

# Quality and Qualifications Ireland Data Protection Policy

## Document Version Information

Name	QQI Data Protection Policy
Version	1.0
Approved by	EMT
Approval date	11 May 2023
Effective date	1 June 23
Review date	By 1 June 26

## Table of Contents

1. Purpose .....	4
2. Scope.....	4
3. Definitions.....	4
4. Principles.....	5
4.1. Lawfulness, fairness and transparency .....	6
4.2. Purpose Limitation .....	6
4.3. Data Minimisation.....	6
4.4. Accuracy.....	6
4.5. Storage Limitation.....	7
4.6. Integrity and Confidentiality .....	7
4.7. Accountability .....	7
5. Data subject rights .....	7
5.1. Right to access .....	8
5.2. Right to rectification .....	8
5.3. Right to erasure.....	8
5.4. Right to restriction of processing.....	9
5.5. Right to data portability.....	9
5.6. Right to object.....	10
5.7. Right to withdraw consent.....	10
5.8. Right to object to automated decision making.....	10
5.9. Right to complain .....	10
6. Responsibilities of QQI.....	11
6.1. Ensuring appropriate technical and organisational measures .....	11
6.2. Maintain a record of processing activities.....	11
6.3. Implementing appropriate agreements with third parties.....	11
6.4. Transfer of personal data outside of the European Economic Area.....	12
6.5. Data Protection by Design and Default.....	12
6.6. Data Protection Impact Assessment.....	12
6.7. Personal Data Breaches .....	12
6.8. Recording compliance activities .....	13
7. Responsibilities of staff and similar parties .....	13

7.1. Training .....	13
7.2. Failing to comply with this policy.....	14
8. Responsibilities of the Data Protection Officer.....	15
9. Governance .....	15
10. Retention Periods .....	16

## 1. Purpose

Quality and Qualifications (“QQI”) is committed to protecting the rights and privacy of individuals in accordance with both the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (“the Act”). QQI shall lawfully and fairly process personal data about learners, employees, suppliers, stakeholders and any other individuals to achieve its mission and functions.

Data protection laws confer rights on data subjects as well as responsibilities on the parties processing personal data. This policy details QQI’s responsibility to protect personal data and ensure its confidentiality, insight and availability. To ensure compliance, QQI is required to put in place appropriate organisational and technical measures to prevent unauthorised internal and external access to personal data.

## 2. Scope

This policy applies to all of QQI’s personal data processing functions in relation to identified or identifiable natural persons, including those performed on learners, employees, suppliers and any other personal data QQI’s process from any source. (Source underlined)

For the purposes of this policy “employees” stand for all persons employed by QQI on a full or part-time basis, persons who QQI contract for services on a seasonal or ongoing basis, trainees with QQI, interns with QQI or agency employees.

## 3. Definitions

Term	Definition
<b>GDPR</b>	The General Data Protection Regulation (EU) 2016/679
<b>Personal Data</b>	Any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
<b>Special Category Personal Data</b>	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
<b>Processing</b>	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

<b>Controller</b>	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
<b>Processor</b>	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
<b>Third Party</b>	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
<b>Personal Data Breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
<b>Data protection laws</b>	The group of laws that govern how organisations can process personal information. These include the General Data Protection Regulation, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2011 (“ePrivacy Directive”)
<b>Data Protection Officer</b>	An appointed individual with oversight of data protection compliance of the organisation.

#### 4. Principles

There are a number of important principles relating to personal data to which QQI adheres. These are:

1. Personal data should be processed lawfully, fairly and in a transparent manner (“**lawfulness, fairness and transparency**”);
2. Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“**purpose limitation**”);
3. Personal data should be adequate, relevant and limited to what is necessary (“**data minimisation**”);
4. Personal data should be accurate and, where necessary, kept up-to-date (“**accuracy**”);
5. Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary (“**storage limitation**”);
6. Appropriate technical and organisational security measures should be applied to personal data to protect against unauthorised or unlawful access and accidental loss, destruction or damage (“**integrity and confidentiality**”);
7. QQI should be accountable for, and able to demonstrate, its compliance with applicable data protection laws (“**accountability**”).

A description of how each of these data protection principles is implemented in practice is set out below.

#### 4.1. Lawfulness, fairness and transparency

##### **Personal data must be processed lawfully, fairly and in a transparent manner**

**Lawfully:** The legal basis for processing personal data is broadly based on Article 6.1(c) or 6.1(e) of the GDPR i.e. 'necessary for compliance with a legal obligation' or 'necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller'. QQI may also process personal data in accordance with certain contracts it has put in place and, in limited circumstances, where it has a legitimate interest in processing personal data. In very limited circumstances, QQI may request the consent of the data subject to process their data. In such cases, consent will be sought at the time that the data is collected, and the data subject will be advised that they can withdraw their consent at any stage during processing.

**Fairly:** For processing to be fair, QQI has to make certain information available to data subjects. This applies whether the personal data was obtained directly from the data subject or from other sources.

**Transparently:** QQI provides the required information to data subjects at the time personal data is collected. QQI ensures that the information provided is detailed and specific, and that such notices are understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. In order to balance the requirements above, QQI may implement appropriate policies to make information available on its websites, forms or booklets. The information provided must include information about personal data collected both directly from the data subject and from other sources.

#### 4.2. Purpose Limitation

##### **Personal data can only be collected for specific, explicit and legitimate purposes**

QQI collects and processes personal data only for the purposes for which it is collected. QQI employees must be alert to requests for processing of personal data for purposes for which it was not collected; no matter how related the processing may appear. Processing should only continue after an assessment of the impact of the new processing has taken place.

#### 4.3. Data Minimisation

##### **Personal data must be adequate, relevant and limited to what is necessary for processing**

QQI ensures that in designing methods of data collection, whether online, forms or at its offices, that only the personal data required to identify the data subject(s) and provide the product or service requested is processed.

#### 4.4. Accuracy

##### **Personal data must be accurate and kept up to date with every effort made to erase or rectify without delay**

All data subjects have a right to ensure that their data is accurate and complete. The means that QQI shall have in place a procedure for identifying and addressing out-of-date, incorrect and redundant personal data when they become aware of it. All data collection procedures should be designed to ensure that reasonable steps are taken to update personal data where new data has

been provided. All changes to personal data should be shared with each third party with whom the previous data had been shared, unless this is impossible or requires disproportionate effort.

#### 4.5. Storage Limitation

**Personal data must be kept in a form such that the data subject can be identified for only as long as is necessary for processing**

Personal data shall be kept for no longer than is necessary for the purposes for which the personal data is collected and shall be kept in line with the QQI retention policy. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes.

QQI implements appropriate policies and procedures to ensure that personal data is retained only for the minimum period required to provide the services requested. This may be done by destroying the personal data, by anonymisation or any other appropriate method.

#### 4.6. Integrity and Confidentiality

**Personal data must be processed in a manner to ensure appropriate security**

QQI implements appropriate technical and organisational measures to ensure that appropriate security of the processing of personal data is applied.

#### 4.7. Accountability

**The Controller shall ensure that it can demonstrate compliance with the principles**

QQI ensures that it maintains adequate records of its processing activities and evidence that it has complied with this policy and related policies and procedures. Responsibility for collecting and maintaining the evidence is with the Data Protection Officer.

### 5. Data subject rights

Data subjects have a number of rights under the GDPR. These rights can be applied by making the appropriate request to QQI by contacting the Data Protection Officer at [dpo@qqi.ie](mailto:dpo@qqi.ie). In processing a data subject request, QQI will:

- Check whether the organisation holds personal data on the data subject;
- Check the validity of the request by confirming the identity of the person making the access request;
- Decide if the request is excessive or manifestly unfounded and if the request will be refused;
- Determine if a charge may be applied if the request is deemed to be unjustified or excessive;
- Determine if additional information or clarification is required from the data subject in order to process the request;
- Determine if the request can be answered within 30 days or if an extension is required;
- Determine if the request complies with the specific requirements of the GDPR; and
- Determine if any exemptions are to be applied to the request.

Where QQI is legally permitted to do so, QQI may decline a data subject's request. Such a refusal will be explained to the data subject in writing. Please note that data subject rights are not absolute. Exceptions or limitations relating to certain of the rights conferred by the GDPR are noted below in the relevant section.

QQI designs and maintains appropriate policies, procedures and training to implement the following data rights of data subjects.

### 5.1. Right to access

Data subjects have the right to access their personal data. They are entitled to receive a copy of their data held by QQI and other information about the processing, sharing and retention of their personal data. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

QQI implements procedures to ensure that requests from data subjects for access to their personal data are identified and fulfilled in accordance with the legislation within the 30 days permitted. **For a copy of the Subject Access Policy, please contact the Data Protection Officer.**

### 5.2. Right to rectification

Data subjects have a right to have their personal data rectified where it is inaccurate or incomplete.

QQI is committed to holding accurate data about data subjects and implements processes and procedures to ensure that data subjects can rectify their data where inaccuracies have been identified.

### 5.3. Right to erasure

Data subjects have a right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'.

Where QQI receives requests from data subjects looking to exercise their right of erasure then QQI will carry out an assessment of whether the data can be erased. Data subjects have a right to erasure of their personal data where one of the following grounds apply:

The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed:

- The data subject withdraws consent and there is no other legal basis for the processing;
- The data subject objects to the processing pursuant to article 21(1);
- The personal data have been unlawfully processed;
- The personal data have to be erased for compliance with a legal obligation; or
- The personal data have been collected in relation to the offer of information society services of a child; article 18(1).

A request for erasure of personal data can be refused where processing is necessary:

- For exercising the right to freedom of expression and information;



- For compliance with legal obligation or for the performance of a public interest task or exercise of official authority;
- For public health reasons;
- For archiving interests in the public interest, scientific, historical research or statistical purposes; or
- For the exercise or defence of legal claims.

#### 5.4. Right to restriction of processing

Data subjects have a right to block or suppress processing of their personal data in defined circumstances. Data subjects have a right to restrict the processing of their personal data where one of the following grounds apply;

- Where the data subject contests the accuracy of their personal data (processing should be restricted for a period enabling QQI to verify the data's accuracy);
- Where the processing is unlawful, and the data subject opposes erasure and requests restriction instead;
- Where the controller no longer needs the personal data, but the data subject requires the personal data to exercise or defend a legal claim; or
- Where the data subject has objected to the processing; processing should be restricted pending verification of whether the legitimate interests of the controller override those of the data subject. Article 18(1).

When a data subject exercises their right to restrict processing, QQI will only continue to process the personal data if:

- The data subject consents;
- The processing is necessary for the exercise or defence of legal claims;
- The processing is necessary for the protection of the rights of other individuals or legal persons; or
- The processing is necessary for public interest reasons under EU/Member State law.

QQI implements and maintains appropriate procedures to assess whether a data subject's request to restrict the processing of their data can be fulfilled. Where the request for restriction of processing is carried out then QQI will contact the data subject to confirm the restriction has been implemented and when the restriction is lifted.

#### 5.5. Right to data portability

Data subjects have a right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability only applies if:

- The processing is based on the data subjects consent or for the performance of a contract; and
- The processing is carried out by automated means.

The right to data portability will not apply to processing necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in QQI. In addition, the right to data portability must not adversely affect the rights and freedoms of others.

## 5.6. Right to object

Data subjects have the right to object to the processing of their personal data on the following grounds:

- Direct marketing; where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to such processing; there are no grounds to refuse to comply with such a request. When a data subject objects to processing for direct marketing purposes, the personal data can no longer be processed for that purpose;
- Processing based on public interest or legitimate interest grounds, including profiling; or
- Processing for scientific, historical research or statistical purposes (unless the processing is necessary for the performance of a public interest).

Data subjects have a right to object to the processing of his or her personal data. The processing must have been undertaken on the basis of public interest or legitimate interest of QQI.

## 5.7. Right to withdraw consent

Data subjects have the right to withdraw their consent to the processing of their personal data at any time.

If the data subject wishes to exercise the right to withdraw their consent, they may at any time directly contact the Data Protection Officer.

## 5.8. Right to object to automated decision making

Data subjects have the right not to be subject to a decision based solely on automated processing or profiling, where such decisions would have a legal effect or significant impact on you.

Where a decision based solely on automated processing, including profiling, occurs on the basis that it is necessary for the performance of a contract or with the explicit consent of the data subject; the data subject will be given “at least the right” to express their point of view and to contest the decision. Article 22(3).

Automated decision making involving sensitive data is only allowed where the data subject has given their explicit consent, or it is necessary for the public interest. Article 22(4).

QQI will inform data subjects at the time the personal data is collected of the existence of automated decision making, including profiling.

QQI may not comply with the objection if the processing is necessary for the performance of a contract; the processing is authorised by EU or Member State law or the processing is based on a data subjects’ explicit consent.

Profiling per se which does not result in solely automated decisions is not prohibited.

## 5.9. Right to complain

QQI maintains a complaints process whereby data subjects are able to contact the Data Protection Officer. The Data Protection Officer will work with the data subject to bring the

complaint to a satisfactory conclusion for both parties. The data subject is informed of their right to bring their complaint to the Data Protection Commission and their contact details

## 6. Responsibilities of QQI

This Policy is maintained by QQI and is approved by the Data Protection Officer. It is reviewed at least annually by the Data Protection Officer to ensure alignment to suitable risk management requirements and its continued relevance to current and planned operations, legal developments and/or legislative obligations.

All QQI employees are expected to be familiar with this policy and to adhere to it as well as to its applicable principles and other related procedures, arising from such principles and obligations.

Further comments or questions on the content of this policy should be directed to the Data Protection Officer. Any material changes to this policy will require approval by the Board.

### 6.1. Ensuring appropriate technical and organisational measures

QQI implements appropriate technical and organisational measures to ensure and be able to demonstrate that personal data is adequately protected. Including, but not limited to:

- The ability to restore the availability and access to personal data in a timely manner in the event of an incident; and
- Regular testing, assessing and evaluating of the effectiveness of the organisational and technical measures in place.

### 6.2. Maintain a record of processing activities

QQI maintains a record of its data processing activities in the manner prescribed by Article 30 of the GDPR. The record of processing is reviewed on annual basis by the Data Protection Officer. Any significant changes to an existing process or where a new process is implemented must be brought to the attention of the Director / Head of Unit in order to update the record of processing.

### 6.3. Implementing appropriate agreements with third parties

QQI implements appropriate agreements, memoranda of understanding and contracts (collectively “agreements”) with all third parties with whom it shares personal data. All such agreements are implemented in writing prior to the commencement of the transfer of the data. The agreement specifies the purpose of the transfer, the requirement for adequate security, right to terminate processing, restricts further transfer to other parties, ensure that responses are given to requests for information and the right to audit.

For the purpose of this policy, the term “third parties” refer to any entity external to QQI, who processes personal data on behalf of QQI.

#### 6.4. Transfer of personal data outside of the European Economic Area

On occasion, QQI may transmit your personal data outside the European Economic Area. In such circumstances, we will ensure that the transfer complies with our data protection obligations and we will ensure that the transfer agreement is based on an approved transfer mechanism, such as the European Commission's standard contractual clauses or an adequacy decision.

#### 6.5. Data Protection by Design and Default

Data protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This helps to ensure better and more cost-effective protection for individual data privacy.

Data protection by default means that service settings are automatically data protection friendly. An example of this would be that new network folders would be accessible only to those that require access specific to their role.

QQI develops processes, prior to the time of determining the means of processing as well as when actually processing, to incorporate appropriate technical and organisational measures to implement the data protection principles and integrate necessary safeguards into the processing to meet GDPR requirements.

#### 6.6. Data Protection Impact Assessment

QQI implements procedures and documentation whereby all new types of processing, in particular using new technologies, that could result in a high risk to the rights and freedoms of its data subjects must carry out a data protection impact assessment ("DPIA"). As part of this process, a copy of the impact assessment must be shared with QQI's Data Protection Officer, who will review the DPIA and provide advice where required.

Where QQI is unable to identify measures that mitigate the high risks identified then QQI will consult with the Data Protection Commission prior to the commencement of processing.

#### 6.7. Personal Data Breaches

QQI defines a "personal data breach" as meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (e.g. the most common breach incidents that can occur are correspondence issuing to an unauthorised third party). QQI deems any loss of personal data in paper or digital format to be a personal data breach.

In the event of a suspected data breach, QQI employees must notify their Director / Head of Unit immediately. The Director / Head of Unit must then immediately report the incident to the DPO. The decision to determine whether or not to report a data breach rests with the CEO after being consulted by the DPO and relevant Head of Unit.

The Data Protection Officer will also assess if the breach is likely to result in a high risk to the data subject(s) involved. Where a high risk is identified, the Data Protection Officer will arrange for the data subjects to be notified.

QQI has put in place organisational and technical measures to prevent personal data breaches; these measures include checking procedures, security and employees training and awareness. For a copy of the Data Breach Policy, please contact the Data Protection Officer.

#### 6.8. Recording compliance activities

QQI retains logs of relevant data protection related events;

- Invocation of data subject rights;
- Breaches; and
- DPIAs assessed and completed.

#### 7. Responsibilities of staff and similar parties

All employees and any related parties, who process personal data on behalf of QQI, share the responsibility for adhering, implementing and complying with this data protection policy. All records created during duties carried out on QQI's behalf are the property of QQI and subject to its overall control.

Anyone who processes QQI's data is required to:

- Read, understand and accept any data protection policies, procedures and guidelines drawn up by QQI;
- Ensure that all the data they access, manage and control as part of their daily duties is handled in accordance with data protection requirements; and
- Ensure data protection compliance within their department.

#### 7.1. Training

All QQI staff will receive data protection training. New joiners will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the law or to our policy and procedures. QQI's approach to training and awareness is:

- The Data Protection Officer assigns data protection responsibilities to employees in relation to QQI's policies and procedures on personal data management.
- The Data Protection Officer shall endeavour to ensure that all employees with day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, exhibit compliance with the GDPR.
- The Data Protection Officer will endeavour to ensure that these employees are kept up to date and informed of any issues related to personal data.
- The Data Protection Officer will endeavour to ensure that all security requirements related to data protection are demonstrated and communicated to employees/staff to the same affect.
- Employees are provided with training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with QQI's policies and procedures.

- All trainings should consider what employees need and how they can learn best. This is why, training may vary and be delivered via multiple training methods like workshops, e-learning, focused presentation and more.
- GDPR awareness training will be included for all employees as part of their on-boarding procedure and at least yearly thereafter.

The following learning objectives have been set out as part of the general staff awareness programme;

- To understand the basics of GDPR and key changes from previous data protection policy;
- To learn about GDPR principles and individual rights;
- To better understand accountability and governance challenges;
- To appreciate new enforcement approaches, fines and penalties;
- What steps to take towards achieving and maintaining compliance.

QQI shall endeavour to implement appropriate measures to make its employees aware of the contents of this Data Protection Policy document and their data protection training requirements.

Completion of data protection training is compulsory, and the HR function will maintain training records and a log of all training that takes place on an on-going basis. Any training outstanding or incomplete will be followed up promptly to ensure employees are aware of their data protection training requirements. The escalation process will include the following;

- In the first instance the HR department will send the employee a reminder of any outstanding training within two weeks;
- HR will then raise the issue of outstanding training with the employee's relevant manager after two weeks;
- If training is still outstanding the Director/ Head of Unit will be made aware within one month of outstanding training.

Training is delivered via in person and virtual methods and covers:

- Relevant and applicable regulatory principles, responsibilities and obligations related to data protection and privacy; and
- The company's data protection and related policies and procedures.

## 7.2. Failing to comply with this policy

QQI takes compliance with this policy very seriously. Failure to comply puts individuals and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to action under existing HR procedures in operation in QQI.

All records created during duties carried out on QQI's behalf are the property of QQI and subject to its overall control.

Anyone who processes QQI's data is required to:

- Read, understand and accept any data protection policies, procedures and guidelines drawn up by QQI;
- Ensure that all the data they access, manage and control as part of their daily duties is handled in accordance with data protection requirements; and
- Ensure data protection compliance within their department.

QQI is required under GDPR to appoint a mandatory Data Protection Officer.

The appointment of a person to the role of Data Protection Officer and any supporting employees is based on a number of criteria, including:

1. Experience and knowledge held by the person to carry out the responsibilities of the role in a reasonable manner;
2. Adequate time to fulfil the requirements of the role; and
3. Sufficient seniority within the organisation to carry out the role independently.

## 8. Responsibilities of the Data Protection Officer

The Data Protection Officer will be responsible for the following duties:

- Provide advice and information to QQI employees and its processors on all aspects of Data Protection law and its effects on QQI's processes and procedures;
- Monitor compliance with the GDPR and all associated QQI policies and procedures by QQI employees and any external processors, through a defined and auditable risk-based monitoring plan;
- Where requested/ required by the circumstances, to provide advice to QQI on the outcome of a data protection impact assessment carried out within the organisation;
- Co-operate with the Data Protection Commission, and any other supervisory authorities which may have cause to contact QQI, and to act as the single point of contact with QQI for issues in relation to the processing of personal data by QQI;
- Be accessible to all data subjects of QQI with regard to the rights of data subjects over their personal data;
- Carry out all of their responsibilities with the appropriate level of confidentiality as required by the circumstances in which they are carrying out their role; and
- Provide regular reporting to the Board of QQI.

## 9. Governance

QQI will monitor compliance with data protection regulations on an ongoing basis. The below outline the reporting and escalation structure currently in place;

- The DPO reports to the Executive Management Team on a quarterly basis;
- The DPO reports to the Board and Audit and Risk Committee on a bi-annual basis.

## 10. Retention Periods

QQI should not retain personal data longer than is required by law, contract or any other legal or contractual obligation. Personal data is retained in accordance with the established guidelines within QQI's retention policy.