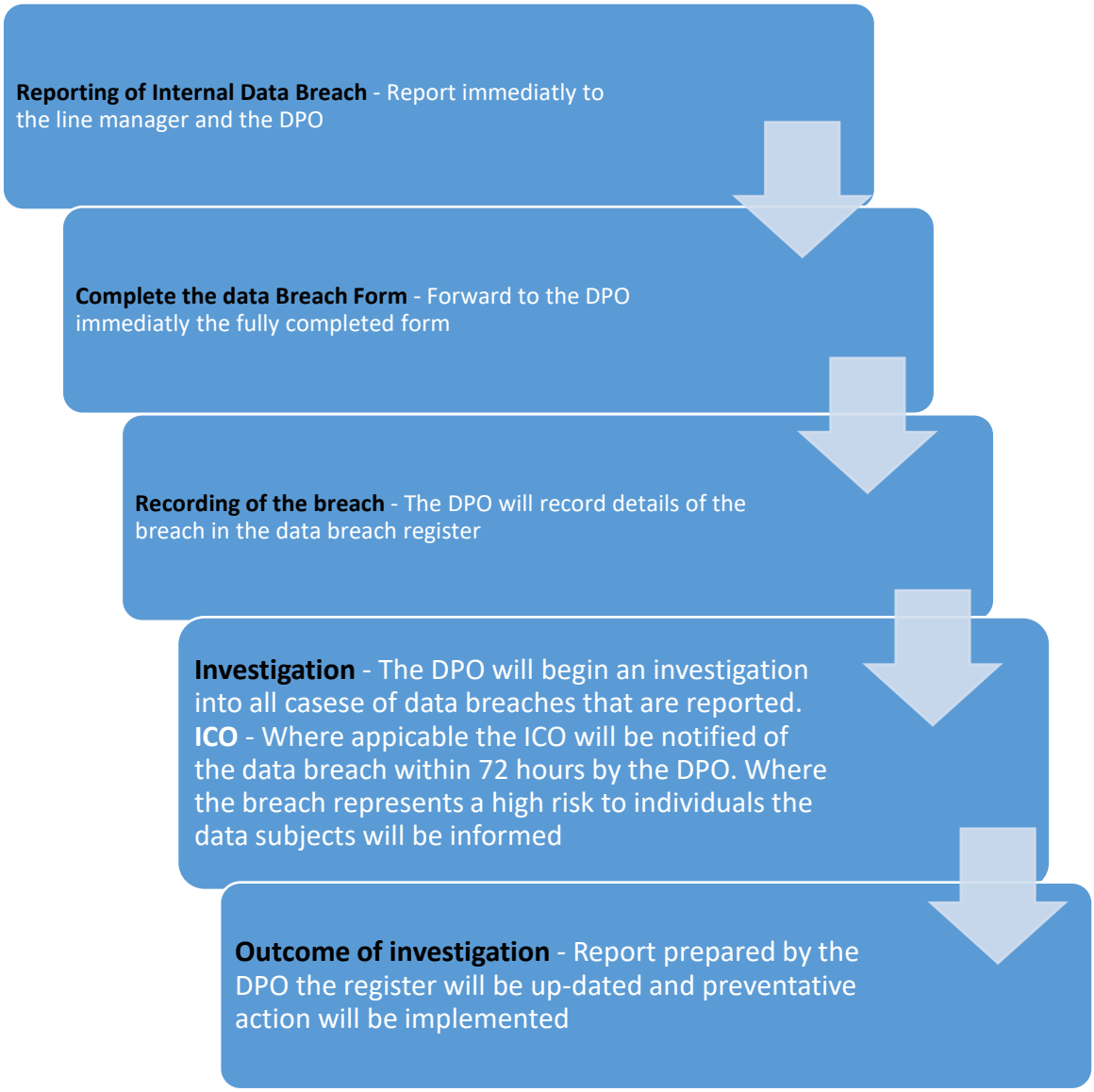
6.4. A possible data breach and or data concern within the organisation will be notified immediately to the data protection officer.

A data breach and or a data concern from outside the organisation should be notified to the DPO.

The organisation will follow guidance from the ICO in determining if a data breach is reportable.

The organisation maintains a register of all data breach incidents and concerns

Policy No: 225



Version	Owner	Author	Signature	Date	Changes made	Next Review
5	HR	Carole Parnell		Jan 2026	Removed the ESFA reference	Jan 2027