DATA PROTECTION CONTRACT

Introduction

Under the General Data Protection Regulation (GDPR) both First Aid Awards (FAA) and approved centres have a responsibility to ensure compliancy in respect of the learner data that is collected and processed during the administration, delivery and award of FAA qualifications.

This contract states how FAA (Data Controller) requires approved centres (Data Processor) to collect, store and process learner data.
The contract details the Data Processor's responsibilities to both FAA and data subjects and states procedures that must be followed in the collection, storage and processing of an individual's personal and special category data.

The contract has been split into sections to allow easy access to important information and procedures:

Section 1 – Roles and definitions under the GDPR
Section 2 – Responsibilities of centre (Data Processor)
Section 3 – Collecting learner's data
Section 4 – Processing learner's data
Section 5 – Storing learner's data
Section 6 – Securely transferring data
Section 7 – Retention periods for learner's data
Section 8 – Securely disposing of data
Section 9 – Data breaches and notification
Section 10 – Rights of FAA (Data Controller)
Section 11 – Centre's declaration

Section 1 – Roles and definitions under the GDPR

What data is covered under this contract?

All learner data collected through the completion of official FAA course paperwork/documentation is included within this contract and includes the following processes:

- The collection of learner's personal data through any official FAA documentation and includes name, email address and date of birth. Gender and a postcode is only collected if a learner requests entry of their achievement onto their personal learning record
- The collection of learner's special category data when a reasonable adjustment is granted. This is only collected and stored when a reasonable adjustment is granted and only includes any disability, medical condition or learning need
- The storage of FAA course paperwork/documentation
- Upload and maintenance of electronic records of a learner's achievement on FAAPlus
- The transfer of FAA course paperwork/documentation

What data is not covered under this contract?

The requirements stated within this contract are purely in relation to the administration and certification of FAA qualifications and data that is collected during qualification delivery and on official FAA course paperwork/documentation.

Under the GDPR approved centres must also consider their own:

- Employee data
- Customer & supplier data
- Learner data for any non-FAA qualifications/courses
- Direct marketing using learner's data
- Business activities that they may conduct
- Additional learner data collected in relation to FAA qualifications, not required by FAA, such as during course enquiries and course booking procedures

This list is not exhaustive, and centres must conduct their own internal audit of the data they collect and process to ensure compliance with the GDPR. Full guidance on how centres can ensure compliancy with the GDPR can be found on the Information Commissioner's Office website – www.ico.org.uk

FAA and approved centre roles

There are two roles that are defined within the GDPR:

- Data Controller
  Determines the purpose for, and the way in which data is collected, stored and processed.

- Data Processor
  Any person who processes the data on behalf of the Data Controller.

For the purposes of the administration and award of learner's achievements, FAA are the Data Controller and FAA centres are Data Processors.

Personal data and special category data

The GDPR state that there are two types of data that FAA and approved centres collect, store and process:

- Personal data
  Includes name, email address and date of birth; gender and postcode may be collected if required for entry onto a learner's personal learning record.

- Special category data
  Special category data is only collected when the learner is applying for a reasonable adjustment and is data relating to the learner's health including any disabilities, medical conditions or learning needs they may have.

Please note that within this contract the word 'data' refers to both personal data and special category data.

Section 2 - Responsibilities of centre (Data Processor)

Acting as a data processor on behalf of FAA

FAA centres must collect, store, process and transfer learner data that is collected on official FAA course paperwork/documentation, as set out within this contract.

The responsibilities of the centre are as follows:

- Ensure all required centre staff are aware of this contract, the centre's responsibility under this contract and the procedures stated within this contract
- Collect, store, transfer, retain and dispose of learner's data as stated within this contract
- Inform FAA of any data breach immediately, no later than 24 hours after discovery
- Ensure decision makers and key personnel are aware of GDPR and their responsibilities
- Provide data protection awareness training
- Integrate data protection into processing activities
- Have and publish a data protection policy
- Document data that is held and how it is processed and moved

Compliance with GDPR for non-FAA activity

Centres must also consider their own business activities for data that is collected by the centre in any other way than through official FAA course paperwork/documentation.

For example, centres must be compliant with the GDPR in their own right should they:

- Collect any learner data in any other way than through official FAA course paperwork/documentation
- Collect learner data during course enquiry/booking procedures
- Process learner's data for any other purpose than the administration of their achievements with FAA
- Market themselves using learner's data
- Be registered with any other awarding organisation
- Collect, store, process or transfer data as part of any other business activity apart from the delivery of FAA qualifications

Section 3 - Collecting learner's data

How do we collect a learner's data?

A learner's data must only be collected on official FAA course paperwork/documentation. FAA course paperwork/documentation has been designed to only request the minimum required data to allow FAA and centres to administrate and award a learner's achievement.

Special category data must only be recorded during the application for a reasonable adjustment and is required for no other purpose.

Can we collect any additional data?

Centres are not permitted to collect any additional data outside of what is required on the official FAA course paperwork/documentation.

Should a centre require additional data for any other purpose, the centre must conduct their own GDPR audit and ensure compliance before doing so.

Section 4 - Processing learner's data

Centres are required to process learner data as part of the administration of the qualification that the learner has chosen to undertake.

Centres are only permitted to process learner data for the purpose of entering it onto FAAPlus for certification and record keeping purposes.

Centres are permitted to electronically store a record of learner's achievements on their own database but only data that is collected from official FAA course paperwork/documentation and only for the purpose of record keeping.

No additional processing of learner data is permitted unless covered by the centre's own GDPR audit.

Section 5 - Storing learner's data

What data do I need to keep?

All data is generated through the completion of official FAA course paperwork/documentation. Full course paperwork packs must be retained for a minimum of three years and six months to provide evidence of a learner's achievement.

How do I securely hold course paperwork/documentation?

Course paperwork/documentation can be stored in either hard copy 'paper' format or in an electronic document such as Word or PDF.

Hard copy 'paper' format

When data is stored in hard copy format the centre must ensure that this is kept securely and take appropriate action to prevent unauthorised access.

Centres must ensure that paperwork/documentation is:

- Securely transported from the course venue to the centre's premises by an authorised person, such as trainer/assessor, or through a secure carrier, such as Royal Mail special delivery service
- Not left unattended
- Securely protected
- Promptly transferred to a secure storage area with access only by authorised persons
- Securely disposed of, as stated below, should it be electronically scanned

Electronic format

When data is stored in electronic format appropriate security measures must be taken to protect learner's data.

Centres must ensure that electronic records and documents are stored on a computer/server/cloud system that is protected by suitable security software and that physical computers are in secure locations with access only available to authorised persons.

It is crucial that the security software is maintained and that important security updates are quickly installed.

Appropriate measures must be in place to cover staff working from home or accessing systems, containing learner data, from remote locations.

All systems must be protected and only accessed through a secure log in system with users having unique user name and passwords.

Loss of data

Centres must take all possible actions to prevent the accidental or deliberate loss of data.

Course paperwork/documentation in electronic format must be appropriately backed up either internally or remotely through the internet.

Course paperwork/documentation in hard copy format must be securely stored and a back up copy generated if being sent through a secure courier.

Section 6 - Securely transferring data?

Course paperwork/documentation may need to be transferred in either hard copy or electronic format. Audit requests from FAA may require the centre to transfer copies of paperwork/documentation which can be done electronically or in hard copy.

Hard copy 'paper' format

Centres must ensure that hard copies of data are secure when being transferred and that measures are taken to prevent loss of data. Secure mail services such as Royal Mail's special delivery service should be used. Centres must ensure a backup copy of any paperwork/documentation is taken before the hard copies are sent to prevent data being lost in transit.

Electronic format

When transferring course paperwork/documentation and data through electronic formats, centres have the following options available:

- Transfer through FAAPlus

FAAPlus is located on a secure server with security being maintained by an international provider. Centres can securely upload documents directly to FAA through the upload facility located within FAAPlus. Access to FAAPlus is gained through a secure log in.

- Transfer through email

Paperwork/documentation and other documents must not be sent via email without being encrypted. 'Zipped' folders and documents must be encrypted, and a suitable alphanumeric password created, before being sent and this can be achieved using software such as 'WinZip'. The password must be sent via a different medium than the documents, such as telephone.

- Transfer through a file hosting service, for example 'Drop Box'

Paperwork/documentation and other documents can be shared using file hosting services such as Drop Box, Microsoft 365, etc. The centre can create an account with the file hosting service and upload documents to the service which can then be shared with FAA.

When using such services, the centre must add a password and expiry time to documents and communicate the link and password in separate mediums, for example the link can be emailed, and the password communicated by telephone.

Section 7 - Retention periods for learner's data

Course paperwork/documentation including assessment papers, must be kept by the centre to allow any learner complaints/appeals/confirmation of achievement requests to be dealt with.

FAA requires centres to retain course paperwork and learner evidence for 3 years and 6 months from the end date of the course.

Centres must securely dispose of course paperwork/documentation, as per section 8 of this document, once this date has been reached unless the course paperwork is required by the centre for any other purpose, such as meeting regulatory requirements set by the Skills Funding Agency.

Centres are able to hold the paperwork for longer than 3 years and 6 months in such situations but centres must consider this data within their own GDPR arrangements after this date has been reached.

Section 8- Securely disposing of data

Data, whether in paper or electronic format, must be disposed of in an appropriate manner.

Paper based data

All paperwork/documentation that contains learner data must be disposed of in a secure way. Paperwork/documentation must be either:

- Shredded onsite by a nominated person and the waste securely disposed of

  OR
- Collected and disposed of by a specialist business providing the centre with a certificate of destruction

Electronically based data

Electronic based records within a database, or any IT document such as Word or PDF, must be deleted in full and removed from all systems in their entirety including any 'recycle bins' that the data may be unknowingly backed up into.

Centres must ensure all archived or backed up versions are also deleted in their entirety. There must be no way that the data is able to be retrieved.

Section 9 - Data breaches and notification

Under the GDPR FAA, as Data Controller, has a legal duty to notify the ICO should a data breach occur.

What is a data breach?

A data breach is described in the GDPR as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The following example situations would be considered a data breach:

- Access to personal data by an unauthorised person or organisation
- Deliberate or accidental deletion of data
- Sending data to the wrong person
- Computers, phones or any electronic equipment on which data is stored, being lost or stolen
- Paper files, on which data is written, being lost or stolen
- Changing a person's data without their permission
- Loss of availability of data

What action do I need to take if a data breach occurs?

All data breaches, no matter how large or small, must be reported to FAA without delay and no later than 24 hours after discovery. FAA has a legal duty to notify the ICO of any data breach within 72 hours of the incident occurring so centres must not delay in notifying FAA of any incidents.

Data breaches must be notified to FAA in the form of an email sent to jason@firstaidawards.com.

The notification should include, where known, the following information:

- A detailed description of the data breach, including cause of the breach
- An approximate number of the individuals and data records affected
- A contact within the centre to liaise with regarding the breach
- A description of the measures taken, or proposed to be taken, to deal with the data breach

FAA is aware that it may not be possible to provide all information at the time of notification. Centres must not delay the notification of a breach and any missing information can be forwarded in subsequent communications.

Section 10 – Rights of FAA (Data Controller)

FAA, in its role as Data Controller, has overall responsibility for the security, collection and processing of learner data. To allow FAA to fulfil this role, centres must provide FAA with access and information when requested, concerning all aspects of the collection, storage, processing and deletion of learner data.

Section 11 - Centre declaration

I can confirm that I am authorised, on behalf of the FAA approved centre, to sign this contract and can confirm that the approved centre will:

- Ensure all appropriate centre staff will be aware of this contract and the procedures and responsibilities stated within
- Only act on the written instructions FAA has stated within this contract
- Ensure that all persons processing the data are subject to a duty of confidence
- Take appropriate measures to ensure the security of data during processing
- Only engage sub-processors with the prior consent of FAA and under a written contract agreed with FAA
- Assist FAA in providing subject access and allowing data subjects to exercise their rights under the GDPR
- Assist FAA in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- Delete or return all personal data, and special category data, to FAA upon termination of approved centre status
- Submit to audits and inspections, provide FAA with whatever information it needs to ensure that we are both meeting our Article 28 obligations, and tell FAA immediately if asked to do something infringing the GDPR or other data protection law of the EU or a member state
- Publish a data protection policy
- Undertake a full review of all non-FAA activities to ensure centre compliance with the GDPR

Name _____

Position within centre _____

Centre name _____

Date _____