End Point Assessment Policies

Data Security Policy
GP11

Document History

Version	Date	Reason for Revision	Issued by
V1.1	July 2019	Initial release	Alan Bates
V2	March 2021	Review of policy	Alan Bates
V3	July 2021	Review of policy for our Ofqual recognition application	Alan Bates / Kay Parker
V4	December 2022	Review of policy	Alan Bates

Contents

DATA SECURITY POLICY

Introduction

The objective of this Policy is to recognise that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, Qualitrain will facilitate the secure and uninterrupted flow of information, both within Qualitrain and in external communications. Qualitrain believes that security is an integral part of the information sharing which is essential to academic and corporate endeavor and this Policy is intended to support information security measures throughout the Company. This procedure works in conjunction with Qualitrain's Document control and Retention and disposal procedures.

Qualitrain understands that General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 25 May 2018 and is actively working towards compliance with that directive.

The Principles

Qualitrain shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:-

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Definition

For the purposes of this document, information security is defined as the preservation of:

- Confidentiality: protecting information from unauthorised access and disclosure;
- Integrity: safeguarding the accuracy and completeness of information and processing methods;
- Availability: ensuring that information and associated services are available to authorised users when required

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films or photos, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

1. Protection of Personal Data:

Qualitrain holds and processes information about employees, learners, and other data subjects for academic, administrative and commercial purposes. When handling such information, Qualitrain, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). Responsibilities under the 1998 Act are set out in the Data Protection Policy. To ensure Data is collated, processed and stored appropriately all staff will be trained in the work instruction QT3P4aWI2 Control of sensitive data.

2. Information Security Responsibilities:

Qualitrain believes that information security is the responsibility of all members of staff. Every person handling information or using Qualitrain information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at Qualitrain. This includes using the Ace360 used by Qualitrain for EPA evidence.

This Policy is the responsibility of the Responsible person at Qualitrain ; supervision of the Policy will be undertaken by the Directors at all times. Qualitrain will work with the IT representative to resolve any connectivity problems as this forms part of the service. For further advice and guidance, Qualitrain will use external qualified IT support companies to resolve any problems/issues.

3. Information Security End point assessment:

Qualitrain recognises the need for all staff and other users of Qualitrain systems to be aware of information security threats and concerns, and to be equipped to support this policy in the course of their normal work. The Directors have implemented a training programme in data protection for all members of staff who process personal data and will provide or arrange the provision of training in information security matters to answer particular requirements. This is completed via standardisation meetings that cover the essential requirements of Information Security and Data Protection.

Monitoring of Operational Logs: Qualitrain shall only permit the inspection and monitoring of operational logs by Directors. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur
(i) when required by or consistent with law;
(ii) when there is reason to believe that a violation of law or of a company policy has taken place; or
(iii) when there are compelling circumstances (circumstances where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of Qualitrain policies).

Access to Qualitrain Records: In general, the privacy of users' files will be respected but Qualitrain reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with policies and regulations, Ofqual audit requirements, lead provider quality checks, and to determine which records are essential for Qualitrain to function administratively or to meet its assessment obligations. Except in emergency circumstances, authorisation for access must be obtained from the Directors, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

Protection of Software: To ensure that all software and licensed products used within Qualitrain comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, Qualitrain may carry out checks from time to time to ensure that only authorised products are being used. Unauthorised copying of software or use of unauthorised products by staff may be grounds for disciplinary, and where appropriate, legal proceedings.

Virus Control: Qualitrain will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of electronic devices issued by Qualitrain or used for business shall comply with best practice, as determined from time to time by the IT representative at Qualitrain, in order to ensure that up-to-date virus protection is maintained.

4. Asset Management:

All Qualitrain information assets (data, software, computer and communications equipment) shall be accounted for and have a designated owner. The owner shall be responsible for the maintenance and the protection of the asset/s concerned. Currently, all ownership belongs to the Directors will share responsibility for all assets within the organisation.

5. Physical and Environmental Security:

Physical security and environmental conditions must be commensurate with the risks to the area concerned. In particular, critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls. There is a CCTV in the ground floors that cover all entry points. All new staff members at Qualitrain will be provided with a guide on all security measures prior to joining the team and this will be included in their staff induction. A copy of all key holders is held and reviewed as part of Qualitrain's audit procedures.

6. Information Systems Acquisition, Development and Maintenance:

Information security risks must be identified at the earliest stage in the development of business requirements for new information systems or enhancements to existing information systems. Controls to mitigate the risks must be identified and implemented where appropriate.

7. Access Control:

Access to information and information systems must be driven by business requirements and be commensurate and proportionate to the business need. The Qualitrain Management Information & Data Protection Policy will govern this by EQA requirements.

8. Communications and Operations Management:

Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities must be established. Overall responsibility will be with the Directors at Qualitrain. The Qualitrain Management Information & Data Protection Policy will govern this by contracts/ESFA/Awarding Body requirements.

9. Retention and Disposal of Information:

All staff have a responsibility to consider security when disposing of information in the course of their work. Owners of information assets follow the Retention and disposal procedure. Retention periods should be set in consultation with the Directors at Qualitrain. The Qualitrain Management Information & Data Protection Policy will govern this by contracts/ESFA/Awarding Body requirements.

10. Reporting:

All staff, students and other users should report immediately via the Directors, any observed or suspected security incidents where a breach of Qualitrain's security policies has or may have occurred, and any security weaknesses in, or threats to, systems or services.

11. Business Continuity:

Qualitrain will implement, and regularly update, a business continuity management process to counteract interruptions to normal activity and to protect critical processes from the effects of failures or damage to vital services or facilities. Please see the current Business Continuity Policy for further details on the process and responsibilities.

12. Use of USB Flash Drives and Type 3 Drives:

USB flash drives and Type 3 drives must only be used and considered if other secure means of data transfer have been explored and not possible for the transfer of personal or business sensitive data or information. Training materials are allowed to be transferred using these methods. Should the need to use a USB flash drive or type 3 drive be required data must be encrypted. Encryption is to be done by Qualitrain's IT support service.