

Decisive First Aid

Data Protection Policy

Data Protection Policy

1. Overview

1.1 The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the customer within the scope of [commissioned processing](#). This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) but also to provide proof of compliance.

1.2 The General Data Protection Regulation (GDPR) is a regulation, which requires any business that processes data belonging to UK & EU citizens to protect it and not misuse it. As a responsible business, [Decisive First Aid](#) aims to robustly implement the requirements of the GDPR. Part of meeting the obligations of GDPR is the production and implementation of this policy.

1.3 [Decisive First Aid](#) is committed to the rules of data protection and abiding by eight data protection principles. These are the principles that must be satisfied when obtaining, handling, processing, moving and the storage of personal data.

1.4 As an ITC First approved training centre, [Decisive First Aid](#) must collect and process information as required by ITC First awarding body and its regulators. [Decisive First Aid](#) is therefore considered the Data Processor and its course candidates and employees the Data Subjects.

2. The 8 Data Protection Principles

- a) Data must be obtained and processed fairly and lawfully.
- b) Data must be obtained for a specified and lawful purpose.
- c) Data must be adequate, relevant and not excessive for its collection purpose.
- d) Data must be accurate and kept up to date.
- e) Data must not be kept for longer than is necessary for its purpose.
- f) Data must be processed in accordance with the Data Subject's rights.
- g) Data must be kept safe from unauthorised access, accidental loss or destruction.
- h) Data must not be transferred to a country outside the European Economic Area.

3. Data Subjects Rights

3.1 Under the GDPR individuals have rights associated with their data, described below:

- a) The right to be informed
- b) The right of access
- c) The right to rectification
- d) The right to erasure
- e) The right to restrict processing
- f) The right to data portability
- g) The right to object
- h) Rights in relation to automated decision making and profiling

3.2 Children's Personal Data

For the benefit of this policy a child is classed as a young person under the age of 16. Children must have parental (or an individual in loco-parentis) consent for ITC First to collect and process their data. ITC will maintain evidence of consent using our learner registration process.

4. Data Collection

4.1 [Decisive First Aid](#) acts on behalf of ITC First, by gathering and submitting learner data securely via the ITC website and/or registered post. [Decisive First Aid](#) have a legally binding Centre Agreement, which confirms that [Decisive First Aid](#) publishes and implement a Data Protection Policy (this document).

4.2 **Decisive First Aid** collects data as part of the booking and registration process required for qualification delivery. **Decisive First Aid** collects and retains data as part of its **Decisive First Aid** administrative tasks.

4.3 When individuals provide their data to **Decisive First Aid**, the data is submitted to ITC First and is used to:

- a) Attribute qualification credit to learners
- b) Produce commemorative certificates
- c) Produce CPD certificates
- d) Receive information pertinent to qualifications
- e) Enable ITC to contact you at your request (depending on when your data is provided and in which specific context or interaction with ITC First)
- f) Monitor ITC First qualifications to ensure equality and inclusivity

4.4 Learners data will only be used for the legitimate purposes described above. Any changes to the ways in which learner data is used will be communicated to those individuals affected.

5. Data Storage

Decisive First Aid will ensure that:

- a) Data is held securely such as password protected computer, locked cabinets/drawers, encrypted, computers have appropriate virus/data protection software appropriate to the business.
- b) Course registrations (which includes, name, address, contact details, ethnicity, signature) are removed from sight and access of other course candidates immediately after completion.
- c) Data is not disclosed or shared verbally or in writing to any unauthorised party.
- d) **Decisive First Aid** will download course candidate data to their part of the ITC website and promptly submit all documentation to ITC First. Data submitted will only be viewable via individual unique User log on and password of **Decisive First Aid** and ITC First.
- e) **Decisive First Aid** will not share their log on and passwords with any unauthorised individuals or companies.

6. Data Retention

- a) **Decisive First Aid** will retain any data in accordance with ITC retention periods, currently 5 years.
- b) **Decisive First Aid** will review its necessity to retain data once it has been submitted and accepted by ITC First.

7. Data Destruction

- a) **Decisive First Aid** will ensure it destroys data in a confidential manner i.e. shredding of paper documents, deletion/pseudonymisation of digital records from computer systems.
- b) **Decisive First Aid** will ensure it does not retain data longer than is required for the purpose of the qualification.

8. Subject Access

8.1 Any party who has provided personal data to **Decisive First Aid**, has the right to request what information is stored and its content.

8.2 Access request may be made in writing by letter or email to the **Decisive First Aid Director** who will discuss the request with the data subject.

8.3 Data will be provided in accordance with the subject's Rights of Access under the GDPR.

9. Breaches of Data Protection

- a) Breaches or suspected breaches should be reported to [Andrew Barras](#) who will make the necessary investigations and provide a response to the informant within 3 weeks of receipt.
- b) Breaches may also be raised with ITC First by contacting their office either via email, telephone or in writing.