Data Protection and Confidentiality Policy

Introduction

DRL Services Ltd ("DRL") is committed to protecting the privacy and security of all personal data it processes. This policy sets out how DRL collects, uses, stores, shares, and safeguards personal data in connection with its delivery of apprenticeship programmes to adults aged 18 and over. DRL fully endorses and adheres to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the Privacy and Electronic Communications Regulations (PECR). The Managing Director has overall accountability for data protection compliance within the organisation.

Scope

This policy applies to all staff, associates, subcontractors, and volunteers who process personal data on behalf of DRL, whether in an online or face-to-face context. It covers all personal data held in any format – electronic, paper, or otherwise – relating to apprentices, employers, staff, and other individuals with whom DRL has a relationship.

Related Policies and Documents

This policy should be read alongside the following DRL policies and external guidance; duplication is avoided and cross-references are used throughout:

- Safeguarding Policy – handling of sensitive data relating to the protection of vulnerable adults
- Equality, Diversity and Inclusion Policy – equalities monitoring data and protected characteristics
- Enrolment and Onboarding Policy – personal data collected at the point of application and during initial assessment
- DfE Apprenticeship Funding Rules 2025/26 – data requirements for funding claims and audit
- ICO Guide to UK GDPR (ico.org.uk)
- ICT Acceptable Use — formerly DRL/PP/032; provisions now incorporated within this policy.

Designated Person and Responsibilities

The Managing Director has specific responsibility for data protection in the organisation and acts as the Data Protection Officer (DPO) unless a separate DPO is appointed. Through appropriate management and strict application of criteria and controls, DRL will:

- meet its legal obligations to specify the purposes for which information is used
- take appropriate technical and organisational security measures to safeguard personal data
- ensure personal data is not transferred outside the UK without suitable safeguards
- ensure everyone handling personal data understands they are responsible for following good data protection practice
- ensure all staff handling personal data are appropriately trained and supervised
- regularly review and audit how personal data is managed
- ensure that anyone wishing to make enquiries about handling personal data knows what to do

Data Protection Principles

All personal data shall be:

- processed lawfully, fairly and transparently in relation to individuals
- collected for specified, explicit and legitimate purposes only, and not further processed in a manner incompatible with those purposes
- adequate, relevant and limited to what is necessary for the purposes for which it is processed
- accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure inaccurate data is erased or rectified without delay
- kept in a form that permits identification of individuals for no longer than is necessary for the purposes for which the data is processed
- processed in a manner that ensures appropriate security against unauthorised or unlawful processing, accidental loss, destruction or damage

Lawful Basis for Processing Personal Data

DRL will only process personal data on one of the following bases:

- Consent – the individual has given clear, freely-given consent for a specific purpose, with the ability to withdraw at any time
- Contract – processing is necessary to deliver or administer the apprenticeship programme
- Legal obligation – processing is required to comply with the law
- Vital interests – processing is necessary to protect someone's life or welfare
- Legitimate interests – processing is necessary for DRL's legitimate operational interests where these are not overridden by the individual's rights

Where processing is required for contractual or legal reasons, individuals are informed of this at the point of data collection.

Types of Personal Data Collected

In the course of administering apprenticeships, DRL may collect and process personal data including: names, contact details, job role, National Insurance number, prior attainment and qualifications, learning progress and assessment records, attendance and engagement data, employer details, and, where disclosed, health information, disability status, ethnicity, and other special category data. Special category data is only processed with explicit consent or where legally required.

DRL may receive personal data from employers, End-point Assessment Organisations, and the DfE or its successor body where this is necessary for the administration of the apprenticeship. Where DRL is provided with personal data about a third party (for example, next of kin), it is the responsibility of the disclosing party to ensure that person is aware and has consented.

How Personal Data is Used

Personal data is used to:

- fulfil contractual responsibilities to apprentices and employers
- administer and track apprenticeship progress and compliance
- carry out statistical analysis, quality assurance, and self-assessment

- meet DfE funding claim and audit requirements
- respond to requests from regulatory and awarding bodies as required by law or funding rules
- contact individuals about programme activities, quality assurance, and relevant updates

Data Sharing

DRL shares personal data only where there is a contractual obligation, legal requirement, or explicit consent. Data may be shared with: the DfE for funding and compliance purposes; EPAOs and awarding organisations for assessment administration; employers as part of the tripartite delivery model; and specialist services where a referral has been agreed with the apprentice. Personal data is not shared with third parties for marketing or commercial purposes without explicit consent. DRL takes all reasonable steps to ensure that partner organisations handle shared data in accordance with UK GDPR, including through the use of data sharing agreements where appropriate. Personal data will be shared with law enforcement or other authorities if required by law.

Data Retention

Personal data will be retained for the duration of any contract and for seven years following its conclusion or the completion of the apprenticeship, in line with funding rule requirements. After this period, data will be securely disposed of: paper records will be shredded and electronic records permanently deleted. Retention periods are reviewed as part of the annual data audit.

Data Subject Rights

DRL recognises all rights afforded under UK GDPR and will respond to all valid requests within one calendar month. Requests are accepted verbally or in writing and will be provided free of charge. A charge may be applied for requests that are manifestly unfounded or excessive. Individuals have the following rights:

- Right of access – the right to obtain a copy of personal data held
- Right to rectification – the right to have inaccurate or incomplete data corrected
- Right to erasure – the right to have data deleted where there is no overriding legal or contractual basis to retain it
- Right to object – the right to object to processing based on legitimate interests or for direct marketing
- Right to restrict processing – the right to limit further use of personal data while a dispute is resolved
- Right to data portability – the right to receive personal data in a structured, commonly used, machine-readable format

To exercise any of these rights, individuals should contact info@drlservices.co.uk with the subject line “Personal Data Request”. Responses will always be concise, transparent and written in plain language. Exceptions may apply where data must be retained for legal or regulatory reasons, and DRL will explain any such exceptions in its response.

Data Storage and Security

DRL’s primary delivery is online, and data is principally held on a cloud-based learner management system managed by DRL’s IT contractor. The following security measures are in place:

- systems are password-protected with strong passwords that are changed regularly and never shared
- electronic devices are locked when left unattended
- sensitive personal data is encrypted before being transferred electronically
- personal data is not shared informally or via unsecured email
- paper records, where used, are stored in locked drawers or cabinets and shredded securely when no longer required
- personal data is not saved to personal devices
- access to personal data is restricted to authorised personnel with a genuine business need
- all data is continuously backed up with full recovery processes tested regularly
- IT security is reviewed and risk-managed by DRL's IT contractor with ongoing monitoring of system security

Acceptable Use of ICT and Communications Systems

DRL's operations are primarily delivered online. All staff, associates, and subcontractors who use DRL's systems, equipment, or communications tools must do so in a manner consistent with UK GDPR and the Privacy and Electronic Communications Regulations (PECR).

Computer Equipment and Authorised Software

Only authorised personnel may access DRL's computer equipment and systems. Only software that has been approved by the Managing Director may be installed or used on DRL equipment. Software must be used for legitimate business purposes only. Unauthorised access to DRL systems, or the installation, copying, or removal of unauthorised software or equipment, may result in disciplinary action up to and including summary dismissal.

Internet Use

Access to the internet via DRL systems or equipment is permitted for legitimate business purposes. Staff are expected to use their judgement and act professionally at all times. The following are not permitted: accessing, downloading, or distributing offensive, inappropriate, or non-work-related material; accessing websites that introduce risk to DRL's systems through viruses or malware; attempting to bypass, disable, or compromise DRL's network or system security; and any activity that may constitute a criminal offence, including unauthorised access to third-party systems.

Where material is published in DRL's name, staff must ensure it is accurate, relevant to DRL's work, and does not infringe intellectual property or copyright. Where personal views are expressed in a public forum, a clear disclaimer must be included stating that the views are personal and not those of DRL.

Email Use

Email is to be used for legitimate business communication only. Messages should be directed only to those for whom they are relevant. Emails containing personal data or confidential information must be treated in accordance with the Data Storage and Security section of this policy and must not be sent via unsecured or personal email accounts.

DRL will not tolerate the use of email for any of the following: messages that could constitute bullying, harassment, or discrimination; personal or social correspondence unrelated to work; accessing or transmitting offensive material; transmitting copyright material without authorisation; or posting confidential information about staff, apprentices, or DRL's business. Offers, instructions, or commitments transmitted by email are as legally binding on DRL as those made in writing.

Staff should always consider whether email is the most appropriate channel before sending sensitive or contentious communications.

Electronic Monitoring

DRL reserves the right to monitor internet and email activity on its systems and equipment for the purposes of ensuring compliance with this policy and with applicable legislation. Such monitoring is carried out on the basis of DRL's legitimate interests in protecting its systems, data, and reputation, and is proportionate to that purpose. Staff will be informed of the nature of any monitoring at induction. Information obtained through monitoring may be used as evidence in disciplinary proceedings where a breach of policy is identified.

Social Media and Personal Data

No work-related content that could identify an apprentice, staff, employer, or other individual connected with DRL may be posted on any social networking site, whether during or outside working hours, and whether via DRL equipment or a personal device. This applies at all times and includes indirect identification — for example, describing a situation in a way that would allow a reasonable person to identify the individual concerned. Sharing such information without consent may constitute a breach of UK GDPR and could result in disciplinary action, termination of engagement, and referral to the Information Commissioner's Office.

Any professional content, contacts, or connections created during the course of your engagement with DRL on an authorised work account remain the property of DRL. On termination of your engagement, you must transfer access to any such accounts and associated content to DRL as directed.

Photography and Image Consent

Any photographs taken in the course of DRL's training or business activities, whether at face-to-face sessions or otherwise, must not be shared on social media or any public platform without explicit written consent from every identifiable individual appearing in the image. A two-stage check must be completed before any image is shared: the photographer must review the image for suitability, and the person uploading or publishing the image must confirm that written consent has been obtained and is on file. Images of apprentices are personal data for the purposes of UK GDPR. Consent must be freely given, specific, and recorded. It may be withdrawn at any time, in which case the image must be removed promptly from all channels.

Laptop and Mobile Device Security

All staff issued with a DRL laptop or mobile device are responsible for its safekeeping. Devices must not be left unattended in unsecured locations, must be locked when not in use, and must not be used by any person other than the authorised user. The loss or theft of any device must be reported to the Managing Director immediately, as it may constitute a personal data breach requiring notification to the ICO under the Data Breach Notification procedures set out below. On return of a device, staff must ensure all DRL data has been transferred to DRL's systems and that no personal copies of DRL data are retained. Where a device is not returned within the agreed period without a satisfactory explanation, DRL reserves the right to recover the cost of the device.

Data Breach Notification

DRL has procedures in place to detect, investigate, and respond to personal data breaches. In the event of a breach that poses a risk to individuals' rights and freedoms, DRL will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it, and will notify affected individuals without undue delay where there is a high risk to them. All actual or suspected

breaches must be reported immediately to the Managing Director. Breaches are recorded in a Data Breach Register, investigated, and used to improve controls and prevent recurrence.

Confidentiality

All staff and associates of DRL are required to maintain strict confidentiality in respect of all personal data and business information they access in the course of their work. Confidential information must not be disclosed to third parties without prior written consent, and must not be used for any purpose other than that for which it was obtained. This obligation continues beyond the end of any working relationship with DRL. All staff sign a confidentiality agreement as part of their induction. Confidential information includes, but is not limited to: learner data, employer information, financial and commercial data, DfE funding information, and any information belonging to DRL's partner organisations.

Compliance, Monitoring and Review

Compliance with this policy is monitored through annual staff training, management review, and periodic data audits. Regular evaluations and reviews of this policy will be undertaken to ensure it remains compliant with UK GDPR, the Data Protection Act 2018, DfE funding rules, and Ofsted requirements. This policy will be reviewed annually or sooner if there are significant changes in legislation, regulatory guidance, or operational practice.

Policy Owner:	DRL Services Ltd
Version:	V6
Date Approved:	20th May 2018
Signed By:	David Jamieson
Last Reviewed Date:	August 2025
Reviewed by:	David Jamieson
Next Review Date:	September 2026