

## UKTD Data Protection Policy (GDPR)

|  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

### 1. Introduction

As both an employer and training provider, UK Training & Development needs to collect and process certain information about its employees, learners, parents and guardians and other individuals with whom it has a relationship as part of its business.

This information may be processed for various purposes, for example (but not limited to) to recruit and pay employees; register learners and record their progress; administrate course programmes and certification; collect fees and set up payment arrangements. UKTD also has a legal requirement to collect and use information to ensure that as a provider of work based learning in receipt of ESFA/ESF funding, we are complying with our statutory obligations to the government and Ofsted.

UKTD regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business.

### 2. Purpose

This policy is intended to ensure that all personal information is treated fairly, lawfully, correctly and in accordance with the Data Protection Act 2018 and principles of the General Data Protection Regulation (GDPR). It applies to the processing of personal data in both manual and electronic records and also covers our response to any data breach and other rights under the GDPR.

All employees have a responsibility to handle information correctly and must adhere to these guidelines. Those involved in the collection, processing and disclosure of personal data will be given additional training and specific handling instructions by their departmental manager. Employees will also need to know how to recognise and escalate a personal data breach.

### 3. Background of GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) directive which came into effect on 25<sup>th</sup> May 2018. Together with the new Data Protection Act 2018 (UK) this replaces the previous Data Protection Act of 1998.

Its purpose is to unify all EU member states' approaches to personal data processing and ensure that data protection laws are applied identically throughout the EU.

Under the GDPR there will be new obligations for organisations regarding how personal information is handled. There will also be a duty to report personal data breaches to the Information Commissioners Office (ICO) and non-compliance can result in significant fines. All personal data obtained and held must be processed according to the GDPR principles.

## UKTD Data Protection Policy (GDPR)

|  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

### 4. Definitions

Personal data – is information (either electronic or manual) that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person’s name, photograph, identification number, location or online identifier. It can also include pseudonymised data (e.g. key coded).

Special categories of personal data (formerly known as sensitive data) - is data which relates to an individual’s health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

Data subject - is the individual to whom the particular personal data is about. The Act does not count an individual who has died (or who cannot be identified or distinguished from others) as a data subject.

Data processing - is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

### 5. Data Protection Principles

Under the new Data Protection Act 2018 and EU GDPR standards, all personal data obtained and held must be processed according to the following core principles. In accordance with these principles UKTD will ensure, so far as is reasonably practicable, that:

- a) processing will be fair, lawful and transparent
- b) data will be collected for specific, explicit and legitimate purposes only
- c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
- d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- e) data is not kept for longer than is necessary for its given purpose
- f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- g) UKTD will comply with the relevant GDPR procedures for international transferring of personal data.

| <b>UKTD Data Protection Policy (GDPR)</b>  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

## 6. UK Training & Development Statement

UK Training & Development is committed to maintaining the above principles and protecting the rights and privacy of individuals in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR) May 2018. UKTD will:

- Inform individuals why information is being collected and how it will be used .
- Ensure that Privacy Notices are written in a clear way that individuals will understand.
- Check the quality and accuracy of the information we hold.
- Ensure we do not retain information for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with GDPR to respond to requests for access to personal information and have a Subject Access Request policy.
- Ensure all staff are aware of and understand UKTD policies and procedures and have been trained on the safe collection, storage and use of data.

## 7. Types of data held

### Employee data

UKTD hold employee data in both paper-based personnel files relating to each employee and also within a secure folder on the computer system.

Specifically, UKTD hold the following types of employee data:

- a) personal details such as name, address, telephone numbers
- b) name and contact details of next of kin
- c) gender, marital status, information of any disability or medical information
- d) right to work documentation
- e) information on race and religion for equality monitoring purposes

## UKTD Data Protection Policy (GDPR)

|  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

- f) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter
- g) references from former employers
- h) details on education and employment history etc
- i) National Insurance numbers
- j) bank account details
- k) tax codes
- l) driving licence details
- m) criminal convictions/DBS records (if required)
- n) IT equipment use including telephones and internet access
- o) information relating to employment with UKTD, including:
  - job title and job descriptions
  - salary details
  - wider terms and conditions of employment
  - induction and probationary period records
  - details of any formal and informal proceedings such as letters of concern, disciplinary and grievance proceedings, annual leave records, appraisal and performance information
  - records of internal and external training undertaken
  - information on time off from work including sickness absence, family related leave, etc

All of the above information is required for UKTD's processing activities.

### Learner/Employer data

UKTD hold learner/employer data in both paper-based files relating to each learner and employing business and also within a secure folder on the computer system.

Specifically, UKTD hold the following types of **learner/employer related** data:

- Personal information (such as name, unique learner number (ULN), National Insurance Number (NI) and address)
- Characteristics (such as ethnicity, language, nationality, country of birth)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Special educational needs (LSF)
- Relevant medical information (e.g. Dermatitis etc)

## 8. Access rights

Under GDPR, individuals have the following rights relating to information that is held about them:

- a. the right to be informed about data that is held and its purpose

## UKTD Data Protection Policy (GDPR)

|  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

- b. the right of access to the data held
- c. the right for any inaccuracies in the data held, however they come to light, to be corrected
- d. the right to have data deleted in certain circumstances
- e. the right to restrict the processing of the data
- f. the right to transfer the data held to another party
- g. the right to object to the inclusion of any information
- h. the right to regulate any automated decision-making and profiling of personal data.

### 9. Responsibilities

In order to protect the personal data of relevant individuals, those within our business who must process the data as part of their role have been made aware of UKTD policies on data protection.

UKTD have also appointed employees with responsibility for reviewing and auditing our data protection systems. The policy review will be undertaken by the Funding Compliance Manager and HR Manager or their nominated representatives.

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months, or as and when a change to legislation happens.

### 10. Lawful basis for processing

The law on data protection allows the processing of data for certain reasons only and UKTD acknowledge that processing may only be carried out where a lawful basis for that processing exists, for example, as part of an employee's terms and conditions of employment or as an ESFA or Ofsted requirement.

#### Seeking Consent

Where no other lawful basis applies, UKTD may seek to rely on an individual's consent in order to process data.

However, UKTD recognises the high standard attached to its use and understands that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, UKTD will do so on a specific and individual basis where appropriate. Individuals will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

| <b>UKTD Data Protection Policy (GDPR)</b>  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

## 11. Access To data

As stated above, individuals have a right to access the personal data that UKTD hold on them. To exercise this right, individuals should make a *Subject Access Request*. UKTD will comply with the request without delay, and within one month unless, in accordance with legislation, it decides that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in UKTD's Subject Access Request policy.

## 12. Data disclosures

The Company may be required to disclose certain data/information to another person. The circumstances leading to such disclosures includes:

- a. for the administration of payroll
- b. smooth operation of insurance policies and pension plans
- c. DBS checks
- d. references
- e. any employee benefits operated by third parties
- f. individuals with disability - whether any reasonable adjustments are required to assist them at work
- g. individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- h. for Statutory Sick Pay purposes
- i. HR management and administration - to consider how an individual's health affects his or her ability to do their job
- j. for required training provider purposes we routinely share learner information with:
  - The Education & Skills Funding Agency ( ESFA)
  - Ofsted
  - Matrix (Information Advice & Guidance Service).
  - PICSs (On-Line Database).
  - OneFile (On-Line Portfolio)
  - Learning Record Service (LRS)
  - ACE (Apprenticeship Certificates England)
  - Training Providers / Colleges Apprentices attend after leaving us

| <b>UKTD Data Protection Policy (GDPR)</b>  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

- k. to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

See the Privacy Notice for Employees or the Learner GDPR Notice for further details.

### 13. Data security

All UKTD employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that they are only accessed by people who have a need and a right to access them, and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to other people. Passwords should not be written down and stored with the equipment to which they relate.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

- a) ensuring that data is recorded on such devices only where absolutely necessary.
- b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow UKTD’s rules on data security may be dealt with via the Company’s Disciplinary Procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

### 14. Third party processing

| <b>UKTD Data Protection Policy (GDPR)</b>  |  |                                    |
|--|--|------------------------------------|
| <b>Issued By:</b><br>Funding & Compliance Manager on behalf of UK Training & Development | <b>Issue No:</b> 4                     | <b>Date of Issue:</b><br>May 2020  |
| <b>Approved by:</b><br>Managing Director   | <b>Signature</b><br>(hard copy signed) | <b>Date of Review:</b><br>May 2021 |

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain UKTD's commitment to protecting data.

### **15. International data transfers**

UKTD does not transfer personal data to any recipients outside of the European Economic Area.

### **16. Requirement to notify breaches**

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner (ICO) within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification Policy.

### **17. Training**

All new employees must read and understand the policies on data protection as part of their induction. All employees will receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach. The nominated compliance officer for UKTD is trained appropriately in their role under the GDPR and Data Protection.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

### **18. Records**

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR and learner data records. These records will be kept up to date, so far as is reasonably practicable, and in accordance with statutory retention periods.

### **19. Data protection compliance**

Our appointed compliance officer in respect of our data protection activities is:

Kevin Bunn, Funding & Compliance Manager

[Kevin.Bunn@uktd.co.uk](mailto:Kevin.Bunn@uktd.co.uk)