Document Title	Data Protection Policy
Policy Area	Area 8: Information and Data Management
Document Code (version #)	QAP8-2 (V2.0)
Applies to	☒ All ☐ Specific
	☐ Staff only ☐ Learners only ☒ Staff and Learners

Document Owner	Managing Director
Approved by	Board of Directors

Approval date	12/3/19
Effective date	13/3/19

Related legislation, policies, procedures, guidelines and local protocols	This policy has been designed with due regard to the following: - Core Statutory Quality Assurance Guidelines (2016), QQI - Sector Specific Independent/Private Statutory Quality Assurance Guidelines (2016), QQI - Qualifications and Quality Assurance (Education and Training) Act 2012 - European Association for Quality Assurance in Higher Education (ENQA), et. al (2015), Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG) - General Data Protection Regulation (GDPR), 2016.

Table of Contents

1. PURPOSE

This policy is a statement of SQT's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Act (2018) and General Data Protection Regulation (GDPR). It sets out the protocols and principles by which SQT operate in order to comply with its statutory requirements.

2. SCOPE/APPLICATION

This policy applies to all processing activities involving personal and sensitive personal data (special categories of personal data), whether in electronic or physical format.

Specifically, the policy applies to:

- Any person who receives, handles or processes personal data on behalf of SQT (direct employees, Tutors etc.).
- Third party companies (data processors) that receive, handle, or process personal data on behalf of SQT.

3. DEFINITIONS

For the purposes of the GDPR and the policies, procedures and protocols set out within this document, the following definitions (as set out in the relevant legislation) apply:

- **personal data** means 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;
- **processing** means 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;
- **filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **controller** means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **third party** means 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;
- **consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **personal data breach** means 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;
- **data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **representative** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
- **enterprise** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- **cross-border processing** means either:
    - processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
    - processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

4. RESPONSIBILITY

The following responsibilities apply with respect to the implementation of this policy:

- The Board of Directors approves this policy
- The Managing Director is responsible for ensuring site wide compliance
- All staff are responsible for ensuring compliance within their respective roles

5. POLICY OVERVIEW

SQT is committed to collecting, processing, storing and destroying personal data in accordance with the General Data Protection Regulation (GDPR) 2016, and any other associated legal, accreditation, or

regulatory body rules or applicable codes of conduct. The organisation has developed policies, procedures, protocols, controls and measures to ensure compliance with the GDPR. Ensuring and maintaining the security and safety of personal and / or special category personal data is paramount to SQT's ethos.

6. PRINCIPLES OF DATA PROTECTION

SQT is committed to complying with the six principles of data protection as set out in the GDPR, which state:

1. Personal data shall only be processed fairly, lawfully and in a transparent manner (Principles of Lawfulness, Fairness and Transparency);
2. Personal data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes (Principle of Purpose Limitation);
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed (Principle of Data Minimisation);
4. Personal data shall be accurate, and where necessary kept up to date (Principle of Accuracy);
5. Personal data shall not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the personal data are processed (Principle of Data Storage Limitation);
6. Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
    a. prevent and / or identify unauthorised or unlawful access to, or processing of, Personal Data; and
    b. prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality);

SQT, whether serving as a Data Controller or a Data Processor, shall be responsible for, and be able to demonstrate compliance with these key principles (Principle of Accountability).

7. PURPOSE OF DATA COLLECTION

In accordance with its function, SQT is required to collect, use and retain (for as long as is necessary for the purpose or purposes for which it was obtained) personal data and information for a variety of necessary purposes about its staff, learners and other relevant individuals. Personal data is collected for the following purposes[1]:

- To administer learner studies, record academic achievements and determine/record the overall award outcome.
- To support learners in their studies i.e. we may use information provided (e.g. information about a disability) and information we collect about experiences with services.

[1] This is not an exhaustive list

- To monitor and evaluate the learner experience.
- To carry out audits (internal and external).
- To administer the financial aspects of learner registration (e.g. payment of fees, debt collection).
- To enable effective communication with data subjects.
- To administer appeals, complaints, grievances, disciplinary matters, and matters relating to conduct and cheating / plagiarism.
- To ensure health and safety polices are complied with.
- To produce reports and aggregated statistics for management and statutory purposes in order to plan and improve services.
- To administer voluntary surveys of learner opinion about experience and the performance of the organisation.
- To confirm the details of academic achievements, and for statistical and historical purposes, a core record of each learners performance is retained indefinitely.
- To enable our continued contact with learners after course completion (e.g. survey of graduates etc.).
- To respond to requests for information made under the Data Protection legislation.
- Recruitment, selection and employment matters (for staff).

SQT may also disseminate promotional and marketing materials to individuals who have consented to provide personal information such as email addresses. Individuals may remove themselves from all mailing lists generated by SQT at any time.

8. COLLECTION OF PERSONAL DATA

This section sets out the protocols in place for the collection of personal data, specifically:-

- sensitive data
- data collected directly from the data subject
- data collected from individuals other than the data subject (for example, Company Course Organiser)

8.1 Sensitive Data

The GDPR refers to sensitive personal data as 'special categories of personal data'. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. SQT collects a minimal level of special category 'health' data in the case of applicants requesting extensions for assessment on the basis of health reason. In addition, applicants on specific courses are asked to provide details of special learning difficulties (if applicable). Such information is

used only for the purpose of learner registrations and is destroyed in accordance with SQT's data retention schedule.

8.2 Data Collected Directly from the Data Subject

SQT's privacy policy is easily accessible to prospective learners (data subjects) when completing online booking forms. This privacy policy includes the following information:

- The identity and contact details for the organisation.
- The purposes of the processing as well as the legal basis for the processing using clear and plain language.
- The recipients or categories of recipients of the personal data.
- Whether the organisation intends to transfer the data to a third country or international organisation and what appropriate and suitable safeguards there are or whether there is an adequacy decision for such transfer.
- The retention period of the data.
- The right to request access to, rectification of, erasure of personal data and the restriction of or object to processing.
- The right to request data portability.
- The right to withdraw consent at any time.
- The right to make a complaint to the supervisory authority.
- If the personal data is required by law or contract or is a necessary requirement to enter into a contract and the possible consequences of failure to provide such data.

8.3 Data Not Collected Directly from the Data Subject

In the case of In-house courses delivered by SQT, the personal data may be provided to SQT by a company representative e.g. Company Course Organiser. In this instance, it is the responsibility of the course organiser to provide the data subject with access to the following:

- Information pertaining to the programme of study
- a link to SQT's privacy policy

This information is provided to the company representative via email when a course booking is confirmed.

9. CONSENT TO DATA PROCESSING

Where consent is considered to be the lawful basis for collecting and processing information (such as the case for collecting personal information for marketing purposes), it is contained in a written declaration which is distinguishable on all hardcopy and online forms which includes but is not limited to, course booking forms, course assessment forms and assessment cover sheets.

SQT ensures that the following protocols are implemented with respect to obtaining consent from data subjects when providing personal information.

- Data subjects are asked to positively opt in.
- Pre-ticked boxes or any other type of consent by default is not used.
- Clear and plain language is used in all cases.
- Data subject is informed of his/her right to revoke their consent at any time - revocation of consent is as easy to do as giving consent and is acted upon without undue delay.
- The purpose(s) for which the personal data is to be used is/are distinct and legitimate and explained in clear, easily understood and transparent terms.
- A record of when and how the consent was obtained and what the data subject was told at the time.
- Consents given are regularly reviewed to ensure that the processing and purposes have not changed. Renewed consents are requested when required.

10. PROTOCOLS - PROCESSING PERSONAL DATA

Personal data is only processed by SQT for the purpose(s) for which it was given and in compliance with the regulation. The following protocols are implemented with respect to the processing of personal data.

10.1 Sharing Data with Third Parties

As a general rule, personal data is not passed on to third parties, particularly if it involves special categories of personal data. However, there are certain circumstances when it is necessary for SQT to carry out its function, for example:

- SQT may disclose learner's personal data and sensitive personal data/special category data to Tutors, client companies and external agencies such as awarding bodies to which it has obligations or a legitimate reason. Such sharing is clearly explained in the privacy statement which is accessible here.
- The data subject consents to the sharing of information.
- The Third Party is operating as a Data Processor and meets the requirements of GDPR. Where a third party is engaged for processing activities, there must be a written contract, or equivalent in place which shall clearly set out respective parties responsibilities and must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.

10.2 Transfer of Personal Data Located Outside of the EU

SQT presently offer a number of programmes which are certified by organisations based outside of the EU, namely, AEE (Association of Electrical Engineers) and the Food Safety Preventative Controls

Alliance (FSPCA). Personal information is required to register and become certified by these organisations. These are clearly stated on the relevant application form.

In circumstances where a learner is resident outside of European Union or SQT delivers a programme outside of the European Union, SQT will exchange personal data with the learner / company.

11. SAFEGUARDING PERSONAL INFORMATION

SQT only processes data in a manner, which ensures appropriate security of the data including protection against unauthorised or unlawful processing and against accidental or unlawful loss, destruction, alteration, unauthorised disclosure of or access to personal data or damage using appropriate technical or organisational measures, which may include encryption.

11.1 Protocols

SQT implements the following protocols, in order to ensure the appropriate safeguarding of personal data.

- access to information is restricted to authorised staff in accordance with defined policy.
- security measures and policies are in place in relation to the use of laptops and other mobile storage devices.
- computer systems are password protected.
- information on computer screens and paper files are hidden from callers to the office.
- no documentation of a “confidential/sensitive nature” is left on desks/photocopiers etc.
- personal data stored on portable devices are protected by encryption mechanisms.
- arrangements are in place to fully delete data from portable devices such as laptops when it is no longer used.
- appropriate facilities are in place for the disposal of confidential waste.
- keeping premises secure, especially when unoccupied.
- audit logs are available in relation to read access, changes, additions deletions on the MIS system.

11.2 Retention of Data

SQT maintains a register of relevant records of personal data and other quality-related records. This register specifies data retention periods. In determining appropriate retention periods, SQT gives regard to statutory obligations imposed such as those defined for financial records. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data is deleted or disposed of in a secure manner.

11.3 Destruction of Personal Data

- **Destruction of Data using Third Party Vendors (i.e. shredding companies)*:*** SQT employs the services of a shredding contractor to destroy hardcopy personal data. A signed contract is in

place ensuring their obligations to comply with data protection legislation and to ensure that the documents are securely and permanently destroyed.

- **Destruction of Data held by Third Parties such as Tutors (i.e. anyone who processes it):** Safeguards specified in Data Protection Agreements are in place, in order to ensure that all processors return or delete securely any personal data including copies as required by the organisation.

12. TRAINING & AWARENESS

All staff receive data protection awareness training specific to their role. This training will be periodically reviewed and refreshed to ensure continuing professional development in the area of data protection law and the general data protection regulation.

13. AUDITING AND DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Prior to the development of this updated policy, SQT carried out a Data Protection Impact Assessment to identify and mitigate against any data protection related risks. A Data Protection Impact Assessment (DPIA) is designed to assist SQT in assessing the risks associated with data processing activities that may pose a high risk to the rights and freedoms of individuals and is a requirement of the GDPR.

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified, examined and assessed in order to enable the organisation to evaluate and address the likely impacts of new initiatives and put in place appropriate measures to minimise or reduce the risks (including non-implementation).

Data Protection Impact Assessments are required under GDPR in certain circumstances including:

- when the processing of personal data may result in a high risk to the rights and freedoms of a data subject
- processing of large amounts of personal data,
- processing of special categories of personal data,
- where there is automatic processing/profiling

SQT is committed to undertaking a DPIA when required under the direction of the Managing Director.

14. FURTHER INFORMATION

Should you require further information regarding this policy or if you have any query about your personal information which has been collected and processed by SQT, please direct your request to the Managing Director.

15. COMPLAINTS

All personal data enquiries, or requests to exercise your rights as a data subject, can be directed to SQT directly.

If you are dissatisfied with the information provided or believe your request to exercise your rights has not been addressed, you can make a complaint to the supervisory authority. As SQT Training Ltd. operates in Ireland, the supervisory authority is the Data Protection Commissioner, who can be contacted through the following means:

- **By post:** Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, R32 AP23, Ireland.
- **By phone:** +353 (0761) 104800
- **By email:** info@dataprotection.ie

16. POLICY MONITORING

Responsibility	Frequency	Methods
Managing Director	Per QA audit schedule	- Review of documentation as set out in QAP2-1: Ongoing Review and Update of QA Documents.
Managing Director	Annual	- Review of Data Protection Agreements (DPA's) from third parties and correspondence relating to same - Review of data protection enquiries, breaches, complaints, requests, withdrawals of consent - Review of integration with associated policies – subject access request policy, website / cookies policy, records retention policy, privacy statement etc.

17. DOCUMENT CONTROL

Version No	Approval Date	Description of Revision	Originator	Approved By
2.0	12/3/19	Policy updated to comply with GDPR.	Senior Management Team	Board of Directors