Apprenticeship Connect

Data Protection Policy

Area: IT, Data and Communications
Effective from: 28/01/2021 Review date: 28/01/2022

Data Protection Policy

Contents

1.Introduction

In the course of carrying out its various functions, Apprenticeship Connect processes a wide range of personal data relating. The organisation takes the privacy of its data subjects very seriously and is committed to:

- Providing a confidential service to its employees, learners and client employers
- Protecting and promoting the rights of its data subjects in regard to their personal data
- Complying with its legal and regulatory obligations as a data controller

The unauthorised access to, or unlawful processing of, personal data could affect the organisation's ability to meet these needs and could damage its reputation, as well as compromising the privacy of its employees, learners and client employers.

1.1 Purpose

The purpose of this policy is to set out the principles and procedures for ensuring that the organisation protects the privacy of its prospective, current and former employees, learners and client employers.

1.2 Scope

This policy applies to all personal data obtained, created, stored and transferred by the organisation and its staff, irrespective of the format in which it is held or the device on which it is stored. Pseudonymised data can fall within the scope of this policy, depending

on how difficult it is to attribute the pseudonym to a particular individual. However, if data is truly anonymised, it does not fall within the scope of this policy.

Data relating to companies or public authorities does not fall within the scope of this policy.

1.3 Definitions

- **Personal data:** any information relating to an identifiable natural person, for example: name and contact details; online identifiers such as cookies and IP addresses; and employment and education history.

- **Special category personal data:** sensitive personal information that could create significant risks to a person's fundamental rights and freedoms, for example, by putting them at risk of unlawful discrimination. Examples include race, religion, sexual orientation and biometric data.

- **Processing:** refers to anything that is done to, or with, personal data, including collecting, storing, using, altering, disclosing and deleting data.

- **Data controller:** any organisation or body that determines the purposes and means of processing personal data.

- **Data processor:** any organisation or body that processes personal data on behalf of a data controller.

- **Data subject:** a natural person whose personal data is processed by a data controller or processor

2.Legislative & Compliance Framework

The organisation's data processing activities are regulated by the Data Protection Act 2018, alongside the UK General Data Protection Regulations (UK GDPR).

The organisation is registered as a data controller with the Information Commissioner's Office (ICO), the independent regulatory office in charge of upholding information rights in the UK:

- **Registered Data Controller Name:** The Recalvi Enterprise Ltd (T/A Apprenticeship Connect)
- **Registration Number:** Z3657410
- **Date Registered:** 29 April 2013

2.1 Key Principles of the UK GDPR

The organisation understands its responsibility to fulfil data subjects' reasonable expectations of privacy when undertaking any form of data processing, and to this end, it endorses and adheres to the seven key principles set out in Article 5 of the UK GDPR:

1. Lawfulness, fairness and transparency:

- **Lawfulness:** The organisation does not permit the processing of personal data unless there is a clear and justified lawful basis for doing so. The lawful basis for any new form of data processing is determined by the Data Protection Board and communicated to data subjects prior to the processing commencing.

- **Fairness:** The organisation only processes personal data for purposes that the data subject would reasonably expect. Consent is requested in an age-appropriate and granular manner at junctures at which the data subject can make an informed decision about how they wish to proceed. They are also informed of how to withdraw their consent should they subsequently wish to do so.

- **Transparency:** The organisation provides data subjects with key information relating to data privacy and their rights in relation to processing in a layered approach throughout their engagement. They are also signposted to the appropriate privacy notice, which provides them with a detailed breakdown of:

  i what personal data is collected

  ii where personal data is obtained from

  iii how and why the organisation uses personal data

  iv the legal justification (lawful basis) for processing personal data

  v where personal data is transferred to

  vi how long personal data is stored for vii what rights data subjects have in relation to the organisation's processing

  viii contact details for the Data Protection Officer and Information Commissioner's Office for the instance that they wish to raise a query or complaint

  2. Purpose limitation: The organisation only collects personal data for explicitly specified and legitimate purposes, and does not conduct further processing in a manner that is incompatible with the purposes initially stated.

  3. Data minimisation: The organisation limits the personal data it obtains and processes to that which is absolutely necessary and relevant to the activity in

hand. This prevents unnecessary processing and reduces the impact on the data subjects' privacy.

4. Accuracy: The organisation takes reasonable steps to ensure that the personal data it processes is accurate, and where necessary, kept up to date. In the instance that inaccuracies are identified, remedial action is taken without undue delay to erase or rectify the data.

5. Storage limitation: The organisation does not keep data in a form which permits identification of data subjects for any longer than is necessary for the purposes it is being processed. The Record Retention & Disposal Policy sets out the organisation's commitment to this principle.

6. Integrity and confidentiality: The organisation takes appropriate security measures to protect personal data from deliberate or accidental loss, damage, unauthorised access or unlawful processing. Staff are granted authorisation to use systems containing personal data on a 'need to know' and 'minimum privilege' basis to prevent unnecessary access to personal, special category, and otherwise confidential information.

7. Accountability: The organisation is able to demonstrate its compliance with principles above through the following measures:

- Implementing comprehensive IT, data and communications policies detailing the organisation's commitment to data protection
- Adopting a 'data protection by design and default' approach to all new systems, projects and other initiatives
- Documenting all processing activities through a Personal Data Index
- Reporting all data breaches, security threats and near misses internally, and referring these to the Information Commissioner's Office where appropriate
- Conducting data protection impact assessments, legitimate interest assessments, compliance audits and annual self-assessments

2.2 Lawful Bases for Processing Personal Data

Under the UK GDPR, organisations data controllers must identify a clear lawful basis for each type of data processing activity they conduct. There are six available lawful bases for processing:

- **Consent:** Organisations may lawfully obtain consent from a data subject in order to process their personal data. Any requests for consent must be specific, age

appropriate, and separate from any other terms and conditions. The data subject must opt in to signify their agreement to processing, rather than their consent being assumed unless they opt out. It must also be clear and easy for a data subject to subsequently withdraw their consent.

- **Contract:** Organisations can process personal data under this lawful basis if the processing is necessary to fulfil their contractual obligations to a data subject, or because the processing is required as a precursor to entering into a contract.

- **Legal obligation:** Organisations can lawfully process personal data if it must do so in order to comply with a common law or statutory obligation.

- **Vital interests:** Personal data can be lawfully processed if it is required in order to protect a data subject's life (for example, in emergency medical situations).

- **Legitimate interests:** This lawful basis can be appropriate where an organisation processes personal data for purposes that the data subjects would reasonably expect, and in a manner that has minimal impact on their privacy.

- **Public task:** Organisations may rely on this lawful basis if the processing is carried out in the exercise of official authority, or to perform a specific task in the public interest that is set out in law.

No single basis is 'better' or more important than the others – which basis is most appropriate to use depends on the purpose of the processing and relationship between the data subject and organisation.

The lawful bases under which the organisation processes personal data are determined by the Data Protection Board and are detailed within the Privacy Notice for Applicants and Learners; the Privacy Notice for Individuals Working at a Client Employer; and the Privacy Notice for Employees. Staff are not permitted to process personal data outside of the lawful bases stated within these notices.

Note, the UK GDPR requires organisations to take particular care when processing children's personal data. The legal age in the UK for providing consent for data processing is 13. The organisation does not provide a service to learners under the age of 16 so does not require parent/guardian consent before commencing data processing. However, the organisation ensures that all consent requests and data protection-related information, advice and guidance are age-appropriate.

2.3 Data Subjects' Rights

Under the UK GDPR, data subjects have the following rights:

- Right to be informed about the collection and use of their personal data

- Right to access their personal data
- Right to have inaccurate or incomplete personal data rectified
- Right to have their personal data erased (commonly referred to as the 'right to be forgotten')
- Right to request the restriction of, suppression of processing activity relating to their personal data
- Right to obtain and reuse their personal data for their own purposes across different services
- Right to object to the processing of their personal data in certain circumstances
- Rights in relation to automated decision-making and profiling

If an individual would like to exercise their rights in relation to personal data, they should submit a request to data@apprenticeshipconnect.co.uk and the organisation will act upon this in line with the Subject Rights Procedure.

3. Responsibilities

3.1 Staff Responsibilities

All permanent, temporary, contracted and volunteer staff are responsible for:

- Ensuring that any information they provide about themselves is accurate and where appropriate, kept up to date
- Ensuring that any processing activity is conducted in line with this policy and the associated privacy notices
- Supporting data subjects to exercise their rights in line with the Subject Rights Procedure
- Maintaining their working environments and electronic devices in a manner that minimises the risk of deliberate or accidental loss, damage, or unauthorised access, in line with the Clean Office Policy, Cyber-Security Policy, and Electronic Communications Policy
- Adhering to the Cyber-Security Policy and the Electronic Communications Policy to prevent unauthorised access to, or disclosure of, personal data stored/transferred electronically

- Reporting data breaches, cyber-security incidents and near misses in line with the Data Breach & Security Incident Reporting Procedure

3.2 Designated Data Controller and Data Protection Officer

The Designated Data Controller, Rafiq Adebambo, or the Data Protection Officer (DPO), Olivia Doyle, will deal with day-to-day data protection matters including, but not limited to:

- Reporting and responding to data breaches, cyber-security incidents and near misses
- Facilitating staff training and promoting a culture of data protection and security
- Providing information, advice and guidance on data protection matters to staff as required

Any individual who considers that this policy has not been followed in respect of their own personal data should raise the matter with one of the above-named persons:

- **Data Controller:**
  - Rafiq Adebambo: rafiq.adebambo@apprenticeshipconnect.co.uk
- **Data Protection Officer:**
  - Olivia Doyle: olivia.doyle@apprenticeshipconnect.co.uk

4. Compliance

If a member of staff fails to adhere to this policy, it may result in disciplinary action up to, and including, termination of their employment. Any individual in breach of this procedure may also face civil or criminal liability if their action violates the law.

This policy does not form part of the contract of employment and any or all of its terms may be amended from time to time.