Data Protection and Confidentiality Policy

Introduction

DRL Services are committed to its apprentices, employers and all customers we will ensure that all personal data will be lawfully stored we maintain confidentiality between ourselves and those we deal with. Within the business, DRL Services need to gather and use certain information about individuals we will not gather any information that is not needed. In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments for business data, for example. This personal information must be dealt with properly, however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material there are safeguards to ensure this as part of the Data Protection (Charges and Information) Regulations.

DRL ensures that our organisation treats personal information lawfully and correctly as shown within the Data Protection Act 2018. DRL fully endorses and adheres to the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

Scope

This policy applies to all staff, contractors, volunteers, suppliers and any individuals with access to the company's systems and information.

General guidelines

This policy explains how we collect personal data, the reasons for this and the legal basis for processing and how we handle and maintain the security of the personal data we process.
We recognise the importance of data security and take several measures to ensure the security of personal data. These include training all staff on data protection and use of an inhouse systems.
The Managing Director has specific responsibility for data protection in the organisation. 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 information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Have an appointed Data Protection Officer in place
- Ensure everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Ensure everyone managing and handling personal information are appropriately trained and appropriately supervised.

- Anybody wanting to make enquiries about handling personal information knows what to do.
- Methods of handling personal information are clearly described.
- A regular review and audit are made of the way personal information is managed.
- Performance with handling personal information is regularly assessed and evaluated.

Data protection principles

All 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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.
- recorded 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; personal data may be stored for longer periods as the personal data will be processed solely for archiving purposes, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- 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.

Lawful Basis for Processing Personal Data

DRL will only ever process personal data for one of the following reasons.

- Consent – you have given clear consent for DRL to process your personal data for a specific purpose.
- Contract – the processing is necessary for a contract DRL has with an individual, or because specific steps were requested before entering a contract.
- Legal obligation - the processing is necessary for DRL to comply with the law (not including contractual obligations)

- Vital interests - processing is necessary to protect someone's life.
- Legitimate interests - the processing is necessary for DRL's 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.

If the lawful basis for processing your personal data is through *consent*, we will clearly explain why we want any data, what we will do with it, and give you the ability to withdraw consent at any time.

When we ask you to supply us with personal data, we will make it clear whether the personal data we are asking for must be supplied so that we can provide the products and services to you, or whether the supply of any personal data we ask for is optional.

Collecting Personal Data

DRL will explain clearly why we are collecting personal data and how we intend to use it. We may collect and process personal data such as your name, e-mail address, postal address, telephone number and job role.

We may collect and process the information you provide to us if you:

- correspond with us by phone, e-mail, or in writing.
- complete a form on our website
- report a problem
- sign up to receive our communications
- enter a contract with us to receive products and/or services
- complete any paperwork that captures data for purpose of training.

We may also receive information from other sources, such as if you are a tutor, apprentice, or apprentice, we may also receive information about you from your centre, training provider, or employer when they register to receive products and/or services from us.

If you provide information to us about any person other than yourself, such as your relatives, next of kin, your advisers or your suppliers, you must ensure that they understand how their information will be used, and that they have given their permission for you to disclose it to us and for you to allow us, and our partner companies, to use it.

Sensitive Data

In certain cases, we may collect sensitive personal data from you (for example information about your physical or mental health, racial or ethnic origin, political opinions, religious beliefs, trade union activities, or details of criminal offences). However, we will only do so based on your explicit consent.

How We Use Your Personal Data

DRL and its associates may use or otherwise process personal data and sensitive personal data, so DRL can**:**

- fulfil our contractual responsibilities to apprentices and awarding bodies.
- contact apprentices directly by email or post about DRL activities, quality assurance activities, and/or to inform them of products or services that DRL and/or selected third parties offer.
- carry out statistical analysis – either ourselves or by third parties on our behalf
- give regulatory and industry bodies appropriate personal data or sensitive personal data about apprentices where there is a contractual or legal requirement – specifically to:
  - ensure they can monitor equal opportunities in ethnicity and disability
  - account for apprentices where there is a requirement to do so
  - allow them to meet the requirement to contact an apprentice directly, when the information is not readily accessible from another source
  - pass apprentices' personal data to regulatory and industry bodies or other selected third parties, solely for the purpose of providing prizes, remuneration and awards for apprentices.

As a routine business activity, DRL will maintain data and ensure that changes or corrections to any personal data or sensitive personal data previously supplied will be undertaken quickly.

Who We Share Your Personal Data With?

We may share your personal data with partner companies we work with but only where consent is expressly sought and given, or a legitimate business interest exists.

We take all reasonable steps to ensure that our staff protect your personal data and are aware of security obligations. We limit access to your personal data to those who have a genuine business need to know it.

We will share personal data with law enforcement or other authorities if required by law.

How long will we keep your personal data?

Where there is a contract between us, we will retain your personal data for the duration of the contract, and for a period of seven years following its termination or expiry.

Your Rights

DRL will accept a request for information verbally or in writing, and this will be provided free of charge. However, if a request is excessive or repetitive, we will charge an admin fee. The information DRL supply about the processing of personal data will always meet the following criteria and be:

- concise, transparent, intelligible and easily accessible.
- written in clear and plain language, particularly if addressed to a child.

If you would like to make a request regarding your personal data, please contact us on info@drlservices.co.uk with the headline – "personal data request".

Right to Access

You have the right to request a copy of the personal data that we hold about you. We will respond within 30 days of your request. There are exceptions to this right. For example, we may be unable to make all information available to you if making the information available would reveal personal data about another person if we are legally prevented from disclosing such information.

Right to rectification

We aim to keep your personal data accurate and complete. We encourage you to contact us to let us know if any of your personal data is not accurate or changes, so that we can keep your personal data up to date.

Right to erasure

You have the right to request your personal data be completed and permanently deleted from DRL's systems. This may be when the personal data is no longer necessary for the purposes for which they were collected, where you withdraw your consent to processing, where there is no overriding legitimate interest for us to continue to process your personal data, or your personal data has been unlawfully processed.

Right to object

You have the right to object to the processing of your personal data where, for example, your personal data is being processed on the basis of legitimate interests and there is no overriding legitimate interest for us to continue to process your personal data, or if your data is being processed for direct marketing purposes.

.

Right to restrict processing

You have the right to request that we restrict the further processing of your personal data. If you contest the accuracy of the personal data, we hold about you and we are verifying the information, you have objected to processing based on legitimate interests and we are considering whether there are any overriding legitimate interests, or the processing is unlawful, and you elect that processing is restricted rather than deleted.

Right to data portability

You may have the right to request that some of your personal data is provided to you, or to another data controller, in a commonly used, machine-readable format. If you would like to request that your personal data is ported to you,

Please note that the GDPR sets out exceptions to these rights. If we are unable to comply with your request due to an exception, we will explain this to you in our response.

Data Storage

- When not required, paper/files will be kept in a locked drawer or filing cabinet.
- All staff will ensure paper and printouts are not left where unauthorised people could see them – for example, on a printer or desk.
- Data printouts will be shredded and disposed of securely when no longer required.
- All staff computers are password protected.
- Electronic data should be protected by strong passwords that are changed regularly and never shared between any unauthorised personnel.
- Personal data should not be disclosed to unauthorised individuals.
- Data should never be saved directly onto personal laptops or any other mobile devices such as tablets or smart phones
- All files and personal data electronic and paper are stored correctly and within a locked office when not maned, the office has an entry alarm that is only known by management.

Our IT systems are essential to apprenticeship delivery and the administration of apprenticeship delivery, all data is stored on our cloud-based system. DRL use an IT contractor to manage our systems and ensure all security is of high importance and risk managed. In the event of any incident our IT team will be able to secure and back up all company data. There are processes in place for ongoing monitoring and management of any risks to our systems.

We will manage these risks ensuring the backup and restoration of the system to ensure

- Full database and system replication
- Regular testing to ensure systems can always be accessed when needed to from other training sites securely
- All data is continuously backed up
- Full security systems are always in place

Data Use

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Sensitive personal data must be encrypted before being transferred electronically.
- Copies of personal data should not be saved directly onto any computer. Always access and update the central copy of any data.
- Personal data should not be shared informally. In particular, it should never be sent by email unless the data is encrypted, as this form of communication is not secure.

Fair Processing Information

All personal data obtained and processed by DRL will be utilised for the purposes of maintaining employees' personal details during their employment with DRL. At all times, this data will be processed only by authorised company personnel and will be stored and treated with the utmost security and confidentiality.

Confidentiality

DRL Services Ltd to provide its customers with a high-quality service and to meet contractual specifications and requirements.

Any confidential information of the Company which may include the following -

- any information obtained by you in the course of your employment which is manifestly confidential.
- Any equipment, intellectual property or materials that are owned, licensed, or used by the Company.
- the financial dealing of the company or identities of customers, suppliers, contractors, licensors, or licensees of the Company.
- the business dealings or affairs of the Company.

You shall not during your employment by the Company or after the termination of your employment without the prior written consent of the Company use for your own purposes, or divulge to any third party, or otherwise make use of any Confidential Information of which you shall become possessed, relating in any way to the business of the Company or its techniques, systems or know-how.

You shall, during your employment by the Company, use your best endeavours to prevent the publication or disclosure of any Confidential Information.

You shall refrain from using and shall keep secret during and after the termination of your employment with the Company any secret or confidential information relating in any way to any business or individual having dealings with the Company.

Any person employed or associated with the company will ensure that all confidential information belonging to the ESFA is treated with a high level of confidentiality and safeguard any information in relation to its purpose. Any person employed or associated with the company will complete and sign a confidentiality agreement this will reinforce that all persons will not disclose any confidential information to any third party unless written consent is granted by the ESFA.

Except to the extent necessary in the proper course of your employment or as required by law, you shall not at any time during or after your employment by the Company reproduce in any form or on any media or device or permit anyone to reproduce any Confidential Information.

You shall not except to the extent necessary in the proper course of your employment or as required by law:

- *Remove any computer disks/memory sticks, tapes or Materials containing any Confidential Information from the Company's premises; or*
- *Send by electronic means any Confidential Information to any third party.*

Confidential Information which is made or received by you during your employment by the Company and all disks/memory sticks, tapes and Materials and any copies containing any Confidential Information shall be the property of the Company.

You shall abide by all directions of the Company from time to time and the Company's standard operating practices concerning the use, disclosure and supply of Confidential Information.

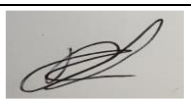
You shall not without the prior authority of the Company make any announcement, publicity or statement about the Company.

On or before termination of your employment by the Company (howsoever occasioned), you shall deliver up to the Company or, at the Company's option, destroy or delete: all disks/memory sticks, tapes, Materials and tangible items and all copies containing any Confidential Information, and all other documents and property of the Company (including but not limited to access cards, security passes and keys), in your possession or under your control.

The rights and obligations under this clause shall continue in force after termination of this Agreement and shall be binding upon your representatives.

Compliance

Regular evaluations and reviews of this policy will be undertaken to ensure compliance of the Act throughout DRL.

Policy Record Details	
Policy Owner	DRL Services Ltd
Version	V2
Approved Date	20th May 2018
Signed By	David Jamieson 
Last Reviewed Date	18th May 2023
Next annual review date	17th May 2024