European Union
European
Social Fund

Education & Skills
Funding Agency

Skills People Group
QUALIFICATIONS & TRAINING

General Data Protection Policy

Skills People Group

Construction Skills People
QUALIFICATIONS & TRAINING
A Skills People Group Company

C&G
ASSESSMENTS
& TRAINING LTD

trainingfutures
(UK) Ltd

1. Introduction

Skills People Group consists of the following companies.

- *Construction Skills People*
- *C&G Assessments and Training Ltd*
- *Training Futures UK Ltd*

The company is committed to comply with the General Data Protection Regulation (GDPR) which forms part of data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018) and the main provisions that apply from the 25th May 2018.

The company collect and retain information about employees, learners and third parties to comply with:

- *Funding rules*
- *Awarding organisation requirements*
- *Government agencies*
- *HM Revenues and Customs*
- *Accounts and Internal Audit*
- *Recruitment*

2. Overview

The company is required to retain certain information about its employees, learners and third parties to monitor: performance, achievement, health and safety, safeguarding, safer recruitment, and pay salaries. It is necessary to collect and process information to enrol learners onto courses, organise training and ensure that legal obligations to funding organisations and government agencies are complied with.

Information may be shared with awarding organisations, regulatory bodies, funding partners and third parties for education, training, employment and well-being related purposes including research. Sharing will only take place where the law allows it and the sharing is in compliance with data protection legislation.

Consent can be withdrawn at any time by contacting the Data Protection Officer.

3. Purpose

The purpose of this policy is to ensure that everyone handling personal information is fully aware of the requirements and that data subjects are aware of their individual rights.

This policy outlines the steps which must be undertaken to ensure the company complies with General Data Protection Regulations (GDPR) and supplementary enacting on Data Protection Legislation.

4. Objectives

To fully comply with the GDPR, the company has appointed a Data Protection Officer, the Group Operations Director who is responsible for and is aware of the organisations obligations under the General Data Protection Regulations.

This policy will be reviewed annually by the Quality Manager and Data Protection Officer and/or in line with changes or new legislation and/or regulations.

Skills People Group

5. Scope

This policy applies to all staff, learners, and to the following when acting on behalf of the company: Employers of apprentices, associate assessor/tutor and any other third party.

6. Definitions

- **Processing**; includes collecting, recording, storing, using, analysing, combining, disclosing or deleting data. Processing is almost anything you do with data.
- **Personal data** only includes information relating to a natural person who:
    - *can be identified or who are identifiable, directly from the information in question; or*
    - *who can be indirectly identified from that information in combination with other information.*
- **Special category data** is personal data which the GDPR says is more sensitive, and so needs more protection. for example, information about an individual's: race, ethnic origin, politics, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation. In particular this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

7. Principles of General Data Protection Regulations

Authorised processing of information takes place as part of the day-to-day business however, the company will ensure that employees who process personal information follow the data protection principles.

In summary, we will ensure that personal data shall:

- be processed in a lawful, fair and transparent manner *(Lawfulness, fairness and transparency)*
- be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes *(Purpose limitation)*
- kept adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed *(Data Minimisation)*
- kept accurate and, where necessary, kept up to date *(Accuracy)*
- kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data is processed *(Storage limitation)*
- processed in a manner that ensures appropriate security of personal data *(Integrity and confidentiality – Security)*
- take responsibility for what we do with personal data and how we comply with the other data principles *(Accountability)*

8. Special Category Data

Data such as race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation data, is only requested where the law allows it and processed in accordance with the data principles.

Criminal Offence Data (convictions and offences) will only be processed where we have a lawful basis to do so. A privacy impact assessment will be completed for this special category data.

Skills People Group

9. Privacy Impact Assessment

Some of the processing that the company carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks

10. Data Security

The company takes the security of personal data seriously. Employees are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party

Unauthorised disclosure will be deemed a disciplinary matter and may in serious cases be considered as gross misconduct.

Personal information whether electronic or paper based will be:

- Secured in a locked filing cabinet, or drawer
- If it is computerised, be password protected
- Moved from its storage location only when necessary

Employees are required to ensure that casual disclosure does not take place; by, for example leaving computer printouts uncovered on desktops or by allowing unauthorised users to view computer screens. Printouts containing any confidential information must be kept securely, and destroyed in a confidential manner.

Extreme care must be taken to ensure that emails are sent securely and emails/attachments containing personal data are encrypted or password protected as a minimum requirement. The encryption key or password must be communicated using a different method of communication. Passwords to are to be provided over the telephone or by text.

Offices where staff are employed to process personal data should be locked when not occupied.

Employees working from home or outside the office are responsible for taking extreme care with personal data to ensure this is keep secure.

Computer screens are locked when employees are away from their workstation.

The company aims to minimise the storage of, and, access to personal data on removable media, such as, laptops, external hard drives, flash drives and USB pens which may be lost or stolen. Permission to store personal data on portable or removable media must be given by a director.

**this list is not inclusive.*

Refer to the following policies for further information.:

- *Password Policy*
- *Email Policy*
- *Network Access and Authentication Policy*
- *Data Classification Policy*
- *Physical Securities Policy*
- *Acceptable Use Policy*
- *Mobile Device Policy*

Skills People Group

11. Employees

Employees are responsible for checking that any information that they provide in connection with their employment is accurate and kept up to date.

12. CCTV

The company will follow the guidance in the Information Commission's Code of Practice for users of CCTV and similar surveillance equipment monitoring spaces to which the public, learners and employees have access.

Areas where CCTV is in operation will have clear signage, so people are aware they are being recorded.

The company retains CCTV images for no longer than 30 days, unless the images are being used for an investigation or have been requested via a subject access request.

13. Personal Data Rights – Right to Access

Employees, apprentices, learners and other third parties have individual rights to access personal data that is being held about them either on computer or in manual files.

Individuals have the right to:

- be informed about information we collect and *share (The right to be informed)*
- access your personal data *(The right of access)*
- rectification of inaccurate personal data *(The right to rectification)*
- erasure of personal data, this right is not absolute and only applies in certain circumstances *(The right of erasure)*
- request the restriction or suspension of your personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the personal data, but not use it. *(The right to restrict processing)*
- receive personal data provided to a controller in a structured, commonly used and machine-readable format. It also gives the right to request that a controller transmits this data directly to another controller. *(The right to data portability)*
- object to the processing of personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. *(The right to object)*

Any person who wishes to exercise their rights is required to submit a subject access request to the Data Protection Officer either by:

- **Email:** quality@skillspeoplegroup.com
- **Letter:** Skills People Group, Data Protection Officer (Quality Team), Unit 1, The Bridge Business Centre, Chesterfield, S41 9FG

In most cases there is no fee charged to comply with subject access requests. However, where a request is manifestly unfounded or excessive a “reasonable fee” for the administration costs associated with the request may be required.

An individual is only entitled to request their own personal data, and not to information relating to other people without their consent.

**Refer to the Subject Access Request Policy for further information.*

Skills People Group

14. Data Breach

Employees are responsible for keeping personal information secure to prevent a data breach.

'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'.

A Personal Data Breach includes:

- *access by an unauthorised third party*
- *deliberate or accidental action (or inaction) by a controller or processor*
- *sending personal data to an incorrect recipient*
- *computing devices containing personal data being lost or stolen*
- *alteration of personal data without permission; and*
- *loss of availability of personal data*

15. Reporting a Data Breach

A notifiable Data breach must be reported to The Data Protection Officer immediately.

The Data Protection Officer will investigate the breach and report the matter to the relevant supervisory authority within 72 hours of becoming aware of it.

If necessary a data breach may be reported to: regulatory bodies, awarding organisations, funding partners and third parties. Awarding organisations include but are not limited to: HABC, Pearson, CITB, Proqual, Lantra, HESA, SQA, City & Guilds.

16. Retention of Data

At the heart GDPR, is the principle that the company will only collect and retain data as long as we need it. Article 5 of the act, states that data must be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet Funding rules, Awarding organisations, Government organisations, HM Revenues and Customs, Accounts and Internal Audit, Safer Recruitment and Employment law.

17. Applicability of Other Policies

This policy will be part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies are reviewed as needed.

18. Enforcement

This policy does not form part of the formal contract of employment, but employees are required to abide by the rules and principles of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018).

Violations to this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

Skills People Group

Any questions or concerns about the operation of this policy, or if you consider that this policy has not been followed, you should raise the matter with the Data Protection Officer, Amanda Warham on 01246 589465/07496 947089 or Quality Manager, Julie Lawton on 01246 589459/07976 745460

The company review their retention periods on an annual basis unless, there is a potential for a significant impact on individuals. The company also review personal data if any individual requests this under their 'right to erasure of personal data' that is no longer needed for specified purposes.

Skills People Group

Document Control

Date of change	Version	Overview of amendment	Amended by / Job title	Approved by	Approval date
20-06-18	6	Policy revised to bring in line with GDPR	Julie Lawton (Quality Manger)	A Warham	20-06-18
24-06-19	7	Annual review Section 4 – title changed to Principles of General Data Protection Regulations Section 6 – Definitions added Section 9 – Impact Assessment added Section 12- CCTV included Section 15 – Awarding organisations, Regulatory bodies and funding partners added as part of reporting a data breach Section 18 – Enforcement section added	Julie Lawton (Quality Manger)	A Warham (Director)	27-06-19

Skills People Group