# DATA PROTECTION AND DOCUMENT RETENTION POLICY

# Data Protection and Document Retention Policy

## 1 Data Protection Policy

1.1 Skills to Group needs to keep certain information about its employees, learners and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Skills to Group must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 (GDPR) and revisions. In summary these state that personal data shall be:

i) processed lawfully, fairly and in a transparent manner in relation to individuals;

ii) 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;

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

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

v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 freedom of individuals; and

vi) 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.

1.2 Skills to Group and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Skills to Group has developed the Data Protection and Document Retention Policy.

## 2 Status of the Policy

2.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Skills to Group. Any failures to follow the policy can therefore result in disciplinary proceedings.

2.2 Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with their Line Manager who will report it to the Data Controller or another member of the SMT. If the matter is not resolved it should be raised as a formal grievance.

## 3 Notification of Data Held and Processed

3.1 All staff and learners and other users are entitled to:

i) know what information Skills to Group holds and processes about them and why
ii) know how to gain access to it
iii) know how to keep it up to date
iv) know what Skills to Group is doing to comply with its obligations under the DPA 2018 (GDPR) and its revisions

## 4 Responsibilities of Staff

4.1 All staff are responsible for:

i) checking that any information that they provide to Skills to Group in connection with their employment is accurate and up to date
ii) informing Skills to Group of any changes to information, which they have provided i.e. changes of address
iii) checking the information that Skills to Group will send out from time to time, giving details of information kept and processed about staff
iv) informing Skills to Group of any errors or changes. Skills to Group cannot be held responsible for any errors unless the staff member has informed Skills to Group.

4.2 If and when, as part of their responsibilities, staff collect information about other people, (i.e. about learners coursework, opinions about ability, references to other academic institutions or details of personal circumstances), they must comply with the guidelines for staff, which are in Appendix 1.

## 5 Data Security

5.1 All staff are responsible for ensuring that: Any personal data which they hold is kept securely. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

5.2 Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out in 5.3 to 5.7 inclusive will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

5.3 Personal information should be; kept in a locked filing cabinet; or in a locked drawer; or if it is computerised, be password protected; or when kept or in transit on portable media the files themselves must be password protected or encrypted.

5.4 Personal data should never be stored at staff members' homes, whether in manual or electronic form, on unencrypted laptop computers or other personal portable devices or at other remote sites.

5.5 Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at

other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller (see 11 below) must be obtained, and all the security guidelines given in this document must still be followed.

5.6 Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

- Suitable backups of the data exist
- Sensitive data is appropriately encrypted
- Sensitive data is not copied onto portable storage devices without first consulting a Data Controller, in regard to appropriate encryption and protection measures
- Electronic devices such as laptops, mobile devices and computer media (USB devices, CDs etc.) that contain sensitive data are not left unattended when offsite.

5.7 For some information the risks of failure to provide adequate security may be so high that it should never be taken home. This might include payroll information, addresses of learners and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of the Data Controllers within the Senior Management Team.

## 6 Learner Obligations

6.1 Learners must ensure that all personal data provided to Skills to Group is accurate and up to date. They must ensure that changes of address, etc. are notified to an appropriate member of staff.

## 7 Rights to Access Information

7.1 Staff, learners and other users of Skills to Group have the right to access any personal data that is being kept about them either on computer or in certain files.

7.2 In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing, in the first instance to the HR Department.

7.3 Skills to Group aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 15 working days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

## 8 Production of Skills to Group Information

8.1 Information that is already in the public domain is exempt from the DPA 2018 (GDPR). It is Skills to Group's policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

i) names and contacts of Skills to Group Directors
ii) list of staff
iii) policy documents
iv) annual accounts

## 9 Subject Consent

9.1 In many cases, Skills to Group can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Skills to Group processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

9.2 Some jobs or courses will bring the applicants into contact with children, including young people below the age of 18. Skills to Group 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. Skills to Group also has a duty of care to all staff and learners and must therefore make sure that employees and those who use Skills to Group's facilities do not pose a threat or danger to other users.

9.3 Skills to Group will also ask learners for information about particular health needs, such as allergies to particular forms of medication, or any medical conditions such as asthma or diabetes. Skills to Group will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

9.4 Therefore, all prospective staff and learners will be asked to sign a consent to process data, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

## 10 Processing Sensitive Information

10.1 Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender and family details. This may be to ensure Skills to Group is a safe place for everyone, or to operate other Skills to Group policies, such as the sick pay policy or equal opportunities policy.

As this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and learners will be asked to give express consent for Skills to Group to do this.

Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

## 11 The Data Controller

11.1 Skills to Group is the data controller under the DPA 2018 (GDPR), and the board is therefore ultimately responsible for implementation. However, there is are designated data controllers who deals with day to day matters.

11.2 Skills to Group has designated 2 data controllers, who are the primary authorisation for receipt and supply of data requests.

They are:

- Data, Funding and Premises Manager
- IT Manager

## 12 Examinations and Assessments

12.1 For the purposes of this policy, all candidates' exam-related information – even that not considered personal or sensitive under the DPA/GDPR – will be handled in line with DPA/GDPR guidelines.

12.2 Learners will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide.

## 13 Retention of Data

13.1 Skills to Group will keep some forms of information for longer than others. Information should not be kept indefinitely, unless there are specific requirements. In line with principle 5 of the GDPR, information should not be kept longer than is necessary.

13.2 Appendix 2, gives a breakdown of timescales for the retention of various types of information.

13.3 When data is no longer required it should be appropriately destroyed through confidential waste disposal.

## 14 Conclusion

14.1 Compliance with the GDPR is the responsibility of all members of Skills to Group. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Skills to Group facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.

**Document Control**

This policy will be reviewed every year or earlier if deemed necessary

Date Last Reviewed: August 2025

Date to be Reviewed: August 2026

**Authorised By**

**Signed**



**Mark Boulting**
**Managing Director**

**Appendix 1 - Staff Guidelines for Data Protection**

1 All staff will process data about learners on a regular basis, when marking registers, or Skills to Group work, writing reports or references, or as part of a pastoral or supervisory role.

Skills to Group will ensure through registration procedures, that all learners give their consent to this sort of processing, and are notified of the categories of processing, as required by the DPA 2018 (GDPR). The information that staff deal with on a day-to-day basis will be standard and will cover categories such as:

i) general personal details, for example name and address
ii) details about class attendance, course work marks and grades and associated comments
iii) notes of personal supervision, including behaviour and discipline

2 Information about a learner's physical or mental health; sexual life or orientation; political or religious views; trade union membership; biometrics (where used for identification); health; or ethnicity or race is sensitive and can only be collected and processed with the learners consent. If staff need to record this information, they should use the Skills to Group standard form.

For example: recording information about dietary needs, for religious or health reasons prior to taking learners on a field trip or recording information that a learner is pregnant, as part of pastoral duties.

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

i) accurate;
ii) up-to-date;
iii) fair;
iv) kept and disposed of safely, and in accordance with Skills to Group policy

4 Skills to Group will designate staff who will be the only staff authorised to hold or process data that is:

i) not standard data; or
ii) sensitive data

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary;

i) in the best interests of the learner or staff member, or a third person, or Skills to Group; and
ii) he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

This should only happen in very limited circumstances e.g. a learner is injured and unconscious, but in need of medical attention, and a staff member tells the hospital that the learner is pregnant or a Jehovah's Witness.

5 Authorised staff will be responsible for ensuring that all data is kept securely.

6 Staff must not disclose personal data to any learner, unless for normal academic or pastoral purposes, without authorisation or agreement from the person involved, or in line with Skills to Group policy.

7 Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated Data Controller, or in line with Skills to Group policy.

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

9 Staff checklist for recording data:

i) do you really need to record the information?
iii) is the information 'standard' or is it 'sensitive'?
iii) if it is sensitive, do you have the data subject's express consent?
iv) has the learner been told that this type of data will be processed?
v) are you authorised to collect/store/process the data?
vi) if yes, have you checked with the data subject that the data is accurate?
vii) are you sure that the data is secure?
viii) if you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the learner or the staff member to collect and retain the data?
ix) have you reported the fact of data collection to the authorised person within the required time?

## Appendix 2 - Data Retention Schedule – Summary

1. Purpose of this document

A vital part of Skills to Group's Data Protection Policy and practice is that personal data is retained by Skills to Group for the appropriate period of time – neither too long nor too short. The Data Protection Policy states that it is the Skills to Group's policy to:

- retain all information only for as long as specified in the Data Retention Schedule and, in general, no longer than two years plus the current year

This document is a summary of the Data Retention Schedule, and gives an indication of the kind of personal data which needs to be retained for longer than the maximum two years stipulated in the policy.

N.B. While this document summarises and clarifies the Data Retention Schedule, running to 113 pages, it does not supersede it.

The time limits for those items subject to legislation as specified in detail in the Data Retention Schedule (and outlined in Section 3 below) remain in force, and should be referred to in cases of doubt.

2. Current plus two-year rule

As stated in the Data Protection Policy, personal data should not be held by Skills to Group for more than two years after it ceases to be current, unless there is a specific reason for doing so (see Section 3 for the specific categories requiring different retention periods).

The definition of current will vary according to the personal data: for example, it will mean until the course has finished where it relates to learners, or until a member of staff has ceased being employed by Skills to Group where it relates to staff.

It should be remembered that the 'current plus two years' rule is a maximum period for retention. If there is no need to keep the personal data that long, then it should be disposed of securely before the two year time-limit.

3. Exceptions to the two-year rule

This section gives a guide to the categories which have legislation determining the length of time for which personal data within that category should be retained. An indication is given to the main section of the Data Retention Schedule dealing with this category.

**Examples and Retention Period**

**Learner Records**
• Enrolment forms, transfers, withdrawals, disciplinary, appeals
• Exams data

Current year plus six

**Financial Records**
• Purchase ledger, sales ledger, cash book payments etc.
• Payroll data

Current year plus six

**Complaints**
• Correspondence with complainants

Current year plus 6

**Contractual Arrangements**
• Service level agreements
• Legal contracts
• Tender documentation

Life of contract plus six years

**Governors' Papers**
• Articles and instruments
• Agendas and minutes of meetings

Current year plus six

**Data Protection/FOI Requests**
• Correspondence regarding DP/FOIA requests

Current year plus six

**Personnel Records**
• Attendance records - holiday/leave, personal/domestic leave, parental leave, maternity leave
• Flexible working requests
• Return to work discussions and occupational health reports
• Employment tribunal records
• Pension
• References
• Disclosure certificates
• Disciplinary and grievance
• Redundancy
• Recruitment

Personnel Data Retention Schedule from six months to 18 years

**Health and Safety Records**

• Please refer to director responsible for Health and Safety

Retention Schedule up to 10 years

- **All of the above documents that relate to ESF Match Funding must be kept until 31/12/2030**