# Data Use and Data Management Policy.

**Introduction**

Each of the services and products provided by the Federation for Industry Sector Skills and Standards (The Federation) collects, holds and manages data about individuals and organisations. We do this to provide a service to each person and organisation. We recognise our fundamental need to ensure that this information is accurate and secure. We go beyond the needs of any legislative requirements. The secure management of data is central to the way that we work and ingrained into the DNA of the Charity.

None of the information provided is used beyond the Federation, for marketing purposes.

This policy sets out how we collect, store and manage data and who is responsible for this. It also sets out how you can request your data and how, if it is incorrect, you can ensure we get it right. This includes ensuring how we protect your data.

**Why we have this policy**

This policy ensures the Federation and its partners:

- Comply with all data protection legislation (GDPR and DPA 1998) and follow the good practice set out by the Information Commissioner
- Protect the rights of customers, partners and staff
- Are open about how it collects, stores, manages, processes and protects individuals' and organisations' data
- Protect themselves from the risks of a data breach.

**What services does this policy cover?**

This policy covers all the Federation's products and services:

- ACE (Apprenticeship Certificates England)
- ACW (Apprenticeship Certificates Wales)
- MAO (Modern Apprenticeship Online)
- ACE360
- HR Flow
- The Assessors Guild (AG)

**Data protection law**

The Data Protection Act 1998 (DPA) implemented the EU Data Protection Directive in the UK. It introduced an extensive data protection regime by imposing broad obligations on those who collect personal data, as well as conferring broad rights on individuals about whom data is collected. It covers both paper based and electronic information.

The DPA sets out eight data protection principles, which require that:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met (e.g. consent, where necessary to carry out a contract with the individual, or for your "legitimate interests") and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met (more stringent, e.g. explicit consent).
2. Personal data 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. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose, or purposes, shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Data Protection Act 1998 will be added to by the General Data Protection Regulation (GDPR) of the European Union in May 2018. The GDPR will become part of UK law and replace the DPA 1998. Our policy takes account of these changes. It provides additional protections to individuals and organisations. These include:

- A clearer definition of:
  - Data Controller (This is the Federation). Responsible for all the data you provide (regardless of whether the Federation collects it)
  - Data Processor (those who collect and/or process the data you provide) This applies to the:
    - Certification Bodies and Training Providers for ACE/ACW/MAO
    - End Point Assessment Organisations, External Quality Assurance Organisations, Training Providers and Employers for ACE360
    - Employers (licence holders) and their employees for HR Flow, and
    - Members of the Assessors Guild (Assessors and End Point Assessment Organisations), Assessors, End Point Assessment Organisations and service providers to the Assessors Guild
- An extension of the data covered. This is extended to cover all paper and online data, including electronic identifiers such as IP addresses.
- Enhanced requirements to notify individuals and organisations affected by a data breach.
- Increased sanctions against those organisations shown to not meet the requirements of the GDPR.
- The introduction of an "Accountability Principle". It requires Data Controllers and Data Processors to be explicitly clear about how they comply with the data protection principles (e.g. by documenting decisions taken in respect of processing activities) and what their lawful basis is for collecting and processing personal data is. Organisations will be expected to put into place proportionate, but comprehensive, governance measures. This includes how long information will be held. There are 6 legal bases for collecting and processing data:
  - 6(1)(a) – Consent of the data subject (ACE/ACW)

  - 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract (MAO/ACE360/AG/HR Flow)
  - 6(1)(c) – Processing is necessary for compliance with a legal obligation (ACE/ACW)
  - 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
  - 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (ACE/ACW)
  - 6(1)(f ) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject
- The need for the individual or organisation to give consent by some form of clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute consent. It must also be verifiable. This means that some form of record must be kept of how, and when, consent was given. Individuals and organisations have a right to withdraw consent at any time.
- Any data held on individuals aged under 16 needs to demonstrate that consent was provided by not just the individual, but also their parent or guardian.
- Some new rights and strengthened existing rights:
  - the right to be informed
  - the right of access
  - the right to rectification
  - the right to erasure
  - the right to restrict processing
  - the right to data portability
  - the right to object
  - rights in relation to automated decision making and profiling.

Our policy meets, and goes beyond, these legal requirements.

**Scope of the Federation's Data Use & Data Management policy**

This policy applies to:
- All Federation staff.
- All contractors to the Federation, using any data provided to them by the Federation.
- Data processors, as defined in the section above.

Its scope applies to all:
- Personal and contact data (including name, address (postal and email), telephone numbers, date of birth, gender, ethnicity, language/form of communication, marital status).
- Employer details and contact data.
- Training Provider details and contact.
- Qualifications taken and achieved.
- Leave and sickness information for employees on HR Flow.
- Skills and competences and ratings based on past performance (including information about Special Educational Needs).
- Documents relating to an individual.
- Any other data required for the individual service provided.

**Purposes for which data can be used**

The data that the Federation holds, as Data Controller, can **only** be used for the following purposes:

- Ensuring the correct issuing of Apprenticeship Framework certificates in England, Scotland and Wales.
- Investigation into fraudulent claims of public funds for Apprenticeship Frameworks in England and Wales.
- Managing the secure exchange of information, to improve the efficiency of the Apprenticeship Standards system in England.
- Managing the storage of information relating to Technical and Apprenticeship assessment and the views of Employers and Apprentices, regarding that assessment.
- Managing the storage and analysis of employee records for individual businesses and the provision of benchmarking data for the users of HR Flow.
- Providing information to users of Federation services about ACE360, the Assessors Guild and HR Flow.
- Research into the demand and supply of skills, competences, qualifications and Apprenticeship certificates issued.

The data that the Federation holds as Data Controller **cannot** be used for the following purposes:

- Marketing to individuals and organisations by third parties.

**Data protection risks**

This policy helps to protect the Federation, as the Data Controller, and its partners, as Data Processors, from some very real security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals and organisations should be free to choose how the Federation uses data relating to them.
- Reputational damage. For instance, the Federation, and as a consequence, individuals and organisations could suffer if hackers successfully gained access to sensitive data.

**Responsibilities at the Federation**

Every member of the Federation team is aware of their data responsibilities, but some have additional responsibilities and accountabilities:

- The Board of Directors and Trustees is ultimately responsible for ensuring that the Federation meets its legal obligations.
- The Finance, Audit and Risk (FAR) Committee of the Federation manages the Data Use and management policy on behalf of the Board of Directors and Trustees.
    - Hearing any appeals against decisions made by the Managing Director regarding requests from individuals and organisations about data held by the Federation relating to them.
- The Managing Director is also the Data Protection Officer (and reports to the FAR Committee) and is responsible for:
    - Developing with the Finance, Audit and Risk Committee this policy and reviewing the data protection risks with the Board at every meeting (as part of its Risk Register).
    - Managing the implementation of this policy (via the Director of Operations).

  - Hearing any appeals against decisions made by the Director of Operations regarding requests from individuals and organisations about data held by the Federation relating to them.
  - Reviewing and approving/signing any contracts or agreements with third parties that involve the sharing of the Federation's data.
  - Dealing with any data use and data management queries from the media.
  - Reviewing the reason/s for, and rectifying, any issues that might lead to a data breach.
- The Director of Operations is responsible for the day to day implementation of this policy. Specifically this includes:
  - Reviewing annually all data use and data management procedures to ensure they meet the objectives of this policy and, at least, meet the Federation's legal responsibilities.
  - Arranging data protection training and advice for Federation staff and providing guidance documents to the users of the Federation's systems.
  - Handling data use and data management questions from staff and the users of the Federation's systems.
  - Dealing with requests from individuals to see the data the Federation holds about them.
- The ICT Manager is responsible for:
  - Ensuring all systems, services and equipment used for storing and processing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is up to date and functioning properly.
  - Evaluating any third party services the Federation is considering using to store or process data.
- The Sales Manager and the Customer Services Manager are responsible for:
  - Drafting any data use and data management statements attached to communications from the Federation (this includes emails and letters).
  - Working with all relevant staff to ensure that any public materials and marketing adhere to the Federation's Data Use and Data Management policy guidelines.
  - Data is used for Federation marketing purposes must first be checked against industry suppression files and the facility for system users to "unsubscribe" must be provided.
- Staff using, or advising on the use of, data are responsible for ensuring that:
  - The only people able to access data, covered by this policy, should be those who need it for their work.
  - No data should be shared outside the Federation without the permission of the individual or the organisation, unless they have consented that others can provide and/or use it on their behalf.
  - The Federation provides training to all employees so that they understand their responsibilities when handling data.
  - All employees keep all data secure and password guidelines (to contain at least 12 alphanumeric characters, contain both upper and lower case letters, contain at least one number (0-9) and at least one special character (!,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
  - Data is never to be disclosed to unauthorised people, inside or outside the Federation.
  - When working with data, all employees should ensure the screens of their computers and laptops are always locked when not attended.
  - Data should not be shared outside of the Federation and should never be sent by email without the permission of the Data Protection Officer.
  - Data must be encrypted before being transferred electronically. The Federation's ICT Manager can advise on how to do this internally or externally.
  - No data should be saved to the local disk drive on the computer or laptop of an employee. All data should be stored and accessed via the Federation's secure servers.

**Data storage**

If in doubt about data storage any questions should be addressed to the ICT Manager or in his/her absence to the Data Protection Officer.

When data is stored on paper, and being processed, it should not be left unattended on a printer or desk where it could be viewed by unauthorised people. When it is not being used, data should be held in a locked cabinet or secure facility and not be accessible to unauthorised people. All printed data that is no longer required must be shredded in the office or via a secure third party contractor.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. To meet these requirements:

- All our data is held in secure UK based servers.
- Data should be protected by strong passwords that are changed regularly and are not shared.
- No data should be stored on removable media, without the written permission of the Data Protection Officer, the Director of Operations or the ICT Manager.
- Data should only be stored on live or development systems and on designated drives and servers.
- Servers containing the data of the Federation are held at a secure location behind multiple firewalls and away from the office location (excepting the need to retain back up data at the office location).
- All servers and secure storage devices containing data should be protected by approved and tested software and firewalls.
- We will retain your data for a maximum of 7 years after the closure of your account or the provision of our final service. During this time the data might be archived from the live system.
- Data should be backed up daily. The ability to rebuild the system and reload data should be tested twice a year.
- No data should be saved onto laptops, tablets, mobile phones, CDs or memory sticks.

**Data accuracy**

For both our operations, and in order to meet the requirements of the GDPR and DPA, the Federation, its staff, the Certification Bodies and system users must take reasonable steps to ensure that data is accurate and up to date:

- Data will only be held in the systems the Federation operates in order to maintain data security.
- Data can only be accessed by those with relevant permissions and access will require a password.
- Both the staff of the Federation and all system users should take every opportunity to ensure that data is kept up to date.
- Data entered onto ACE via the ADTF (Automated Data Transfer Facility) needs to be verified.
- System users of HR Flow and the Assessors Guild will be reminded to review and update core data each time they access the system.
- All data that is no longer valid will be removed. For example, if a telephone number can no longer be accessed then it should be removed from a record.

**Data requests by individuals or organisations**

All individuals or organisations are entitled to ask about data held about them by the Federation. They can:

- Ask what information the Federation holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed on how the Federation is meeting its data protection obligations.

Such a request for information is called a "subject access request". All such requests must be forwarded to the Director of Operations and their receipt logged.

Applications for subject access data can be made by email to info@fisss.org or by post. The title of the email should state that it is a "subject access request". The Federation will aim to provide the relevant data within 10 working days.

The Federation will always verify the identity of a person making a subject access request before providing any information.

In certain circumstances the GDPR and the DPA allows data to be disclosed to law enforcement agencies (and in the cases of ACE/ACW/MAO to the relevant funding bodies) without the consent of the data subject. The Federation will only disclose data if the request is found to be legitimate and will seek advice from the Board and/or from the charity's legal advisers, where necessary.

**Privacy Policy**

When you use the Federation's services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it and what we do with it. This is important; we hope you will take time to read it carefully.

As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy. Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

If you have any questions contact info@fisss.org.

**Information that we collect**

We collect information to provide better services to all of our users.
We collect information in the following ways:

- **Information you give us.** Some of our services require you to sign up for a service and a licence (HR Flow and the Assessors Guild) to use that service. When you do, we'll ask for personal and contact information, like your name and contact details (address, email address, mobile and telephone numbers) and other details to store with your account. When you make a payment we will not collect or keep your payment details. These will be managed by an FCA regulated organisation, on our behalf. For the Assessors Guild you can take full advantage of the sharing features we offer by creating a publicly visible Assessors profile, which may include your name and photo, skills, competencies, areas of specialism, geographical availability and contact details. What you choose to include is up to you.
- **Information you give others.** Some of our services mean that you will authorise a third party (normally a training provider) to provide information into our systems. To do this you need to have signed a consent form (on paper or electronically) and that will enable them to provide information for ACE, ACW, and ACE360, on your behalf
- **Information we collect from your usage.** As you use our services there will be a number of other ways we collect information that tell us about how you use our services. These will only be used to improve the service that you use. These include:
    - **Log information**
      When you use our services or view content provided by the Federation, we automatically collect and store certain information in server logs. This includes:
        - Details of how you used our service, such as your data input history and search queries.
        - Telephony and email log information, such as your phone number, email address, time and date of calls/emails, duration of calls and nature of the enquiry.
        - IP address.
        - Device event information, such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
        - Cookies that may uniquely identify your browser or your user account.
    - **Unique learner, user or member number**
      Certain services include a unique reference number. This number and information about your usage/account means we can keep a record of your usage history and will enable us to improve our services to you.

- **Cookies and similar technologies**
  We use various technologies to collect and store information when you visit our services, and this may include using cookies or similar technologies to identify your browser or device.

When information is associated with your account, we treat it as personal information and it is covered by the GDPR and the DPA. More information about how you can access, manage or delete information that is associated with your account has been provided previously in the Federation's Data Use & Data Management Policy.

**How we use information that we collect**
We use the information we collect from all of the services we provide to maintain, protect and improve them and to inform the development of new ones.

The specifics of why we collect data and how we process data is set out below.

| Service | Legal basis for collecting data | Reason for collecting data | Data processing activity |
|---|---|---|---|
| ACE | 6(1)(a) – Consent of the data subject<br>6(1)(c) – Processing is necessary for compliance with a legal obligation<br>6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller | To verify Apprenticeship regulations in England are adhered to and relevant qualifications are achieved to issue an Apprenticeship completion certificate. | Collection and verification of both electronic and paper qualification data against Apprenticeship Framework qualification requirements.<br>Collection and verification of Apprentice consent form.<br>Review of Apprentice/Employer/Training Provider data against approved Government regulations and Registers.<br>Research into Apprenticeship certificate completion patterns and trends. |
| ACW | 6(1)(a) – Consent of the data subject<br>6(1)(c) – Processing is necessary for compliance with a legal obligation<br>6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller | To verify Apprenticeship regulations in Wales are adhered to and relevant qualifications are achieved to issue an Apprenticeship completion certificate. | Collection and verification of both electronic and paper qualification data against Apprenticeship Framework qualification requirements.<br>Review of Apprentice/Employer/Training Provider data against approved Government regulations and Registers.<br>Research into Apprenticeship certificate completion patterns and trends. |

| Service | Legal basis for collecting data | Reason for collecting data | Data processing activity |
|---|---|---|---|
| MAO | 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract | To verify Modern Apprenticeship regulations in Scotland are adhered to and relevant qualifications are achieved to issue a Modern Apprenticeship completion certificate. | Collection and verification of both electronic and paper qualification data against Modern Apprenticeship Framework qualification requirements.<br>Review of Apprentice/Employer/Training Provider data against approved Government regulations and Registers.<br>Research into Apprenticeship certificate completion patterns and trends. |
| ACE360 | 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract | To provide the organisations involved in managing the delivery and assessment of English Apprenticeship standards with a secure data warehouse | Electronic and manual data entry for verification against pre-set English Apprenticeship standard and End-Point Assessment Organisation pre-set criteria.<br>Sampling and statistical analysis of data by External Quality Assurance Organisations to deliver their contractual requirements (as defined by the Institute for Apprenticeships)<br>Research into Apprenticeship training and assessment patterns and trends. |
| AG | 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract | To support the purpose and objects of the Assessors Guild for both individual and Corporate Members and enable the delivery of Membership services | Collect and validate individual and corporate member records<br>Present individual member profiles to gain new assignments and job roles<br>Present freelance and job opportunities to individual members<br>Present CPD activities to members |
| HR Flow | 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract | To support the purpose and objects of HR Flow Ltd. By enabling the delivery of an Employee record system | Collect and provide statistical analysis of employee records in individual businesses<br>Benchmark individual businesses against other groups of businesses |

When you contact the Federation, we keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies to improve the quality of our services.

**Transparency and choice**

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can review and control the information in your account and either change it or let us know it is incorrect so we can change it.

You may also set your browser to block all cookies, including cookies associated with our services or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not work properly if your cookies are disabled.

**Accessing and updating your personal information**

Whenever you use our services, we aim to provide you with an opportunity to update your information. If information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your information, we may ask you to verify your identity before we can act on your request.

Where we can provide information access and correction, we will do so free of charge, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems. For ACE and ACW we are required to retain records for 7 years before deleting them.

**Information that we share**

We do not share personal information with companies, organisations and individuals outside of the Federation, unless one of the following circumstances applies:

- **With your consent**

We will share information with organisations or individuals outside the Federation when we have your consent to do so. We require "opt-in consent" for the sharing of any information.

- **For research**

We provide information to some research organisations who use it to research it to develop the skills policies of the four UK nations. You can ask for your data not to be shared. Any data that is shared will only be shared with trusted organisations who fulfil our data security, confidentiality and security requirements.

- **For legal reasons**

We will share personal information with the Governments of the UK and agencies thereof and organisations or individuals outside the Federation if we have a belief in good faith that access, use, preservation or disclosure of the information is reasonably necessary to:

  - meet any applicable law, regulation and legal process or Governmental request.
  - enforce applicable Terms of Service, including investigation of potential violations.
  - detect, prevent or otherwise address fraud, security or technical issues.
  - protect against harm to the rights, property or safety of the Federation, our users or the public, as required or permitted by law.

We may share anonymised information publicly and with our partners, like the Government, to ensure the development of skills policies, for the benefit of the nation concerned.

**Information security**

We work hard to protect the Federation and our users from unauthorised access to or unauthorised alteration, disclosure or destruction of information that we hold. In particular:

- We encrypt many of our services using SSL (Secure Sockets Layer). It is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
- We may offer you 2 step verification when you access your account.
- We regularly review our information collection, storage and processing practices, including physical security measures, to guard against unauthorised access to systems. This is carried out at least annually.
- We restrict access to personal information to the Federation's employees and to those you have given consent to view the information, who need to know that information in order to process it for us and they are subject to strict contractual confidentiality obligations. They may be disciplined, or their contract terminated, if they fail to meet these obligations.

**When this Privacy Policy applies**

Our Privacy Policy applies to all of the services offered by the Federation.

**Compliance and cooperation with regulatory authorities**

We regularly review our compliance with our Privacy Policy. We also ensure that we meet the GDPR and DPA. When we receive formal, written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot directly resolve with our users.

**Changes**

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes). We will also keep prior versions of this Privacy Policy in an archive for your reference.

**We keep your personal information private and safe — and put you in control.**