

DATA PROTECTION AND UK GDPR POLICY

Policy Author	Sam Collins
Approved by	Si Ung
Position	Data & AI Director
Approved date	12/03/2026
Signed	
Next review date	12 Months from Approval
Version 2	Version 3



1. Skills4 contact details

Web Address	Home Skills4Group
Info	Info@skills4group.co.uk
Telephone	01617940528

INTRODUCTION

I&F Limited, T/A Skills4Group is committed to a policy of protecting the rights and privacy of individuals (which includes Learners, staff and others) in accordance with the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018.

The Skills4 Group needs to process certain information about its staff, learners, and other individuals it has dealings with for administrative purposes. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and Learners of the Skills4 Group. Any breach of the Data Protection Act 2018 or the Skills4Group's UK GDPR Policy is considered to be an offence and in that event, disciplinary procedures may apply. As a matter of good practice, other parties and individuals working with the Skills4 Group, and who have access to personal information, will be expected to have read and comply with this policy.

Background to the Data Protection Act 2018

The Data Protection Act 2018 enhances and widens the scope of the previous Data Protection Act 1998. Its purpose is to protect the rights and privacy of individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Definitions (Data Protection Act 2018)

Personal Data

Data relating to an individual who can be identified from that information or from that data and other information in possession of the data controller. This includes name, address, telephone number, identification number. It also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, and criminal convictions. Sensitive data is subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes obtaining and recording data, accessing, altering, adding to, merging, deleting data, retrieval, consultation or use of data and disclosure or otherwise making available of data.

Third Party

Any Individual/organisation other than the data subject, the data controller or its agents.

Relevant Filing System

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Responsibilities under the Data Protection Act 2018

The Office Manager acts as the Data Protection Officer and is responsible for day to day data protection matters and for developing data protection awareness.

All staff in managerial roles are responsible for developing and encouraging good information handling practice within the Skills4Group.

Compliance with data protection legislation is the responsibility of all members of the Skills4 Group who process personal information.

Members of the Skills4 Group are responsible for ensuring that any personal data supplied to the Skills4Group are accurate and up to date.

The Data Protection Act 2018

All processing of personal data by Skills4 Group must comply with the Seven Principles of Data Protection, as set out in Article 5 of the UK GDPR. These are:

1. Lawfulness, Fairness and Transparency
Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. Purpose Limitation
Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **Data Minimisation**
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**
Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
5. **Storage Limitation**
Personal data must be 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.
6. **Integrity and Confidentiality (Security)**
Personal data must be 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.
7. **Accountability**
The data controller is responsible for, and must be able to demonstrate, compliance with the above principles.

Data Subject Rights

Under the UK General Data Protection Regulation (UK GDPR), individuals (Data Subjects) have the following rights regarding the processing of their personal data:

- **Right of Access (Subject Access Request - SAR):**
Data Subjects have the right to request access to the personal data Skills4 Group holds about them, including information about how their data is being used and to whom it has been disclosed.
- **Right to Rectification:**
Individuals can request the correction of any inaccurate or incomplete personal data held about them.
- **Right to Erasure ("Right to be Forgotten"):**
In certain circumstances, individuals can request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

- **Right to Restrict Processing:**
Data Subjects may request that the processing of their personal data is restricted in specific cases, such as when contesting the accuracy of the data or objecting to its processing.
- **Right to Data Portability:**
Where applicable, individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another data controller.
- **Right to Object:**
Data Subjects have the right to object to the processing of their personal data for direct marketing purposes and, in certain situations, to other types of processing based on legitimate interests or public tasks.
- **Rights Related to Automated Decision making and Profiling:**
Individuals have the right not to be subject to decisions made solely by automated means, including profiling, where such decisions have legal or similarly significant effects.
- **Right to Lodge a Complaint:**
Data Subjects have the right to lodge a complaint with the Information Commissioner's Office (ICO) if they believe their data protection rights have been infringed.

To exercise any of these rights, Data Subjects should contact the Data Protection Officer (DPO) using the contact details provided at the end of this policy.

Data Breach Notification

In the event of a personal data breach, Skills4 Group will assess the impact and risk to data subjects. If a breach is likely to result in a risk to the rights and freedoms of individuals, Skills4 Group will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it. Data subjects affected by a high risk breach will also be notified without undue delay.

Data Protection Impact Assessments (DPIAs)

Skills4 Group will conduct Data Protection Impact Assessments (DPIAs) for processing activities that are likely to result in a high risk to the rights

and freedoms of individuals. DPIAs will identify risks, assess their impact, and outline measures to mitigate those risks.

Automated Decision Making and Artificial Intelligence (AI) Processing

Skills4 Group may use systems and technologies that incorporate Artificial Intelligence (AI) or automated decision-making tools to support its business operations. This includes platforms and software that may assist in analysing data, generating insights, or streamlining administrative processes. However, Skills4Group does not rely solely on automated processes to make decisions that produce legal effects or significantly impact individuals without meaningful human involvement.

Where AI or automated processing is used, Skills4Group will ensure that:

- Individuals are informed when automated decision making is involved in processing their data.
- No significant decisions affecting individuals will be made solely by AI or automated means without human review.
- Appropriate safeguards are in place to protect individuals' rights, including the right to request human intervention, express their views, and contest any automated decisions.
- AI tools used in data processing will be subject to regular review to ensure compliance with data protection principles, including fairness, transparency, and accountability.

Skills4Group recognises its responsibility to ensure that any AI technologies used in data processing are applied ethically and in accordance with UK GDPR requirements and the Skills4 AI Policy.

Consent

Personal data will only be processed where a lawful basis under Article 6 of the UK GDPR is satisfied. These lawful bases include consent, contract, legal obligation, vital interests, public task, or legitimate interests. **Consent is one lawful basis, but it is not always required if another lawful basis applies. Skills4 Group will only seek consent where it is the appropriate and necessary basis for processing.**

Where consent is used, Skills4 Group understands this to mean that the data subject has been fully informed of the intended processing and has actively agreed, whilst being in a fit state of mind to do so and

without pressure being exerted upon them. Consent obtained under duress or through misleading information will not be considered valid. There must be clear communication between both parties, such as the individual signing a form freely of their own accord. Consent cannot be assumed from silence or non-response.

For special category (sensitive) data, explicit written consent will be obtained where required, particularly in cases where the data is used or disclosed outside of routine activities like registration.

In most instances, consent to process personal and sensitive data is gathered through Skills4 Group's standard forms (paper based or digital), which will clearly explain the purpose of data collection and who the data may be shared with. Where data may be published online (e.g., on a website or social media), specific consent will be sought, as this data can be accessed globally.

If an individual objects or withdraws consent for certain types of processing (such as direct marketing), Skills4 Group will take appropriate steps to ensure that the processing does not continue, unless another lawful basis applies that overrides the objection, in which case the individual will be informed.

Data Security

All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that they are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it.

Staff should form a judgement based upon the sensitivity and value of the information in question but always consider keeping personal data in a lockable room with controlled access, or in a locked drawer or filing cabinet, or if computerised, password protected or kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without

password protected screensavers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and Learners who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data.

Data Access Rights

Members of the Skills4 Group have the right to access any personal data that is held by the Skills4Group in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Skills4Group about that person.

Data Disclosure

The Skills4 Group must ensure that personal data are not disclosed to unauthorised third parties which include family members, friends, government bodies, and in certain circumstances, the Police. All staff and Learners should exercise caution when asked to disclose personal data held on another individual to a third party.

For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Skills4Group business. Best practice, however, would be to take the

contact details of the person making the enquiry and pass them onto the member of the Skills4 Group concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. The individual has given their consent (e.g. a Learner/member of staff has consented for the Skills4 Group corresponding with a named third party).
2. Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other Skills4 Group employees, if it is clear, that those members of staff require the information to enable them to perform their jobs).
3. Where the institution is legally obliged to disclose the data (e.g. awarding bodies, funding agencies)
4. Where disclosure of data is required for the performance of a contract (e.g. informing a Learner's LEA or sponsor of course changes/withdrawal etc).

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security.
- Prevention or detection of crime, including the apprehension or prosecution of offenders.
- Assessment or collection of tax duty.
- Discharge of regulatory functions (includes health, safety and welfare of persons at work).
- To prevent serious harm to a third party.
- To protect the vital interests of the individual, this refers to life and death situations.

Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the Skills4 Group, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even

confirming whether or not an individual is a member of the Skills4 Group may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally, a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the Skills4 Group may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer.
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of "the Skills4 Group " to avoid confirming their membership of their presence in or their absence from the institution.

Retention and Disposal of Data

Skills4 Group will only keep personal data for as long as it is needed. Retention periods are determined by statutory and regulatory requirements, including ESFA and Awarding Organisation guidelines. While we collect a lot of data on current staff and learners, once someone leaves, it's unlikely we'll need to keep all of that information. Some data will need to be kept for longer to meet legal, funding, or auditing requirements, but anything that is no longer necessary will be securely disposed of once its retention period has expired. Data will not be kept "just in case" and will only be held for as long as there is a clear business or legal need.

Learners

In general, electronic Learner records containing information about individual Learners are kept indefinitely and information would typically

include name and address on entry and completion, programmes taken, examination results, awards obtained.

The Registry and other departments should regularly review the personal files of individual Learners in accordance with the Skills4Group's Learner Records Retention Schedule.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

Publication of the Skills4Group Information

All members of the Skills4 Group should note that the Skills4 Group publishes a number of items that include personal data and will continue to do so. These personal data are:

- Internal Telephone Directory.
- Committee / other handbooks
- Learner pass lists including grades. if applicable
- Information in prospectuses (including photographs), alumni newsletters, etc.
- Staff information on the Skills4 Group website/intranet (including photographs).

It is recognised that there might be occasions when a member of staff, a Learner, or a lay member of the Skills4 Group, requests that their personal details in some of these categories remain confidential or are restricted to internal access.

All individuals should be offered an opportunity to opt out of the publication of the above (and other) data. In such instances, the Skills4 Group should comply with the request and ensure that appropriate action is taken.

Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

Review and Monitoring

This policy will be reviewed annually or sooner if required by legislative or regulatory changes. Feedback from Learners, staff, and stakeholders will inform updates to ensure the policy remains effective and relevant.

Raising Concerns

The named Data Protection Officer (DPO) at Skills4 Group is: **Si Ung**

The DPO is responsible for overseeing Skills4 Group's compliance with data protection laws, managing data subject rights requests (such as Subject Access Requests), providing guidance on data protection issues, and acting as the main point of contact with the Information Commissioner's Office (ICO).

Any concerns, breaches, or questions relating to Data Protection or UK GDPR should be raised immediately with Si via email at si.ung@skills4group.co.uk