European Union
European
Social Fund

Education & Skills
Funding Agency

Skills People Group
QUALIFICATIONS & TRAINING

General Data Protection Policy

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, workers, self employed associates, 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Consent can be withdrawn at any time by contacting the Data Protection Officer.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.

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.

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*

11. Employees, Workers and Self-Employed Associates

The Company is committed to protecting the privacy and security of your personal information.

This document describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all employees, workers and self-employed contractors

The company is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained within this document.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence and Car insurance for staff claiming business mileage
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process along with any occupationally relevant certification).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.

- Disciplinary and grievance information.
- CCTV footage which is used for security only and not on the basis on monitoring staff.
- Telephone monitoring for quality purposes
- Information about your use of our information and communications systems.
- Photographs.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies (where applicable) or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your vital interests (or someone else's interests).
2. Where it is needed in the public interest [or for official purposes].

Situations in which we will use your personal information

We need all the categories of information as listed primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing company benefits (where applicable).
- Liaising with your pension provider.
- Administering the contract, we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information.

We may process special categories of personal information in the following circumstances:

1. Where we need to carry out our legal obligations or exercise rights in connection with employment.
2. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations (where applicable).

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations.
Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We do not transfer your personal information outside the EU.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so, for example issuing a copy of your CV and / or certificates to Funders and Awarding Organisations to determine occupational competence

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors, Funding Partners, Awarding Organisations and designated agents) and (where applicable) other entities within our group.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. In order to determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please

keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Quality Team in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. In order to withdraw your consent, please contact your Quality Department (including the legal basis for your belief that your consent can be withdrawn). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to,

unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact your Quality Department;

By Telephone: 01246 589459
By Email: quality@skillspeoplegroup.com

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.*

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, 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.

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.

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
09-07-20	8	Policy merged with 'GDPR Policy for Employees, Workers and Self Employed Page 2 – Added 'workers, self employed associates' to Overview. Page 13 – Removed 'HESA' from Awarding Organisation List	Sarah Booth (HR Assistant)	D Read	16-07-20