Quest Vocational Training Ltd

Data Protection & Privacy Policy

Policy Review Statement:	This policy will be reviewed and updated as necessary in line with industry or business changes. All of Quest's policies are reviewed at least once a year to ensure relevance and currency.
Responsibility:	Claire Reade – Data Protection Champion
Authorised by:	Carolyn Maple – Managing Director
Version:	V.1.6 May 21

Contents

1. INTRODUCTION

It is Quest's policy to comply with applicable Data Protection and Privacy laws and regulations. Quest understands the importance of safeguarding the confidentiality, security and integrity of personal information submitted to us and treats all of its legal and compliance obligations with the utmost importance.

This policy conforms to the General Data Protection Regulation (GDPR).

1.1 Policy Statement

Quest receives, uses and stores personal data about job applicants, employees and learners, including Apprentices, for a variety of purposes connected with delivering training and the general running of the business. It is important that this information is handled lawfully and appropriately in line with the requirements of the General Data Protection Regulation (GDPR).

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

This policy sets out how Quest seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that Quest's Data Protection Champion is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. Any data breaches must reported by staff immediately to Quest's Data Protection Champion.

1.2 About This Policy

This policy applies to all staff, which for these purposes includes employees, temporary, associates and volunteers. All staff must be familiar with this policy and comply with its terms.

Quest has a nominated Data Protection Champion who is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Champion or reported in line with the organisation's Whistleblowing Policy or Grievance Policy.

1.3 What is Personal Data?

Personal Data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession). For example, information relating to identifiable individuals, such as job/course applicants, current and former employees/learners, associates, volunteers. This includes expression of opinion about the individual.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Business Purposes means the purposes for which personal data may be used by Quest, e.g. personnel, administrative, financial, regulatory, payroll and training purposes.

2. DATA PROTECTION PRINCIPLES

Quest's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All employees have personal responsibility for the practical application of Quest's Data Protection policy. Quest will observe the following principles in respect of the processing of personal data.

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.
e. Kept in a form which permits identification for no longer than necessary for the intended purposes.
f. Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
g. Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

2.1 Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

2.2 Adequate, Relevant and Not Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

2.2.1 Gathering Data:
When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. See **annex A** for **Quest's privacy notices.**

2.2.2 Sensitive Data:
It will normally be necessary to have an individual's explicit consent to process 'sensitive personal data', unless exceptional circumstances apply or the processing is necessary to comply with a legal requirement. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact Quest's Data Protection Champion for more information on obtaining consent to process sensitive personal data.

2.3 Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask Quest to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held in inaccurate, they should nevertheless record the fact this it is disputed and inform Quest's Data Protection Champion.

Staff must ensure that personal data held by Quest relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform Quest so that Quest's records can be updated.

2.4 Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if the data processor agrees to comply with those procedures and policies, or if the data processor puts in place adequate measures.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) **Confidentiality** means that only people who are authorised to use the data can access it.
b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Quest's central software systems instead of individual PCs.

Security procedures include:

a. **Entry controls**. Any stranger seen in entry-controlled areas should be reported.
b. **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
c. **Data minimisation**.
d. **Pseudonymisation and encryption of data**.
e. **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
f. **Equipment**. Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC/laptop/tablet when it is left unattended.
g. **Transferring Personal Data Outside of the EEA**. We may transfer any personal data we hold to a country outside the European Economic Area ('EEA') or to an international organisation, provided that one of the following conditions applies:

a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
b) The data subject has given his consent.
c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Quest does not currently transfer or share data with any partners outside the EEA which includes the EU countries, Norway, Iceland and Liechtenstein. Staff should consult with Quest's Data Protection Champion to discuss the necessary steps to ensure adequate protection if such arrangements exist in the future.

Quest holds the Cyber Essentials Certification. Further details can be found in **Quest's Information Security Policy.**

2.5 Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Data Retention
The length of time over which data should be retained will depend upon the circumstances including the reasons why the personal data were obtained. See Quest's Document Storage, Retention and Disposal Policy and Quest's Information Security Policy.

2.6 Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:
a) Confirmation as to whether or not personal data concerning the individual is being processed.
b) Request access to any data held about them by a data controller (see also Clause 3 Subject Access Requests).
c) Request rectification, erasure or restriction on processing of their personal data.
d) Lodge a complaint with a supervisory authority.
e) Data portability.
f) Object to processing including for direct marketing.
g) Not be subject to automated decision-making including profiling in certain circumstances.

All requests from Data Subjects should be referred immediately to Quest's Data Protection Champion. This is particularly important as Quest by law must respond to a valid request with 1 month.

2.7 Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in Quest's privacy notices. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, prime-contractors and others).

We will only process personal data for the specific purposes set out in Quest's privacy notices. or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

2.8 Notifying Individuals

If we collect personal data directly from an individual, we will inform them through privacy statements about:

a) The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b) Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
c) The types of third parties, if any, with which we will share or disclose that personal data.
d) If applicable, the fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place.
e) How individuals can limit our use and disclosure of their personal data.
f) Information about the period that their information will be stored or the criteria used to determine that period.
g) Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
h) Their right to object to processing and their right to data portability.
i) Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
j) The right to lodge a complaint with the Information Commissioners Office.
k) If applicable, other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
l) Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data and our contact details and who Quest's Data Protection Champion is.

2.9 Reporting Breaches.

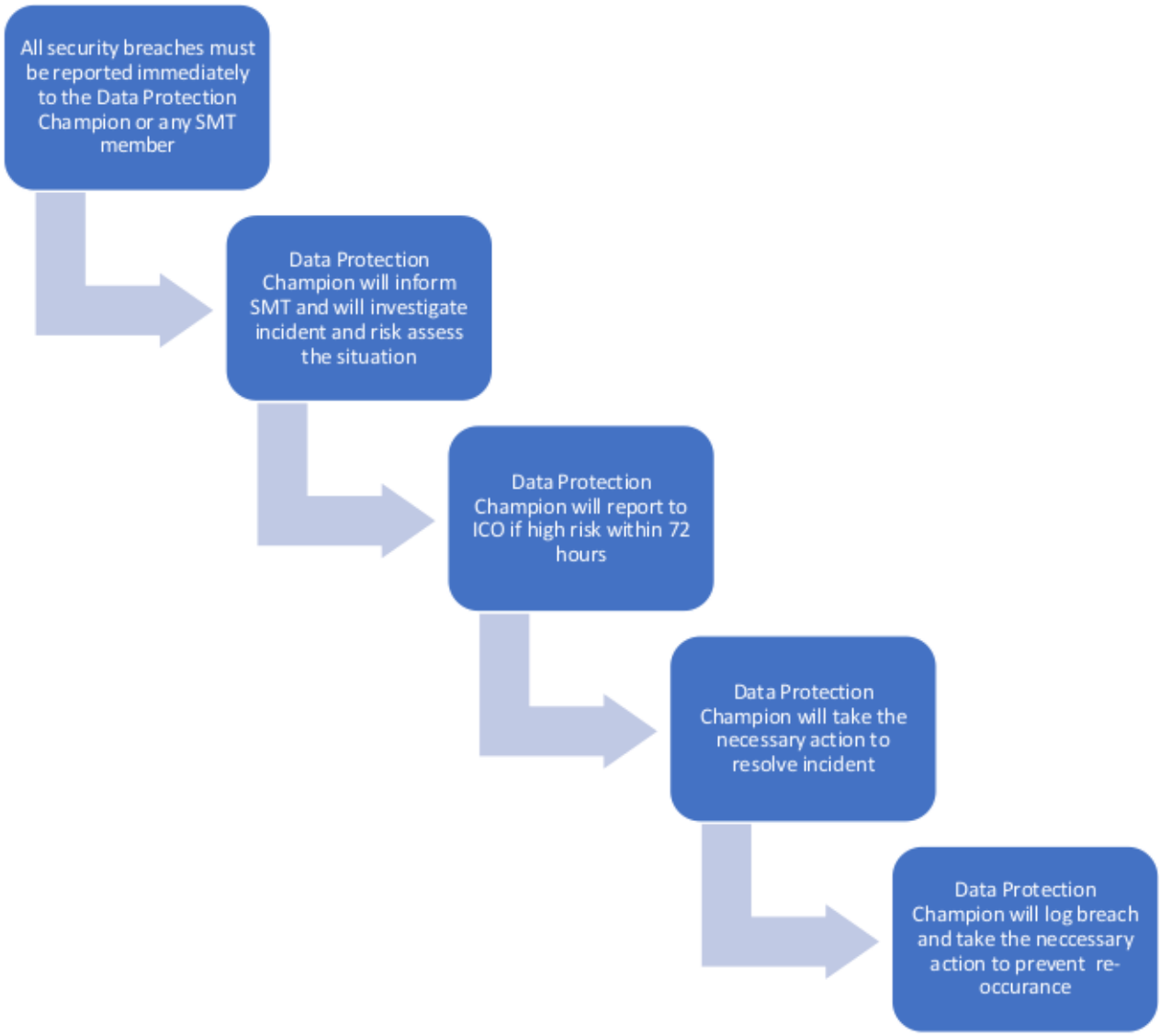
All staff have an obligation to report actual or potential data protection compliance failures to Quest's Data Protection Champion.

This allows Quest to:

2.9.1 Investigate the failure and take remedial steps if necessary.

2.9.2 Make an applicable notification to the Data Protection Regulator for the UK (The Office of the Information Commissioner - ICO).

How to report a breach flowchart



3. SUBJECT ACCESS REQUESTS

Individuals must make a formal request for information we hold about them. Employees who receive a request should forward it to Quest's Data Protection Champion immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Where a request is made electronically, data will be provided electronically where possible in a secure manner.

Our employees will refer a request to Quest's Data Protection Champion for assistance in difficult situations.

4. CONSEQUENCES OF FAILING TO COMPLY

Quest takes compliance with this policy very seriously. Failure to comply puts both staff and Quest at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

5. STAFF TRAINING

All staff including associates and volunteers will be trained in Data Protection and training will be regularly updated as follows:

Staff member	Formal Training
New member of staff	Within induction programme
Existing staff member	Every two years
Data Protection Champion	Ongoing and regular CPD

Records will be held by Human Resources showing who has been trained and when and this information will be shared with Data Protection Champion.

It is the responsibility of the Data Protection Champion to raise awareness amongst staff on a regular basis.

The rationale behind the training is to develop a competent, vigilant management framework. In doing so, the protection of learners will not rely solely on the screening of employees through recruitment and DBS checks but through a systematic approach to safeguarding.

Training will be revised and developed in line with changes in Data Protection Law and internal audits on policies and procedures.

6. MONITORING ARRANGEMENTS

- Through queries and issues raised with the Data Protection Champion.
- Through audits carried out by the Data Protection Champion.
- Through feedback i.e. complaints, suggestions and surveys.
- Through annual Policy review by the Data Protection Champion.

7. CHANGES TO THIS POLICY

Quest reserves the right to change this policy at any time. Staff will be informed of any changes.

8. KEY CONTACTS

ROLE	CONTACT DETAILS
Quest's Data Protection Champion	Claire Reade, Data Protection Champion Quest Vocational Training, Ground Floor West Pear Tree Business Centre, Cobham Road, Ferndown, Dorset BH21 7PT Tel: 01202 237378 Mobile:0797 150 2852
Data Protection Regulator	The Office of the Information Commissioner (ICO) Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF Tel: 01625 545 745 Website: www.ico.org.uk

Annex A – Quest's Privacy Notices

Quest has carried out an audit of personal data collected, processed and held. A full record is maintained by the Data Protection Champion. We have four clear privacy notices to support the work that Quest carries out:

Privacy Notice	Purpose	How Advised
Website Privacy Notice	To describe how Quest collects and uses personal information about people who visit our website and give us their data over the telephone, face to face and in writing.	Available on website
Staff recruitment Privacy Notice	To describe how Quest collects and uses personal information on applying for a job with Quest.	Available on Careers page of website with summary version on application form.
Employee Privacy Notice	To describe how Quest collects and uses personal information on joining Quest as an employee.	Available on issue of contract of employment and in the HR section of the staff zone
Apprentices at Quest - Privacy Notice	To describe how Quest collects and uses personal information on joining an Apprenticeship with Quest.	Available before sign up process.
Commercial Learners at Quest – Privacy Notice	To describe how Quest collects and uses personal information on joining a training course with Quest.	Available before sign up process.