Data Protection, Security of Information Policy
January 2020

Policy Group: Data Protection, Security of Information
Policy Number: 5.1
Policy Title: Data Protection Policy
Date and current version: January 2020
Review Date: January 2021

Scope

This policy sets out Skills4's rules on data protection and the eight data protection principles contained within the Act. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of Personal Data.

The policy does not form part of the formal contract of employment, but it is a condition of employment that employees and associates abide by the rules and policies made by Skills4. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any employees, who consider that the policy has not been followed in respect of Personal Data about themselves, should raise the matter with the Data Coordinator initially. If the matter is not resolved it should be raised as a formal grievance.

Data Subjects may include employees, associates, contractors, learners, customers and suppliers and relatives of any of the forgoing. For purposes of the remainder of this document references to employees should be taken to include associates. The information processed may relate to present, past and prospective Data Subjects. In addition, we may be required by law to collect and/or process certain types of Data to comply with requirements of Government departments and regulatory agencies.

Purpose

As a Data Controller Skills4 need to collect and process information including personal information about the people it deals with (data subjects) in order to operate effectively and efficiently.

Comment

Skills4 ("the Company") is fully committed to compliance with the requirements of the Data Protection Act 2018 ("the Act"). The company will therefore follow procedures that aim to ensure that all employees, contractors, agents, assessors or other servants of the company who have access to any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the Act.

Employees should note that unauthorised disclosure will usually end in disciplinary action and may be judged as gross misconduct. The Information Commissioner maintains a public register of data controllers. Skills4 is registered as such.

The Data Protection Act 2018 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

Policy Statement

In order to operate efficiently, Skills4 must collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

Skills4 regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with who it carries out business. The company will ensure that it treats personal information lawfully and correctly.

To the end the company fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

The principles of data protection

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and, shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and where necessary, kept up to date
5. Shall not be kept for longer than is necessary for that purpose or those purposes
6. Shall be processed in accordance with the rights of data subjects under the Act.
7. Shall be kept secure i.e. protected by an appropriate degree of security.
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data and "sensitive" personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data.
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin.
- Political opinion.
- Religious or other beliefs.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- Criminal proceedings or convictions.

Handling of personal/sensitive information Skills4 will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the right of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information within the statutory 40 days.
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, Skills4 will ensure that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriate supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will follow approved procedures.

All managers and employees within Skills4 will take steps to ensure that personal data is always kept secure against unauthorized or unlawful loss or disclosure and will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems are protected using secure passwords, which where possible have forced changes periodically.
- Individual passwords should be such that they are not easily compromised.

All employees are responsible for:

- Checking any information that they produce in connection with their employment is accurate and up to date
- Informing Skills4 of any changes in information
- Informing Skills4 of any errors in personal data

All contractors, consultants, partners or agents of the company must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the company and that individual, company, partner or firm.
- Allow data protection audits by the company of data held on its behalf (if requested).

- Indemnify the company against any prosecutions, claims, proceedings, actions or payments of compensation or damages without limitation.

All contractors who are users of personal information supplied by the company will be required to confirm that they will abide by the requirements of the Act regarding information supplied by the company.

Rights to access information

Data Subjects have the right to access and Personal Data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete Skills4's "Access to Information" form and forward it to the nominated Data Coordinator as appropriate.

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 using the standard form attached (Form 1).

Skills4 will make a charge to Data Subjects of £10 on each occasion that access is requested, although there is discretion to waive this.

Skills4 aims to comply with request for access to Personal Data as quickly as possible but will ensure that it is provided within 40 days of receiving your 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.

Data Subjects also have certain rights under the Act to require Skills4 to cease processing or using their Personal data if it causes them unwarranted damage or distress. Further information will be provided if required.

Subject Consent

In some, Skills4 can only process personal data with the consent of the individual. If the data is Sensitive Personal Data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs within Skills4 will bring the applicants into contact with children, including young people between the ages of 16 and 18. Skills4 has a duty under the Children Act and other enactments to ensure staff are suitable for the job offered. Skills4 also has a duty of care to all staff and customers and must therefore make sure that employees and those who use Skills4's facilities do not pose a threat or danger to other users.

Skills4 will also ask for information about health needs, such as allergies to forms or medication, or any conditions such as asthma or diabetes. Skills4 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.

Therefore, all prospective staff and associates will be asked to sign a Consent to Process Form, regarding types of information when an offer of employment is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure Skills4 is a safe place for everyone, or to operate other organisational policies, such as sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognized that the processing of it may cause concern or distress to individuals, staff and customers will be asked to give express consent for Skills4 to do this. Offers of employment may be withdrawn if an individual refuse to consent to this, without good reason. More information about this is available from the Data Controller and from Line Managers.

The Data Controller and Designated Data Coordinators

Skills4 is a Data Controller under the Act, and the Managing Director is ultimately responsible for its information. However, the designated Data Controller (s) will deal with day to day matters.

At present Skills4 has one Data Controller who is the Office Manager

Data Processors

Skills4 must ensure that any Data Processor or any third party of the Data Processor will not misuse Skills4 Data or process it in any way incompatible with Skills4's specified and lawful purpose for that Data. Therefore, adequate controls must be in place, and relevant wording included on contracts with all Data Processors and third parties.

Retention of Data of employees

Skills4 will keep some forms of information for longer than others. In general information about staff will be kept for a maximum of 10 years after they leave Skills4. This will include:

- Name and address (including email address)
- Promotion/development whilst at Skills4
- Relevant academic achievements whilst at Skills4
- Copies of and reference written

Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information for job references. A full list of information with retention times is available from Human Resources.

All other data, including any information about health, race or disciplinary matters will be destroyed within 6 years of the employment ending subject to statutory requirements. Student work and assessment records will be kept for 3 years.

Skills4 has a statutory responsibility to ensure compliance with the eight principles of the Act. There is therefore a responsibility for compliance placed on staff and personal liability may arise where irresponsible or neglect noncompliance occurs. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, 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 coordinator.

Records Retention Schedule (RRS)

This is a list detailing the length of time for which Skills4 undertakes to keep each class of records. The retention schedules are based on legislative requirements and the retention periods are those recommended by JISC for use within the FE sector, but other legal advice may be taken on an ad-hoc basis. Retention periods apply to the record and to any associated index data held with the record. Audit trail data should be held for at least if the record but may be held longer.

The retention schedule will capture:

- Type of data
- Person responsible
- Disposal
- When and who it will be disposed by

And covers the following functions:

- Quality
- MIS
- Business Development

Staff are responsible for ensuring the Data Coordinator has up to date records of data held and will do so using the Data Information Template.

Document Retention for ESF

Skills4 have robust systems and controls in place to maintain and monitor access to documentation throughout the retention period.

All documents (including any electronic information) are readily accessible to requests from auditors and DWP upon request and stored in accordance with DWP standards.

Documentation must be retained as a minimum to meet audit requirements until at least 31 December 2022 is included below:

No.	Document/Information
1	Evidence on the 2-way conversation/action planning to support fee payment as detailed in Work Programme Guidance
2	Participant Action Plan or Development Plan
3	Sustainable Development Policy and Action Plans
4	Equality and Diversity Policy and Action Plans
5	Marketing and Publicity documents including Marketing/Communication plans and products produced to promote ESF to participants
6	Supporting information for job and sustainment claims detailed in programme specific guidance
7	Supporting information to validate the agreed Progress Measures as detailed in the ESF Families with Multiple Problems Guidance
8	Evidence to support the assessment and decision on eligibility for the ESF families with multiple problems programme secondary referral route
9	Document Retention Policy and Plan

Disposing of Data

Data will be disposed of through either confidential shredding or purging from the company servers.

Disposal of Computer and IT Equipment

Where computer equipment is disposed of, all data shall be removed and storage media such as hard disks, Tablets, iPads and USB memory sticks will be “electronically” shredded or a similar procedure to ensure that data can’t be “reclaimed”.