Data Protection (GDPR) Policy

Prepared by	Authorised by	
Name: Peter Garcia	**Name:** Warwick Nash	
Date last reviewed:	**31/07/25**	
Effective from:	**01/08/25**	
Date of new review:	**31/07/26**	

Background

This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards and comply with the Data Protection Act 1998 and General Data Protection Regulation (GDPR) from May 2018

All Apprentify employees, temporary staff, consultants, contractors and third parties have a duty to protect Apprentify data that they create, store, process, or transfer.

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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.
- 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

In addition, Article 5 of the GDPR states that the controller (i.e. Apprentify) will be responsible for, and able to demonstrate compliance with these principles.

Key Definitions

Personal data means data which relates to living individuals who can be identified from that data, or from that data and other information, which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data relating to the data subject which includes information such as: racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexuality; information relating to commission of criminal offences.

Processing means obtaining, recording, or holding information or data or carrying out any operation or set of operations on that data.

Data subject means an individual who is the subject of personal data.

Data controller means a company or person who determines the purposes for which, and the way personal data is processed.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Purpose

The purpose of this document is to safeguard the personal information of learners, staff, and any other people for whom Apprentify collects or processes personal data and to make them aware of their rights under GDPR. In particular:

- To ensure data protection good practice across the organisation.
- To ensure compliance with GDPR and other applicable legislation and regulation related to personal data.

This document outlines internal policy in respect of data handling, but this policy is subject to all the laws, rules, and regulations that Apprentify is governed by. In the event this policy allows employees of Apprentify to exercise discretion, such discretion must be exercised within the confines of Apprentify statutory obligations and must not contravene any of its legal, accounting, or other regulatory requirements.

Scope

This policy applies to all Apprentify Group personnel irrespective of status, including temporary staff, contractors, consultants, and third parties.

Statement of Policy

- It is the policy of Apprentify to ensure that all data shall be protected in proportion to the sensitivity of the data, and in line with all legal and regulatory requirements.

- For the purposes of this document, we are a Data Processor and Data Collector. This means we are responsible for deciding how we hold and use personal information, and we also process data on behalf of Data Collectors that we subcontract from.
- This policy explains what personal data we hold, how we share it, how long we keep it and what legal rights a data subject (a living, identified or identifiable individual about whom we hold personal data) has in relation to it.
- Employees have an obligation to ensure they do not disclose or release sensitive personal information to any unauthorised person.

The Legal Basis of Collecting and Processing Data:

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever Apprentify processes personal data:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose. This must be freely given, fully understood, and the subject must "opt in" to consent. Consent will only be used as a lawful reason for processing if none of the other reasons applies
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). For Apprentify, these legal obligations would include safeguarding, meeting the requirements of the equality act, or meeting employees' rights. In particularly, much of the learner personal data we collect is legally required by our funding or regulatory bodies, i.e., ESFA, DfE.
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. As a training provider, our public task is to provide education and training, and any personal data necessary to achieve those ends will be lawful for this reason.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Procedure

Apprentify will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's (DPO) responsibilities:

- Responding to individuals such as clients and employees who wish to know which data is being held on them by Apprentify.
- Answering questions on data protection from staff, board members and other stakeholders.
- Keep the management team updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging relevant GDPR training for staff and other stakeholders.

Apprentify Group's DPO is Peter Garcia.

The categories of personal information that we may collect, store, and use about Apprentices in relation to the Apprenticeship Programme include:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Next of kin/accompanying staff and emergency contact information.
- Passport or other proof of identity details.
- Employment status and details.
- Previous qualifications and experience.
- Residency status in the UK.
- If a learner is a care leaver or has an Education & Health Care Plan.

We will also collect, store, and use the following "special categories" of more sensitive personal information, but are not limited to:

- Health information, including any medical condition or learning difficulty and disability status
- Information about your race, religion, nationality, ethnicity, sexual orientation, and criminal convictions
- Household situation

Special category data requires further conditions to lawfully process under Article 9 of the GDPR. The lawful reasons that Apprentify are most likely to use are:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. Apprentify has a lot of such obligations, including the equality act and employment law.
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent. However, this would only be used in very serious situations
- Processing is necessary for reasons of substantial public interest.

How Apprentify use information provided to us:

- We typically collect personal information about learners through the information provided to us during the application/enrolment process.
- We also collect information about parents/guardians where relevant. We collect information about parents/guardians from learners.
- We collect information about Employers during the application process.
- We may collect other additional personal information while organising and delivering the Programmes.

Information that we collect from others:

- The Learning Records Service (LRS). We use this service to check what prior qualifications you hold, to compare the qualifications on the LRS to those you declare on enrolment paperwork, as well as to confirm your Personal Learning Record (PLR) and add this information to your evidence pack.
- Your employer, to confirm your eligibility to enrol on to an Apprentify course and to check basic information including the spelling of your name, your employee number and the location and branch number of your workplace.
- Cognassist - We ask our learners to undertake a Cognassist assessment for the purposes of identifying any additional learning needs. This helps Apprentify to provide bespoke support for the individual learner to ensure they receive the best possible opportunity to complete their course. All learners receive a copy of the assessment results for future usage when engaging with educational programmes.

- The levy digital account, if you have joined us on an Apprenticeship course, to collect information from the Digital Apprenticeship Service account.
- Criminal Convictions – We will collect details of criminal convictions and carry out DBS checks for all staff and certain visitors, e.g., regular contractors, volunteers, governors, as required by law. Where Apprentify deems it necessary for the reasons mentioned, we will record and process that information as necessary.

When might personal data be used:

- Apprenticeship Matching Recruitment sifting
- Getting the Unique Learner Number from the Learner Records Service
- Enrolment Process in BUD
- ILR Submission to the ESFA
- Development Coach & key Teaching & Learning staff
- Change of Circumstance (New provider, redundancy, new employer, new line manager)
- End Point Assessment Organisation
- Certificate
- ESFA Satisfaction Surveys
- Auditors

Subject Rights

Under the GDPR, data subjects have the right to:

- Access and obtain a copy of their data on request
- Require Apprentify to change incorrect or incomplete data
- Prevent processing for the process of direct marketing, although we will continue to contact where necessary to provide learning – for example change of session that is going to be delivered and also if we need to contact you to obtain destination information as required by the Education Skills Funding Agency (ESFA).
- Require Apprentify to delete or stop processing your data, for example where the data is no longer necessary for the stated purposes of processing.
- Object to the processing of your data where Apprentify is relying on its legitimate interests as the legal group for processing. Apprentify will only use “legitimate interests” as grounds of processing in a very few situations.

Sensitive Personal Data

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g., to comply with legal obligations to ensure health and safety at work or safeguarding). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- Data should be regularly backed up.
- Data should never be saved directly to mobile devices such as laptops, tablets, or smartphones

Data Use

- When working with personal data, employees should ensure the screens of computers are locked when left unattended.
- Personal data should not be shared informally. It should never be sent by e-mail, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data retention

Apprentify staff must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Our contracts with the Education and Skills Funding Agency stipulate specific timeframes that data must be held for auditing purposes.

The categories of personal data we collect, store, and use in relation to prospective employees joining Apprentify include:

- Full name.
- Address.
- Contact numbers.
- Email address.
- Gender.
- Passport or other proof of identity details.
- Employment status and details.
- Previous qualifications and experience.
- Residency status in the UK.
- Electronic files will be encrypted and only employees with authorisation will have access.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Retained only for as long as necessary and for the purposes we have stated.
- Processed in an appropriate manner to maintain security.

Staff Training

All Apprentify staff will receive training on GDPR. All staff will receive training as part of our mandatory quarterly staff e-learning programme. Further training will be provided on an annual basis or whenever there is a substantial change in law or our policy and procedure.

Staff Personal Data

All staff must take reasonable steps to ensure that the personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data Breaches

Apprentify has a procedure designed to quickly identify if personal data has been compromised, its significance, who is affected, what actions are required, and whether the ICO needs to be informed.

The process will immediately escalate to Management level if appropriate. The process includes a log of any data breaches, actions required, and action taken. All breaches will be logged and reviewed.

ICO must be informed of details within 72 hours of Apprentify becoming aware of any non-minor breach of personal data.

ICO require information about the date and time or the breach, when it was detected, information about the type of breach and about the information concerned, the number of individuals affected, and the possible effect on them, measure taken to mitigate effects, and information about the notice to customers.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Employees should keep all data secure, by taking sensible precautions, such as using strong passwords and ensuring these are not shared.

- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the DPO if they are unsure about any aspect of data protection.

Review

This policy will be reviewed annually or earlier if deemed necessary.