



Data Protection and GDPR Policy

Change history		
Version	Issue Date	List of Amendments or remarks as applicable
1.	7 December 2021	1 st authorised version
2.	1 February 2022	Companywide policy review completed and new version issued
2.1	1 February 2023	Annual review, minor changes.
2.1	1 February 2024	Annual review, no changes.



APPRENTICESHIPS

Table of Contents

<i>Scope</i>	3
<i>Purpose</i>	3
<i>Review Period and Ownership</i>	3
<i>Promotion of Policy</i>	3
<i>Engagement and Training</i>	3
<i>Glossary</i>	4
<i>Our Commitment</i>	4
<i>Types of Data Held</i>	5
<i>Data Protection Principles</i>	6
<i>Procedures</i>	7
<i>Access to Data</i>	8
<i>Data Disclosures</i>	8
<i>Data security</i>	9
<i>International Data Transfers</i>	9
<i>Breach Notification</i>	10
<i>Data Protection Training</i>	10
<i>Data Protection Compliance</i>	10
<i>Policy Sign Off</i>	10



APPRENTICESHIPS

Scope

The Data Protection and GDPR Policy covers all LDN Apprenticeship employees. The terminology in this policy also refers to clients, potential clients, suppliers, competitors, website visitors, office visitors, job applicants, existing and former employees, apprentices, learners, volunteers, placement students and self-employed contractors. These are referred to in this policy as relevant individuals.

Purpose

The purpose of LDN Apprenticeships Data Protection and GDPR Policy is to comply with the law and to do what is reasonable to protect the personal data of relevant individuals.

This policy applies to the processing of personal data in manual and electronic records kept by LDN Apprenticeships in its day-to-day business. It also covers our response to any data breach and other rights under the General Data Protection (GDPR) Regulations.

Review Period and Ownership

The Data Protection and GDPR Policy will be reviewed annually and may be altered from time to time considering legislative changes or other prevailing circumstances. The Data Protection and GDPR Policy is owned by the COO.

Promotion of Policy

A shortened version of the policy is available as part of the Employee Handbook, which all staff are required to sign on joining. Updates to the handbook are completed annually, and staff are required to confirm that they have read the updates by signing.

Staff are required to complete training in relation to this policy / topic as part of their onboarding compliance training. Compliance training is refreshed by all staff annually.

Engagement and Training

This policy can be accessed by employees via the Company's Intranet. This policy is also referred to in the Employee Handbook which all staff have access to via the Company's intranet and are also required to read and sign. In addition, the Company sends a general notice through Slack, our communication platform for staff to read and sign the policy when required.

Staff will be issued with this Policy when there are any updates, or as part of refresher training.



APPRENTICESHIPS

Glossary

“Personal data” is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person’s name, identification number, location, online identifier. It can also include pseudonymised data.

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

“Criminal offence data” is data which relates to an individual’s criminal convictions and offences.

“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.

Our Commitment

We commit to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all our employees conduct themselves in line with this, and other related, policies.

We do not carry out profiling and/or automated decision-making using personal data.

Where third parties process data on our behalf, we will ensure that the third party takes such measures to maintain our commitment to protecting data. In line with GDPR, we understand that we are accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

As part of this commitment, we will protect the privacy of our employees, apprentices and learners. We will:

- Not sell information to outside entities.
- Not use data to target advertising.
- Use data for authorised purposes only.
- Not change or modify privacy policies without notice and opportunity to opt out.
- Maintain and enforce limits on data retention.

Our overriding principle is that we will only use personal data in a way that an individual would reasonably expect. For example, use client email addresses only to communicate



APPRENTICESHIPS

to them the service we provide, or obtain staff ID documents to prove right to work in the UK.

Types of Data Held

Personal data is kept in both paper and electronic files and/or within our software systems.

The following types of data may be held by us, as appropriate, on relevant individuals:

From Clients, Potential Clients and Suppliers:

- individual names, phone numbers, email addresses and social media accounts
- invoices, contracts, other documentation containing client / supplier information
- correspondence

From Job Applicants:

- personal information including nationality, normal CV information and application answers
- correspondence
- information about their current compensation package
- interview notes
- medial history
- referee responses
- psychometric test results

From Employees and Sub-Contractor Employees - same as from Job Applicants plus:

- proof of ID and right to work in the UK
- proof of address
- P45, NI number, tax code and other normal tax information
- bank account details
- emergency contacts
- normal HR records
- DBS checks
- correspondence
- emails sent and received
- timesheet data of hours worked as well as authorised and unauthorised absence

From Apprentices

- Personal Information
- Contact details



APPRENTICESHIPS

- Photograph
- Demographics
- Eligibility criteria
- Interview Information
- Performance Information
- Qualifications
- Disability / learning difficulty / mental health details
- Emergency contact details
- Apprenticeship progress information

From Competitors:

- individual names, phone numbers, email addresses and social media accounts
- correspondence

From Head Office Visitors:

- personal details
- details of any RIDDOR incidents

From Website Visitors:

- device and IP address information held in a cookie
- personal details entered into web forms

Please refer to the Company's Privacy Policy for more information on the reasons for our processing activities, the lawful bases we rely on for data processing, when we collect data and our data retention periods.

Data Protection Principles

All employees, apprentices and learners personal data obtained and held by us will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes it is collected and processed
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- 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
- comply with the relevant GDPR procedures for international transferring of personal data.



APPRENTICESHIPS

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

We have taken the following steps to protect the personal data of relevant individuals, which we hold or to which we have access:

- we provide information to our employees, apprentices and learners on their data protection rights, how we use personal data, and how we protect it. This information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
- we provide our employees, apprentices and learners with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially.
- we can account for all personal data we hold, where it comes from, who it is shared with and also who it might be shared with.
- we recognise the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining some types of personal data, and regularly review our procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. We understand that any consent must be freely given, specific, informed and unambiguous. We will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
- we have the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. We are aware of our duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and we are aware of the possible consequences of non-compliance.
- we are aware of the implications of the transfer of personal data internationally.
- we have written procedures for how we respond to any request of an individual to exercise their rights under GDPR.
- we have written a procedure for how to deal with a data breach.



APPRENTICESHIPS

Access to Data

Relevant individuals have a right to be informed whether we process personal data relating to them and to access the data that we hold about them. Requests for access to this data will be dealt with under the following summary guidelines:

- To make a subject access request an email must be sent to dataprotection@ldnapprenticeships.com
- We will not charge for the supply of data 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.
- We will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform us immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. We will take immediate steps to correct the information.

Data Disclosures

We may be required to disclose certain data to a 3rd party. The circumstances leading to such disclosures include:

- use of IT systems and software to run or day-to-day business (e.g. Slack, Office 365, MS Planner, BambooHR, SharePoint, Thinkific, MS Teams, Salesforce, Xero)
- at the request of relevant government agencies when required to do so (e.g. HMRC, The Home Office)
- when our professional service providers need the information to provide their services to us (e.g. lawyers, accountants, bank)
- when using 3rd party marketing providers (e.g. Google, Digital Marketing Agency)
- when using sub-contractors who deliver elements of our service
- where we have outsourced any various HR Services to an external provider
- where we require advice on a specific HR issue from an external provider (e.g. sharing health data when we are obtaining advice as to whether a disabled individual requires reasonable adjustments to be made to the working environment)
- sharing health data to comply with health and safety or occupational health obligations towards the employee

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



APPRENTICESHIPS

Data security

We adopt procedures to maintain the security of data when it is stored and transported.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- follow the guidelines for where regular documents are saved in the filing system to ensure the correct access rights are applied
- not email any personal data outside of the organisation unless absolutely necessary and in any instance only to approved 3rd Party Data Processors as defined in the Personal Data Register
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- ensure that all files, photos and scanned documents are deleted from local devices in line with the retention policy on the Personal Data Register
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not share passwords with people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Directors. Where personal data is held on any such device it should be protected by:

- devices are secured with appropriate passwords and encryption
- devices are maintained and managed by LDN with the ability to remotely lock or wipe them
- ensuring that it is held on such devices only where absolutely necessary
- ensuring that it is held in the correct location on the filing system (not on the desktop or in personal folders)
- ensuring that laptops or USB drives are not left lying around where they can be stolen
- deleting personal data from devices promptly after use

Failure to follow these rules on data security may lead to disciplinary action including dismissal with or without notice dependent on the severity of the failure.

International Data Transfers

The Company may be required to transfer personal data to other countries. This is because marketing, software and accreditation providers may operate outside of the



APPRENTICESHIPS

UK. Where this occurs, safeguards are adopted through the 3rd Party Data Processor Addendum to our agreement with the third parties.

Breach Notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the organisation becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, we will do so without undue delay.

Data Protection Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.


All employees who need to use our computer systems are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the organisation of any potential lapses and breaches.

Data Protection Compliance

Our Data Protection Officer/ Lead is Matthew Rogers, COO and can be contacted at dataprotection@ldnapprenticeships.com

Policy Sign Off

The current version of this policy has been signed off by the Chief Executive Officer.

Signature	
Name	Simon Bozzoli
Date	1 February 2024