General Data Protection Regulation (GDPR) Policy

Document control

Document reference:	P20V4
Document:	General data protection regulation policy
Version:	Version 4
Issue date:	May 2023
Review date:	May 2024
Replaces version/date:	Version 3.1 May 2022
Author:	Jayne Wass
Owner:	Data protection officer / compliance manager
Summary:	This policy has been produced to ensure to provide staff with clarity and to make sure they are aware of the statutory duties the UK GDPR and other relevant data protection legislation places on our organisation and to ensure they are aware of their legal obligations and responsibilities under the UK GDPR and other relevant data protection legislation.

Authorisation

Signature:	Graham D Howe	**Title**	Managing Director	4th May 2023

Purpose

This Data Protection Policy has been produced to ensure our compliance with the UK General Data Protection Regulation (UK GDPR) and associated legislation, such as the Data Protection Act 2018.

The Policy is intended to complement our data protection procedure and provides a framework for compliance and will provide advice and keep staff up-to-date with good practice.

Objectives

The Policy's objectives are:

- to ensure staff are aware of the statutory duties the UK GDPR and other relevant data protection legislation places on our organisation.

- to ensure staff are aware of their legal obligations and responsibilities under the UK GDPR and other relevant data protection legislation.

- to provide clarity to staff on key aspects of data protection legislation.

- to ensure staff are aware compliance with this policy is compulsory and any member of staff who fails to comply may be subject to disciplinary action.

Scope

This policy applies to all staff. This includes anyone who works on behalf of us, consultants and suppliers. It also covers any staff or learners who may be involved in activities that requires them to process or have access to personal data. In such cases, it is the responsibility of the relevant department to ensure that data is processed in accordance with relevant data protection legislation (including the UK GDPR) and that learners and staff are advised of their responsibilities.

This policy is concerned with personal data (including Special Category data) as defined by the UK GDPR. Personal data is any information relating to an individual who can be directly or indirectly identified, by reference to an identifier, such as a name, an identification number, location data, and an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Examples of categories of personal data include:

- Name
- Date of birth
- Address
- National insurance number
- Passport number
- Payroll number
- Learner ID

Special Category (formerly known as sensitive personal) data is a subset of personal data and means personal data consisting of information relating to;

- Racial or ethnic origin,
- Religious or philosophical beliefs,
- Genetic data (used for identifying an individual),
- Biometric data (used for identifying an individual),
- Data concerning an individual's health,
- An individual's sex life or sexual orientation.

Any processing of criminal offence data should be handled (similarly special category data) by determining the legal basis of processing in accordance with Article 6 of the UK GDPR, with the condition of also ensuring compliance with Article 10.

Data protection legislation

The Data Protection Legislation (UK GDPR and the Data Protection Act 2018) provides a framework for organisations (controllers) which ensures personal data is handled properly, as well as providing legal rights to individuals (data subjects). The legislation works in two ways: firstly, it states anyone who processes personal data must comply with the data protection principles, as defined by the relevant data protection legislation; secondly, it provides individuals with important rights, including the right to find out what personal data is held in both digital and paper records.

The Data Protection Principles Data protection legislation requires us (as a controller),our staff and others who process or use any personal data to comply with the data protection principles. The principles are listed below:

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Accountability.

The UK GDPR, provides various rights to individuals, these are listed below;

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure (right to be forgotten).
- Right to restriction of processing.
- Right to data portability.
- Right to object.
- Rights relating to automated decision making, including profiling.

If any member of staff receives a request relating to any of the above rights it must be sent immediately to the data protection officer, who will process it. The most commonly exercised individual right is that of the right of access. The right of access allows an individual to know what information we hold and processes about them. This is called a subject access request, which also allows for individuals to be given a copy of the information, as well as supplementary information, such as where and with whom the information may have been shared. The right of access, like many of the individual rights, is not an absolute right and disclosure of the requested information is subject to exemptions.

Unless the information requested is provided as part of the normal course of business, the individual who is the subject of the data (the data subject) should be directed to the data protection officer for advice on how to make a Subject Access Request (SAR). We must respond to these requests within one month of their receipt.

Registration

The Information Commissioners Office (ICO) publishes a register of controllers on its website which is available to the public for inspection. Our notification can be found on the ICO's website by entering our registration number: ZA125194. The Information Commissioner's Office is the UK's independent authority (Supervisory Authority) established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforces and oversees the relevant data protection legislation as well as the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations. The ICO has the power to take regulatory actions to enforce compliance with the data protection legislation, it also receives and responds to complaints from individuals and organisations who feel they are being denied access to personal data they are entitled to or feel their information has not been handled according to the data protection principles or legislation. Further information about the ICO can be found on its website at http://www.ico.org.uk.

Responsibilities

Staff who process personal data as part of their duties must ensure they are complying with the Data Protection Principles and more generally in compliance with relevant data protection legislation. "Processing" data is a collective term for any action taken relating to personal data and includes obtaining, recording, storing, using, sharing, disclosing, transferring, or destroying data.

Obtaining Personal Data

Only personal data necessary for a specific apprenticeship college-related business reason should be obtained, and it should be collected in a secure manner. A privacy notice (also known as a fair processing notice) must be actively communicated to an individual at the point their personal data is collected and subsequently if requested by individuals. Ideally the privacy notice should be provided in the same medium in which the data was collected. A privacy notice must as a minimum include the following:

- The name and contact details of the controller (The apprenticeship college).
- Contact details of the data protection officer or compliance department.
- The purposes of the processing.
- The legal basis of this processing.
- Details regarding any processing based on legitimate interest.
- Categories of personal data being processed.
- The recipients or categories of recipients of the personal data.
- Details regarding any transfers of personal data to a third country, or international organisations.

- Retention periods for the personal data.
- Information regarding individual rights.
- The right to withdraw consent (if this is the basis of the processing).
- How to make a complaint, and how to do so.
- Details of any statutory or contractual processing.
- The existence of any automated decision making, including profiling.
- Details of any examples where the controller is likely to process the personal data for a different purpose than it was originally collected.

In some cases individuals will have a choice whether or not to provide their personal data, or the use that can be made of it. In these cases clear consent must be obtained. All consent mechanisms must be compliant with the threshold stipulated by the UK GDPR. 'Opt-out' consent is no longer valid.

When new projects and initiatives are being developed that could have implications on individuals' privacy, TA Data Protection Impact Assessment (DPIA) screening checklist must be completed. Staff must comply with the concept of Data Protection by Design and Default. This is a mandatory concept enforced by the UK GDPR, from the beginning and throughout the lifecycle of personal data. Data Protection by Design and Default requires controllers to implement appropriate technical and organisational measures:

- Which are designed to implement the data protection principles;
- Ensuring that, by default, only the minimal amount of personal data is processed for each of the processing purposes.

Recording Personal Data

Staff must ensure mechanisms are in place for keeping personal data accurate and up-to-date and for the purpose for which it is held. Personal data should be retained in accordance with any retention period specified in the relevant privacy notice, and in accordance with our records retention schedule.

Staff should be aware that any material they produce, which refers to an individual (or individuals) may be accessed by the individual, regardless of the informality of the information, how or where it is held. This includes any opinion of or about the individual. Staff should be aware of this when documents/records are created, including emails.

Storing Personal Data

Staff whose work involves processing personal data, whether in electronic or paper form, must take personal responsibility for its secure storage. Access to personal data, in electronic or paper form, should be restricted to staff who need to access the information in the course of their duties. Personal data in paper form must be kept in a lockable filing cabinet, cupboard or drawer. Documents containing personal data should only be printed when there is a business need to do so. Personal data in electronic form should be stored within the company drive and should not be kept on local hard drives. As a minimum, user accounts should be password protected and consideration should be given to the use of additional folder, file or database level password protection, access restrictions and/or encryption.

Staff who intend to store personal data on a portable storage device, such as a laptop, tablet, memory stick, hard drive, disk or mobile phone, must be encrypted and the device must be kept in a lockable filing cabinet, cupboard or drawer.

Staff must continue to comply with the data protection legislation when working remotely. Staff should review the relevant policies and guidance relating to remote working, available on BREATHE and the shared drive to ensure that personal data is kept secure whilst working remotely. If personal data are processed off-site electronically, this must be done so using apprenticeship college approved equipment.

Using Personal Data

Personal data should only be processed for the specific purpose contained in the relevant privacy notice which was provided when the data was collected. If staff wish to use the personal data in a new and unforeseen way, the privacy notice should be updated to reflect the change. If the change would not reasonably be expected by the data subjects, staff must actively communicate the revised privacy notice to them. In certain cases clear consent from the data subjects must be obtained before the personal data is used in the new way.

Data Protection by Design and Default must be considered throughout the lifecycle of personal data. All marketing activities, including communications which involve processing personal data must be managed in accordance with both the UK GDPR and the Privacy and Electronic Communication Regulation (PECR). Unsolicited marketing activities involving messages sent by telephone, fax, email or text must conform to UK GDPR and PECR.

Staff should be aware of the possible risk of unauthorised persons viewing personal data displayed on computer screens or in paper documents, particularly in open plan or public areas. Preventative measures such as facing computer screens away from high traffic or public areas and taking care not to leave documents containing personal data in view, should be taken. The use of privacy filters on computer screens should also be considered.

Sharing and Disclosing Personal Data

When personal data is shared between departments for valid business reasons the data must be relevant and the minimum necessary to achieve the objective. Any sharing of documents containing personal data, including special category data, should be shared using Microsoft OneDrive; files and folders can be shared using links to documents rather than sent as an attachment.

If a file must be shared as an attachment (e.g. due file type), it must be either password and/or encryption protected. When using a password to protect the data, it must be conveyed to the recipient in a separate message. Best practice is to relay the password by telephone to the intended recipient. Following sharing, departments must assess whether any new use of data will be compatible with the purpose for which it was originally collected. If not, the data subjects may need to be made aware of the intention to use their data in this way and in some instances consent may be required. Departments must also consider the retention and disposal of the shared information. Where the data is required for a single purpose the duplicate information should be destroyed after use. Where a permanent record is required, the department must establish a process to ensure the data continues to be held in line with the Data Protection Principles and our retention schedule.

In some instances we may be required, for mandatory or statutory reasons, to share information with certain third parties. Personal data may also be shared with other third parties if there is a clear and lawful purpose for doing so, if the data sharing is a proportionate means of achieving that purpose, and if the data sharing is transparent to the data subjects. In most cases, where the sharing of data is regular, then an information sharing agreement between the parties is required.

We, as the controller, continues to remain liable for ensuring personal data is processed in compliance with the Data Protection Principles, when the processing is undertaken by an external company or organisation (known as a data processor). Although the processor is now also liable for any inappropriate processing activities. If a department decides to outsource a data processing function, it must ensure a data processing agreement is in place before any activity is undertaken by the processor, on the controller's behalf. There is a necessity to provide assurance the data processor will meet their legal obligations as stipulated by relevant data protection legislation, which are known as 'sufficient guarantees'.

Relevant data protection legislation allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Staff who receive a request to disclose personal data for reasons relating to national security, crime prevention or taxation should contact the data protection officer / compliance manager for advice to enable the request to be recorded and processed in accordance with our procedures. In response to most other requests, staff must not disclose personal data, or particularly special category (sensitive) data, without the consent of the data subject. If consent is received, staff must ensure that the data is given to the correct enquirer, for this reason disclosure should be made in writing and not by telephone. If a request for the disclosure of personal data is received, and consent has not been given by the data subject, the request should be sent to the data protection officer / compliance manager to process appropriately. If personal details are requested by a data subject or third party that is not provided as part of normal business, the individual requesting the data should be directed to the data protection officer / compliance manager for advice on how to make a Subject Access Request (SAR). We must respond to SARs within one month of their receipt.

Transferring Personal Data

Any transfer of personal data must be done securely. Email is not a secure method of communication and sending personal data via external email should be avoided unless it is encrypted, with the password provided to the recipient by separate means (such as via telephone), by other encryption techniques; or by the use of a link to shared folders or our OneDrive facility.

While internal email (within our email system) is more secure, it is still advisable to consider encrypting attachments which contain data belonging to a large number of data subjects, or sensitive personal data, in order to mitigate the risks associated with emails being sent or forwarded to unintended recipients. Emails containing personal data should be marked as 'Confidential', have an appropriate subject heading, and explain clearly to the recipient why they are being sent the information, and what they are expected to do with it.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important emails are correctly addressed and care is taken when using the 'Reply All', forwarding functions, or when copying others into emails. Personal email accounts must not be used to send or receive personal data for work purposes. When sending personal data externally by paper form, a Royal Mail tracking service or courier service must be used. If personal data is sent via Royal Mail, it is recommended the 'Special Delivery' service is used, particularly if Special Category data is being transferred. When sending personal data internally in paper form, it should be sealed in an envelope marked 'confidential' and ideally hand-delivered to the recipient.

Destroying Personal Data

Departments should adhere to our record retention schedule for all data (including personal data) they hold and ensure it is destroyed when no longer required. On destruction, personal data in paper form must be shredded. Personal data in electronic form should be deleted. Portable devices that hold personal data can be destroyed by I-team.

Reporting a Data Breach

It is important we respond to data breaches quickly and effectively. A breach may arise from a theft, a deliberate attack on our systems, unauthorised use of personal data, accidental loss, by disclosure (including emails, containing personal data being sent to the wrong recipient), or equipment failure. Data breaches should be reported to the data protection officer and I-team Helpdesk as soon as possible so mitigation techniques can be implemented quickly to limit any potential repercussions. All initial contact must be made via telephone, to ensure a member of I-team Helpdesk can respond as quickly as possible.

ANNEX 1

The Data Protection Principles

"Personal data shall be:

- processed lawfully, fairly and in transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

- 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

• 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 ('accuracy')

• kept 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 insofar as the personal data will be processed solely for the purposes of archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

• 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 ('integrity and confidentiality')

• the controller shall be responsible for, and be able to demonstrate compliance with, the first principle" ('accountability')"

Legal Basis for Processing Personal and Special Category Data

Personal Data

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;

(c) Processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Sub-paragraph 1(f) shall not apply to processing carried out by public authorities in the performance of their tasks.

Special Category Data

1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member state law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally capable of giving consent;

(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without consent of the data subjects;

(e) Processing relates to personal data which are manifestly made public by the data subject;

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of the health or social care or treatment of the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical services, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes of statistical purposes in accordance with Article 89(1) based in Union or member State law which shall be proportionate to the aim pursued, respect of the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.