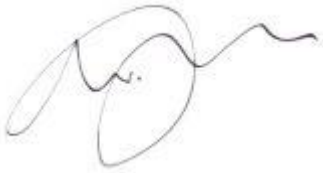
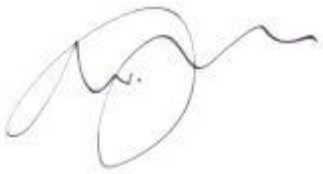
Data Protection Policy

Version Control:

Date created	Created by	Next Review date
February 2018	Liz Moran	August 2022

Version Number & Date of amendment	Summary of amendments	Quality Board Member Approval Name	Signature	Date approved
3	Updated to include Learners	Mike Monaghan		12/01/21
4	Change of DPO and Company Address	Mike Monaghan		19/08/21

System Group collects and uses personal information about staff, learners and other individuals who come into contact with System Group. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the System Group complies with its statutory obligations.

System Group is a data controller and processor and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. System Group must be able to demonstrate compliance. Failure to comply with the Principles exposes System Group and staff to civil and criminal claims and possible financial penalties.

Details of System Group's purpose for holding and processing data can be viewed on the data protection register: https://ico.org.uk/ESDWebPages/Entry/Z5761085

System Group's registration number is Z5761085. This registration is renewed annually and updated as and when necessary.

Aim and scope of policy

This policy applies to the processing of personal data in manual and electronic records kept by the Company. It covers the Company employee and learner data policies, including Company's response to any data breaches, focusing on rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors, and learners. These are referred to in this policy as relevant individuals.

"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, and 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.

The Company makes a commitment 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. Also, all Company employees will conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the Company, the Company will ensure that the third party takes such measures in order to maintain the Company's commitment to protecting data. In line with current data protection legislation, the Company understands that it will be 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.

Types of data held

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

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

Relevant individuals should refer to the Company's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles

All personal data obtained and held by the Company 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 of processing
- 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 data protection procedures for international transferring of personal data.

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.

Company procedures

The Company has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.

  There are clear lines of responsibility and accountability for these different roles.

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees 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
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Company
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Company understands that consent must be freely given, specific, informed and unambiguous. The Company 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
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences
- it is aware of the implications international transfer of personal data internationally.

Access to employee data

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

- a form on which to make a subject access request is available from HR. The request should be made to the HR Manager.
- the Company 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
- the Company will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

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

Data disclosures relating to Company employees

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

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

Data security rules for Company employees

The Company adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the Data Transfer Security Policy, Appendix A.

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
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- refrain from sending emails containing sensitive work related information to their personal email address
- check regularly on the accuracy of data being entered into computers

- always use the passwords provided to access the computer system and not abuse them by passing them on to 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 Data Protection Officer. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

New Company 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.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR data record. These records will be kept up to date so that they reflect current processing activities.

International data transfers

The Company does not transfer personal data to any recipients outside of the EEA.

Security incidents and data breaches

A data breach is when unauthorised access to data or distribution of data has occurred.

We investigate all potential data breaches - by reporting and investigating all perceived data breaches quickly, steps can be taken to confirm, secure the data, and prevent the incident becoming an actual breach. Company staff are instructed to report potential breaches immediately.

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 Company becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that 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, the Company will do so without undue delay.

Data Protection Officer

The Company's Data Protection Officer is Mike Monaghan, Head of IT & Systems. Mike can be contacted at dpo@system-group.com

Overall data protection responsibility resides with the CEO, Paul Hudson.

Appendix A
Data Transfer Security Policy

The Company stores a large volume of information electronically. This policy governs the procedures to protect this information and sets out how data should be transferred around the Company, and outside the Company, in a secure and protected way.

The law
Data storage is regulated by the General Data Protection Regulation (GDPR) and current domestic legislation. Standards are set out in the Regulation and the current Data Protection Act and one of the key points for consideration in a data transfer situation is that personal data must not be transferred to a country/territory outside the European Economic Area (EEA) unless that country/territory ensures appropriate safeguards.

Sensitive data
Sensitive data, for the purpose of this policy, includes data which contains:

- personal details about an individual (including those which are classed as special categories of data including data relating to health and race etc)
- confidential data about the Company
- confidential data about goods, products or services
- confidential data about Company customers and suppliers.

If employees have any doubt as to whether data is or is not 'sensitive data', the employees must refer the matter to the department manager.

Data transfers
Employees must seek consent from their department manager to authorise the transfer of sensitive data.

Data (sensitive or not) should only be transferred where it is strictly necessary for the effective running of the Company. Accordingly, before any data transfers are requested, the necessity of the transfer should be considered in advance.

After authorisation has been granted, the data must be referred to the Company IT department so that it can be encrypted, compressed and password protected before it is sent.

Data transfers by post/courier

Data transfers which occur via physical media such as memory cards or CDs must only be dispatched via secure post. The use of first or second class Royal Mail is not permitted; only special delivery or recorded delivery should be used. For non-Royal Mail services, a secure courier service must be used with a signature obtained upon delivery.

The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.

The recipient should be advised in advance that the data is being sent so that they are aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The employee responsible for sending the data is responsible for confirming the data has arrived safely.

Lost or missing data
If an employee discovers that data has been lost or is missing, the employee is required to inform the department head immediately.

The Company's breach notification policy will be followed. An investigation will be initiated immediately to establish the events leading to the data loss/theft and to determine whether a breach of personal data has occurred. If it has, a determination will be made as to whether the breach is notifiable under that policy.

The head of department must consider referring a matter to the police if it is found that unauthorised individuals have accessed sensitive data. Data which is held in the correct encrypted, compressed and/or password protected formats, which has been accessed by an unauthorised individual, has been accessed unlawfully.

Negligent data transfers
Employees who fail to comply with the requirements of this policy are likely to have their actions considered as gross misconduct, which may result in summary dismissal. Personal data breaches may result in exceptionally large fines for the Company.

Employees must not be negligent when transferring sensitive data. Examples of negligence include failing to obtain authorisation from the department manager, failing to ensure the Company IT department encrypted, compressed and password-protected data, or using non-secure post services which are not tracked or insured

Appendix B

Privacy Notice

The Company is aware of its obligations under the General Data Protection Regulation (GDPR) and domestic data protection legislation and is committed to processing Company employee and learner data securely and transparently. This privacy notice sets out, in line with current data protection obligations, the types of data that we hold on you as an employee of the Company. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

This notice applies to current and former employees and workers, and learners.

Data controller details

The Company is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows: System Group, Business Unit 6, Liverpool International Park, DeHavilland Drive, Speke, Liverpool L24 8RN.

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the duration of your employment or learning
- only collect data that is needed
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

Types of data we process

We may hold many types of data about you, for the purpose of delivering training, and/or managing the business and its legal obligations, potentially including:

For learners and Company employees:

- your personal details including your name, address, date of birth, email address, phone numbers
- your photograph
- gender
- marital status
- dependants, next of kin and their contact numbers
- medical or health information including whether or not you have a disability
- information used for equal opportunities monitoring about your sexual orientation, religion or belief and ethnic origin
- information included on your CV including references, education history and employment

history

- documentation relating to your right to work in the UK
- other learner information relating to your enrolments and learning programmes, such as courses, attendance, start and end dates of study, learning progress, submitted work and assignments (which may include audio and video content), and exam results
- National Insurance number

For Company employees we may also hold:

- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment/engagement with us
- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings or, in the case of workers, confirmation of other discussions about your conduct
- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms or, in the case of workers, confirmation of other discussions about your performance
- driving licence
- bank details
- tax codes
- leave records including annual leave, family leave, sickness absence etc
- details of your criminal record
- training details
- CCTV footage

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment or enrolment exercise, where we typically will collect the data from you directly. Further information will be collected directly from you when you complete forms at the start of your employment/engagement or training, and during your employment/training. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, employers, and former employers.

Personal data is kept in within the Company's secure IT systems.

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

in order to perform the employment contract that we are party to

- in order to deliver and manage your enrolment and training courses (such as apprenticeship programmes and AEB training)
- in order to carry out legally required duties

- in order for us to carry out our legitimate interests
- to protect your interests and
- where something is done in the public interest
- where we have obtained your consent.

All of the processing carried out by us falls into one of the permitted reasons.

We also need to collect your data to ensure we are complying with legal requirements such as:

- carrying out checks in relation to your right to work in the UK
- making reasonable adjustments for disabled individuals
- and for Company employees ensuring tax and National Insurance is paid

We also collect data so that we can carry out activities which are in the legitimate interests of the Company, for example

- making decisions about who to offer initial employment/engagement to, and subsequent internal appointments, promotions etc
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- if you are an employee, effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- if you are an employee, offering a method of recourse for you against decisions made about you via a grievance procedure
- assessing training needs
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- gaining expert medical opinion when making decisions about your fitness for work
- managing statutory leave and pay systems such as maternity leave and pay etc
- business planning and restructuring exercises
- dealing with legal claims made against us
- preventing fraud
- ensuring our administrative and IT systems are secure and robust against unauthorised access

Special categories of data

Special categories of data are data relating to your:

- health
- nationality
- ethnic origin

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring
- in our sickness absence management procedures
- to determine reasonable adjustments

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data for Company staff only

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data as part of Disclosure & Baring Service (DBS) checks.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract with us. If you do not provide us with the data needed to do this, we will be unable to perform those duties. We may also be prevented from confirming, or continuing with, your employment/ engagement or training programme with us in relation to our legal obligations if you do not provide us with this information.

Sharing your data

Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties. We share your data with third parties as reasonably necessary to fulfil our obligations for the purposes as set out in this privacy statement. For Company employees, we may obtain references as part of the recruitment process and any third parties which process data on your behalf.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

Except as provided in this privacy statement, we will not provide your information to third parties without your prior consent.

We do not share your data with bodies outside of the European Economic Area.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such. Please see the Appendix A, Data Transfer Policy.

Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with current data protection requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

Data retention - How long we keep your data for

We take information security extremely seriously. We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

In line with data protection principles, we only keep your data for as long as we need it for, which is typically the duration of your employment or training with us, though in some cases we will keep your data for a period after your employment/training has ended due to legal or regulatory obligations. For learners who attended funded training courses, we keep your data only for the period to meet our regulatory obligations, typically driven by the ESFA.

When personal data is no longer required, or has passed its retention date:

- paper records are shredded or disposed of using a reputable disposal contractor
- electronic records are permanently deleted, with particular care taken that 'hidden' data cannot be recovered.

Automated decision making

We will make some decisions about you based on automated decision making (where a decision is taken about you using an electronic system without human involvement) eg DBS check.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request (SAR) to the Data Protection Officer
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold on you for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact the Data Protection Officer.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioner's Office (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

Data Protection Officer

The Company's Data Protection Officer is Mike Monaghan, IT & Systems Manager and can be contacted on dpo@system-group.com.

Overall data protection responsibility resides with the CEO, Paul Hudson.