Document Title	Management of Data Breaches
Policy Area	Area 8: Information and Data Management
Document Code (version #)	QAP8-3 (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 - 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)

Table of Contents

1. Introduction 3
2. Purpose 3
3. Scope/Application 3
4. Definitions 3
5. Responsibility 4
6. Procedure for Managing a Data Breach 4
6.1. Step 1: Identification & Initial Assessment of the Incident 4
6.2. Step 2: Containment & Recovery 5
6.3. Step 3: Risk Assessment & Classification 5
6.4. Step 4: Notification 6
6.5. Step 5: Evaluation & Response 6
7. Policy Monitoring 7
8. Document Control 7

1. INTRODUCTION

SQT is legally required to notify the Office of the Data Protection Commissioner (ODPC) within 72 hours of becoming aware of a data breach. It is also required to notify the data subjects affected where the data breach in question is likely to result in a "high risk" to their rights and freedoms.

2. PURPOSE

This document governs the process to be followed in order to ensure a consistent and effective approach is in place for managing data breach and information security incidents at SQT. The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and to consider what action is necessary in order to secure personal data and prevent further breaches.

3. SCOPE/APPLICATION

The policy relates to all personal and sensitive data held by SQT, regardless of format. The procedure applies to all personnel involved in the handling or processing of personal data on behalf of SQT. This includes Programme Directors, Tutors, contractors, consultants, suppliers and data processors working for, or on behalf of SQT.

4. DEFINITIONS

A **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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. For the purpose of this procedure, data security breaches include both confirmed and suspected incidents.

An incident includes but is not limited to the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record).
- Equipment theft or failure.
- Unauthorised use of, access to or modification of data or information systems.
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- Sending personal data to an incorrect recipient.
- Unauthorised disclosure of sensitive / confidential data.
- Website defacement.
- Hacking attack.
- Unforeseen circumstances such as a fire or flood.

- Human error.
- 'Blagging' offences, where information is obtained by deceiving the organisation who holds it.

5. RESPONSIBILITY

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

- All staff have a responsibility for reporting data breaches and information security incidents, as soon as is possible, taking into account the severity of the breach.
- Training Partners are responsible for ensuring that their staff follow this policy and ensure that all relevant information is provided, as soon as is practicable, to support the breach investigation process.
- The Managing Director is responsible for ensuring full implementation of this policy and specifically for all duties identified in section 6 below.

6. PROCEDURE FOR MANAGING A DATA BREACH

In the event that SQT identifies or is notified of a personal data breach, the following steps should followed:

6.1. Step 1: Identification & Initial Assessment of the Incident

- The person who discovers/receives a report of a breach must inform the Managing Director or, in their absence, the Director of Quality and Academic Affairs and the Executive Director (in the case of high-risk breaches). Under the GDPR, SQT must report certain types of personal data breaches to the ODPC without undue delay, and within 72 hours of becoming aware of it. If the breach occurs or is discovered outside of normal working hours, this should begin as soon as is practicable.
- Upon receiving notification of a data breach, the Senior Management Team, in conjunction with other appropriate staff, will conduct an initial assessment of:
    - Whether a personal data breach has taken place;
    - The nature of the personal data involved in the breach;
    - The cause of the breach;
    - The extent of the breach (i.e. the number of individuals affected)
    - The potential harm to which affected individuals may be exposed and whether the breach can be deemed "high risk" so as to warrant notification to those individuals involved;
    - Any steps that may be taken to contain the breach, in consultation with the relevant staff members.

Following this initial assessment of the incident, the Managing Director, according to the severity of the incident, will brief the Board of Directors, if considered necessary.

6.2. Step 2: Containment & Recovery

Where a data breach occurs, immediate and appropriate steps are taken to limit the extent of the breach. The Senior Management Team, in consultation with relevant staff, will:

- Establish who needs to be made aware of the breach so as to ensure they act as required in containing the breach (e.g. isolating a compromised section of the network etc.);
- Develop correspondence for issue to affected individuals, where required, and preparation of notification and/or a report to the ODPC, if necessary.
- Establish whether there is anything that can be done to recover any losses and limit, so far as possible, the damage caused by the breach (this may be done in conjunction with relevant third part service providers, as relevant);
- Where appropriate, inform the Gardaí (for e.g. in cases involving criminal activity).

6.3. Step 3: Risk Assessment & Classification

A Risk assessment and classification is led by the Managing Director. Assessing the risk will depend on how likely it is that adverse consequences will materialise, and in the event of materialising, how serious or substantial they are likely to be. The following needs to be considered:

- The type of data involved e.g. personal, financial or medical.
- How long the breach has been going on. How sensitive the data is? Some data is sensitive, because of its very personal nature (health records), while other data types are sensitive because of what might happen if it is misused (bank account details).
- If data has been lost or stolen, was encryption or other protection methods in place?
- What has happened to the data? If data has been stolen it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been altered or damaged, this poses a different type and level of risk.
- How many individuals are affected?
- What could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic thief, while the loss of apparently trivial pieces of information could help a fraudster build up a detailed picture for identity theft.
- Who are the individuals whose data has been breached? What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these, as well as other aspects of their life?
- Are there wider consequences to consider such as loss of public confidence in the service SQT provides?
- If information has been deleted, can it be retrieved from backup systems?

Once a risk assessment has been carried out, the Managing Director determines the classification of the Risk (Low, Medium or High) and whether the risk should be reported to the ODPC.

6.4. Step 4: Notification

Based on the outcome of Step 3 above (classification and grading of the risk), in accordance with the requirements of the GDPR, incidents in which personal data has been breached must be reported to the ODPC within 72 hours of SQT becoming aware of the incident. All contact with the ODPC will be made through the Managing Director only. In the case of their absence this will be done through the Director of Quality and Academic Affairs.

SQT will also be required to notify the data subjects affected where the data breach in question is likely to result in a "medium or high risk" to their rights and freedoms. All contact with those data subjects affected will be made only after consultation and agreement with the Managing Director or Director of Quality and Academic Affairs.

6.5. Step 5: Evaluation & Response

The Senior Management Team will conduct a further assessment of the incident, as deemed appropriate by the Managing Director. Consultation with relevant staff members may be necessary to provide any additional information to the ODPC (if necessary) and to identify and mitigate any risks emerging from the breach.

In addition, in the aftermath of a data breach, the Managing Director will conduct a review of the incident with the relevant staff to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas for improvement. The Managing Director will brief the Board of Directors on the incident.

SQT maintains a log of data breaches.

7. 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 breaches and relevant documentation - Review IT security in association with IT service provider

8. DOCUMENT CONTROL

Version No	Approval Date	Description of Revision	Originator	Approved By
2.0	12/3/19	Complete revision in line with GDPR requirements and new document format.	Senior Management Team	Board of Directors