Apprenticeship Connect

Data Protection Policy

Area: IT, Data & Communications

VERSION 2.0 Effective August 2018

Data Protection Policy

The organisation is fully committed to the General Data Protection Regulations (GDPR). GDPR applies to all organisations operating within the EU, as well organisations outside the EU that offer goods or services to individuals in the EU. It sets out principles which should be followed by those who process personal data relating to their employees, customers, contractors, clients or any other individual; and it gives new and extended rights to the individuals whose data is being processed.

To this end, the organisation fully endorses and adheres to the seven principles of data protection, as set out in the Article 5 of the GDPR:

1. Lawfulness, fairness and transparency: Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose limitation: Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data minimisation: Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy: Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

5. Storage limitation: Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Integrity and confidentiality: Data must be processed 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.

7. Accountability: The organisation is responsible for, and must be able to demonstrate compliance with, the principles of data protection detailed above

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the organisation will:

- fully observe the conditions regarding the fair collection and use of information including the giving of consent
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- take appropriate technical and organisational security measures to safeguard personal information

- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

Status of this Policy

The Policy does not form part of the formal contract of employment for staff, but it is a condition of employment that staff will abide by the rules and policies made by Apprenticeship Connect; therefore, any failure to follow the Data Protection Policy may lead to disciplinary proceedings.

Designated Data Controllers and Data Protection Officers

The Designated Data Controller, Rafiq Adebambo, or the Data Protection Officer (DPO), Olivia Doyle, will deal with day-to-day data protection matters. Any member of staff, or other individual, who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with one of the above-named persons.

Staff Responsibilities

All staff are responsible for:

- checking that any information that they provide to the organisation in connection with their employment is accurate and up to date
- informing the organisation of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The organisation cannot be held responsible for any errors unless the employee has informed it of such changes
- responding to data subjects' requests to exercise their rights under the GDPR, in line with the *Subject Rights Procedure*

Data Security

All staff are responsible for ensuring that:

- any personal data that they hold is kept securely
- personal information is not disclosed either orally or in writing or online or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be encrypted, or password protected. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Disaster Recovery

- The organisation backs up data every day and has multiple copies. Records of these backups are kept.
- Backups are kept off site and are monitored by our IT contractor, Runtech.
- Backups are verified regularly by software and system suppliers and Runtech.
- Firewalls and virus checkers are kept up to date and running at all times

Subject Consent

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the GDPR, the organisation takes a "granular" approach, i.e. it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, the organisation ensures that people can easily withdraw consent (and tells them how this can be done).

It should be noted, however, that consent is only one of the lawful bases under which processing personal data can be justified. In brief, the others include the following:

- Contract: if the processing is necessary to fulfil the organisation's contractual obligations to an individual
- Legal obligation: if the processing is necessary to comply with a common law or statutory obligation
- Vital interests: if the processing is necessary to protect an individual's life
- Legitimate interests: if the processing is conducted in a way that people would reasonably expect and that has a minimal privacy impact, or where there is a compelling justification for the processing
- Public task: 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

The organisation processes personal data in accordance with these lawful bases. The lawful basis used for each type of processing is detailed within the Privacy Notice.

Note that the GDPR provides for special protection for children's personal data and the organisation will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

Subject Rights

Individuals have the following rights under the GDPR:

- 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
- 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*.

The organisation will act upon the request within one month of receipt and if there is any reason for a delay, this will be communicated within the one-month time period. Requests that are manifestly unfounded or excessive may be refused. This will be communicated within the one-month time period and the individual will be informed of their right to contest this decision with the supervisory authority (the ICO). The organisation will not charge a fee for complying with requests unless the request is manifestly unfounded or excessive, or repetitive in nature.