DATA PROTECTION & PRIVACY POLICY

Policy Statement

DCS Logistics Services Ltd is committed to:

- A policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.
- The new regulatory environment demands higher transparency and accountability in how Centre's manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.
- The GDPR contains provisions that we will need to be aware of as data controllers, including provisions intended to enhance the protection of student's personal data. For example, the GDPR requires that we must ensure that our Centre's privacy notices are written in a clear, plain way that staff and students will understand.

DCS Logistics Services Ltd need to process certain information about its staff, learners, parents / guardians and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of programmers of study and courses.
3. Student enrolment.
4. Examinations and external accreditation.
5. Recording student progress, attendance and conduct.
6. Collecting fees.
7. Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) we must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff and learners of DCS Logistics Services Ltd. Any breach of this policy or of the Regulation itself will be considered an offence and the Centre's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with us and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy. The sign off sheet at the end of this document will be obtained and stored for each member of staff in their staff folder.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

This piece of legislation came into force on the 25th May 2018. The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

The GDPR also sets out specific rights for College's / Centre's learners in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Pupil Information) (England) Regulations 2000'. For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

Responsibilities under the GDPR

Everyone who works for or with DCS Logistics Services Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
The Management Team is ultimately responsible for ensuring that DCS Logistics Services Ltd meets its legal obligations
The Data Protection Manager is Dilly Sing
The Data Protection Officer is Sunny Singh

- Compliance with the legislation is the personal responsibility of all members of the Centre who process personal information.
- Individuals who provide personal data to the Centre are responsible for ensuring that the information is accurate and up-to-date.
- How we will use your data and who will have access to it. ***Please refer to the flow chart on page 10 of this document.***

Data Protection Register

DCS Logistics Services Ltd is registered with the Data Protection Register ZA168280 and will renew their registration annually as per the expiry date on the register entry.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles.

In order to comply with its obligations, we undertake to adhere to the eight principles:

1. **Process personal data fairly and lawfully.**
   We will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; are given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. **Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.**
   We will ensure that the reason for which we collected the data originally is the only purpose for which we will process the data, unless the individual is informed of any additional processing before it takes place.

3. **Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.**
   We will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data is given by individuals, this will be destroyed immediately.

4. **Keep personal data accurate and, where necessary, up to date.**
   We will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify us if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Centre to ensure that any notification regarding the change is noted and acted on.

5. **Only keep personal data for as long as is necessary.**
   We undertake not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means we will undertake a regular review of the information held and implement a weeding process.

   We will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6. **Process personal data in accordance with the rights of the data subject under the legislation.**
   Individuals have various rights under the legislation including a right to:
   - be told the nature of the information the Centre holds and any parties to whom this may be disclosed.
   - prevent processing likely to cause damage or distress.
   - prevent processing for purposes of direct marketing.
   - be informed about the mechanics of any automated decision making process that will significantly affect them.
   - not have significant decisions that will affect them taken solely by automated process.
   - sue for compensation if they suffer damage by any contravention of the legislation.
   - take action to rectify, block, erase or destroy inaccurate data.
   - request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

   We will only process personal data in accordance with individuals' rights.

7. **Put appropriate technical and organizational measures in place against unauthorized or unlawful processing of personal data, and against accidental loss or destruction of data.**

   All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

   We will ensure that all personal data is accessible only to those who have a valid reason for using it.

   We will have in place appropriate security measures e.g.
   ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- Keeping all personal data in a lockable cabinet with key-controlledaccess.
- Password protecting personal data held electronically.
- Archiving personal data which is then retained securely (lockablecabinet).
- Placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorized staff.
- Ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, we will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and learners who process personal data 'off-site', e.g. when working at home, and in such circumstances additional care must be taken regarding the security of the data.

8. **Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

   We will not transfer data to such territories without the explicit consent of the individual.

   This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so we will always seek the consent of individuals before placing any personal data (including photographs) on its website.

   If the Centre collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Consent as a basis for processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when we are processing any sensitive data, as defined by the legislation.

DCS Logistics Services Ltd understand consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form / Funding Evidence Pack) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication. Any data collection documents will contain the following fair collection statement.

"Personal Details - For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to the Centre holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in the Centre's data protection policy. This will include marketing images and the Centre's CCTV."

We will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

How We Use Your Personal Information
This privacy notice is issued by the Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the Department of Education (DfE). It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organizations. For the purposes of the Data Protection Act 1998, the DfE is the data controller for personal data processed by the ESFA. Your personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a personal learning record (PLR).

Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 1998.

The European Social Fund (ESF) Managing Authority (or agents acting on its behalf) may contact you in order for them to carry out research and evaluation to inform the effectiveness of training.

You can opt in for contact for other purposes by ticking any of the following boxes;

- ☐ *About courses or learning opportunities. For surveys and research.*
- ☐ *By post. By phone. By email.*
- ☐ *Further information about use of and access to your personal data, and details of organizations with whom we regularly share data are available at: https://www.gov.uk/government/publications/esfa- privacy-notice*

We will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the Centre. Any individual wishing to exercise this right should apply in writing to the Centre Manager. Any member of staff receiving a SAR should forward this to the Centre Manager.

The Centre reserves the right to charge a fee for data subject access requests (currently £20).

Under the terms of the legislation, any such requests will be complied with within 40 days.

Disclosure of Data

Only disclosures which have been notified under the Centre's Data Protection policy notification must be made and therefore staff and students should exercise caution when asked to disclose personal data held on another individual or third party. *Please refer to the flow chart on page 10 as to who will be given access to data by the Centre.*

DCS Logistics Services Ltd undertakes not to disclose personal data to unauthorized third parties, including family members, friends, goverment bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- The individual has given their consent to the disclosure.
- The disclosure has been notified to the Centre Manager and is in the legitimate interests of the Centre.
- The disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual.
For detailed guidance on disclosures see the Code of Practice (CoP).
In no circumstances will we sell any of our databases to a third party.

Data Breach

Please refer to our Continuity Policy / Disaster Plan on how we will deal with any breaches in data security. Should any breaches in our security result in a Data Breach, we will;

- Our Data Protection Manager will contact the persons that are affected by the Data Breach
- Provide details of the data that has been breached and what information has been taken, this should include;
    - the date, or date range, of the unauthorized access or disclosure,
    - the date we detected the data breach, the circumstances of the data breach (such as any known causes for the unauthorized access or disclosure),
    - who has obtained or is likely to have obtained access to the information
- Relevant information relating to what steps we will take to contain and remedy the breach and what steps that we recommend the affected person(s) take

Publication of Centre Information

Floortrain (GB) Ltd publishes various items which will include some personal data, e.g.

- Internal telephone directory.
- Event information.
- Photos and information in marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential or restricted to Centre access only. Therefore, it is our policy to offer an opportunity to opt-in for the publication of such when collecting the information.

Email
It is our policy of to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the Centre's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the Centre may be accessed by someone other than the recipient for system management and security purposes. We will use Encryption 256-Bit AES (Advanced Encryption Standard) for all out going emails containing personal data.
The following statement will appear in all email signature blocks;

CCTV
There are some CCTV systems operating within Centre for the purpose of protecting our members and property. We will only process personal data obtained by the CCTV system in a manner which ensures compliance with thelegislation.

Learners, Employers and Staff

The process of sharing of data that does not comply with the requirements of this policy will be treated as a serious breach of confidentiality and will be investigated and dealt with accordingly.

Examples of inappropriate data sharing could include:

- Giving away learner's details to someone without authorization.
- Using social Media – This also relates to images of learners whereby permission must be granted.
- Emails containing data of learners or employers.
- Keeping employer/learner addresses/details on file without a valid reason.
- Giving delivery information to a delivery company without prior permission.

Rules state that you must make sure the information is kept secure, accurate and up to date. For example, when you collect someone's personal data you must tell them:

- Who you are
- How you'll use their personal information
- They have the right to see the information and correct it, if it's wrong

We will also say if the information will be used in other ways – e.g. if it may be passed to other organizations. E.g. we are constantly discussing learner profiles with our funding providers via the phone and email. Staff's are also in touch with learners via phone/email contact on a regular basis and need to ensure these contact details are only given to staff or authorized persons.

Recruitment and Managing Staff Records

- Recruiting staff – The job advertisement must show the company's business name and contact details. Only relevant personal information can be collected when recruiting staff via applications E.g. you cannot ask for bank details on an application. Information gained for recruitment must only be kept and used for as long as necessary and for the intended purpose– e.g. do not use it for a marketing mailing list.

- Managing staff records – This information should only be kept as long as it benefits the business; after this it should be shredded. Records should be password protected or locked in a folder. Staff have the right to request information you hold about them unless it concerns someone else E.g. A harassment claim directed at them.
- Marketing products/services and the use of social media
- Using CCTV
- Recording staff working hours.

Monitoring Staff

We must be able to justify monitoring staff at work, which could include:

- Keeping records of phone calls
- Logging their email or internet use
- Searching staff or their work areas

Employees have rights at work and we will treat them fairly. We will make them aware that they're being monitored, and why – e.g. by sending them an email. We will also explain our policies on things such as using work computers or phones for personal use. Once we have informed them it is up to them to follow the rules set.

The only way in which we can monitor staff without them knowing is if:

- we suspect they're breaking the law
- letting them know about it would make it hard to detect the crime

We will only do this as part of a specific investigation and stop when the investigation is over.

Employee Information

Employees' personal data will be kept safe, secure and up to date by an employer.

Data we will / can keep about an employee includes:

- name
- address
- date of birth
- sex
- education and qualifications
- work experience
- National Insurance number
- tax code
- details of any known disability
- emergency contact details

We will also keep details about an employee such as:

- employment history with the organization
- employment terms and conditions (e.g. pay, hours of work, holidays, benefits, absence)
- any accidents connected with work
- any training taken
- any disciplinary action

What an Employer Should Tell an Employee

An employee has a right to be told:

- what records are kept and how they're used
- the confidentiality of the records
- how these records can help with their training and development at work

If an employee asks to find out what data is kept about them, we will have 40 days to provide a copy of the information. We will not keep data any longer than is necessary and will follow the rules on data protection.

Further Resource

- Register of Shredding / Disposal located as a separate TAB within the Company Quality Assurance System CQAS.
- Data Request form

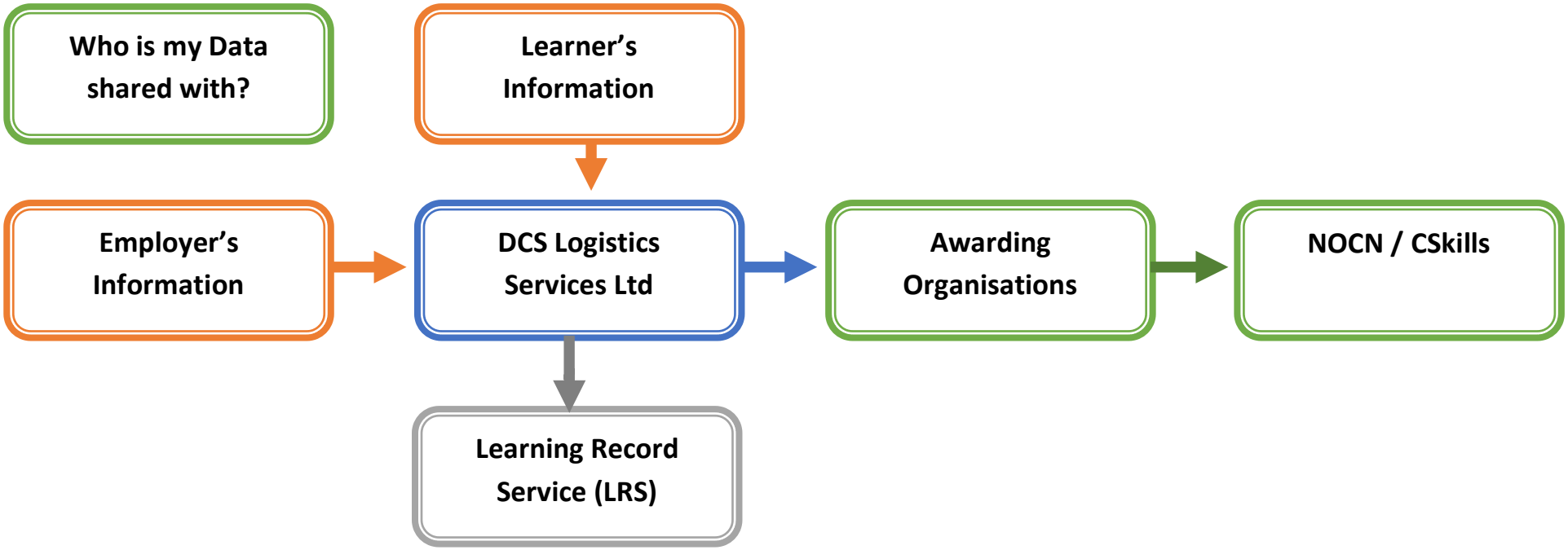
REVIEW

The EU General Data Protection Regulation (GDPR) was adopted in April 2016 and will take effect across the European Union (EU) on 25 May 2018, when it supersedes the 28 current national data protection laws based on the 1995 Data Protection Directive (DPD).

As such, this policy will undertake a full review within 6 months of its introduction.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact:

The Data Protection Manager – Dilly Singh
The Data Protection Officer – Sunny Singh


Who is my Data shared with?
Learner's Information
Employer's Information
DCS Logistics Services Ltd
Awarding Organisations
NOCN / CSkills
Learning Record Service (LRS)

Data Protection & Privacy Policy Staff Acceptance and Sign off

Please complete the details below and return this page via email to dilly@dsclogisticservices.co.uk/

I, being the person detailed below, have read and understood the policy and agree to abide by its contents. Furthermore, I give my consent to use this data for the manner in which it was intended and understand that my data will not be passed to any third parties not connected with the Centre activities.

Name	
Signature	
Date	

Personal Data Requests Form

Your Details

Title	First Name	Last Name	Position	Your Organisation

Your Address

House name / Number	Street	Town / City	Post Code

Contact Details

Telephone Number	Mobile Number	Email Address

Your Request

If you have already been in contact with a member of staff, please provide staff details and the nature of your enquiry below.				
Is this your first official request for data	**No ☐ Yes ☐**	***If the answer is yes, please provide details below.***		
Please provide details of the data that you require, provide as much detail as you can				
How would you like to receive the data?				
Spreadsheet ☐	Text File ☐	Video / Audio ☐	Word Document ☐	PDF File ☐

Upon completion, please return this form via email to dilly@dsclogisticservices.co.uk/or by post to: 47 New House Lane, Gravesend, Kent, England, DA11 7LP for the attention of Dilly Singh.

As per our GDPR policy, we will reply to your request within 40 days of receipt of this request.