CIDORI

Igniting careers,
Transforming workplaces.

# Data Protection Policy

# Policy Statement

The Data Protection Act 2018, UK GDPR, Privacy and Electronic Communications Regulations (PECR), and the Data (Use and Access) Act 2025 (DUAA) together form the primary framework for data protection and privacy law in the UK. The DUAA amends and supplements the UK GDPR and Data Protection Act 2018 to support responsible data use, innovation, lawful data sharing, and modernised data governance requirements while maintaining high standards of protection for individuals' rights and freedoms.

Gateway Managed Services (GMS) is committed to a policy of protecting the rights and privacy of individuals, including but not limited to learners, employees, and anyone else we engage with, in accordance with the current, relevant data protection legislation.

GMS needs to process certain information about candidates, learners, our staff, and other individuals it engages with for administrative purposes e.g., to recruit and pay staff, to administer courses and training with our college and training partners, to record training progress and to comply with our legal obligations to funding bodies, the government, and its agencies. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff within the company. Any breach of the DPA, GDPR or the company Data Protection Policy is considered to be an offence and in such an event, GMS disciplinary procedures will apply.

**As a matter of good practice individuals working with the company who have access to personal (for definition see 'Data Security' below) information will be expected to have read and comply with this policy.**

This policy and the rules upon which it is based apply regardless of whether data is stored electronically, on paper or other materials.

GMS is registered with the Information Commissioners Office, Registration number: **ZA374768**

# Compliance

In order to ensure GDPR compliance, GMS implements specific measures:

- **Website Data Collection & Consent, Privacy Policy:** we provide an updated framework and privacy policy to incorporate the GDPR obligations.

- **Data Impact Assessments & Data Inventory:** we undertake an ongoing systematic review of the data we store, manage, maintain, collect, process and control. This includes offline storage and paper records. Assessments of the data will review information flow, any data transfers, risk reviews, and structural position in relation to Lawfulness, Purpose, Minimisation, Accuracy, Consent, Limitation, Integrity & Confidentiality, Record Keeping and Accountability.

- **Training & Awareness:** we undertake training across the Group on the GDPR and its impact on the new policies, procedures, and responsibilities of staff & stakeholders in this new regime.

- **Controls & Gap Analysis:** running alongside the work already underway, we review the controls in place or required.

- **Supplier & Partner relationships:** where relevant and related, we use all reasonable endeavours to ensure that our third party and suppliers are complying with the GDPR.

- **Technology:** we review our technology platforms to analyse their operation, security, compliance in order to ensure that they meet the standards we have laid down and identify any gaps and risks.

Compliance is supported by a review of existing contracts with data controllers, and GMS's Data Protection Officer will inform, advise, and monitor compliance.

As data processor, GMS undertakes risk assessments to include more detailed consideration of the data types held and a data protection impact analysis of personal information stored and processed. Policies such as incident response plans and backup data retention are periodically reviewed and updated.

# Data (Use and Access) Act 2025 (DUAA)

GMS recognises the requirements introduced by the Data (Use and Access) Act 2025 (DUAA), which amends aspects of the UK GDPR, Data Protection Act 2018, and PECR.
GMS will:

- Maintain lawful, fair, and transparent processing of personal data.
- Implement procedures to support responsible data sharing and accountability.
- Ensure individuals are able to raise complaints regarding the handling of their personal data.
- Apply additional safeguards where automated decision-making or profiling is used.
- Continue to apply appropriate technical and organisational measures to protect personal data.
- Review international data transfer arrangements to ensure compliance with updated UK adequacy and transfer requirements.
- Ensure that any online services likely to be accessed by children consider children's privacy and data protection needs.
- Conduct reasonable and proportionate searches when responding to Subject Access Requests.

# Principles of data protection outlined in the DPA & GDPR

Staff involved in the processing of personal data must comply with enforceable principles of good practice upon which the DPA is founded, and which mean that data must:

1. Be processed lawfully, fairly, transparently, and accountably.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant, and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Be processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.
9.Personal data processing activities involving automated decision-making or profiling must include appropriate safeguards, including the right for individuals to request human review where legally required.

# Data Protection Strategy

This data protection policy aims to ensure that GMS:

- Complies with data protection laws and follows good practice.
- Protects the rights of staff, learners, partners, and customers.
- Is open about how it stores and processes data.
- Protects itself from the risks of data breach.

To ensure that the Data Protection Policy is delivered and achieved a number of strategies are maintained.

These strategies will be reviewed annually by the Senior Management Team in consultation with the nominated Data Protection Officer.

Any employee who believes that this policy has not been followed regarding their own personal data should immediately raise the matter through designated reporting lines. If the matter is unresolved, it should then be raised as a formal grievance under the Grievance Procedures.

# Data Security

All staff are responsible for ensuring that all personal data held is kept securely.

Personal data is defined as any information about a living person. Sensitive personal data includes data on the following subjects:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Physical or medical health conditions
- Sexual life/orientation
- Criminal offences
- Criminal proceedings and convictions (collected and held only with the data subject's express consent)

Care must be taken to ensure that personal or sensitive information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. This includes visual images held by a GMS CCTV security system.

Staff should note that unauthorised disclosure would usually be a disciplinary matter and may be considered gross misconduct in some cases. Our policy regarding data security is as follows:

- We will ensure that all personal data held is maintained securely and safely and that information is not disclosed to any unauthorised third parties.
- We will ensure that all data held is accessible only by those who require access to it, all data held in an electronic format is password protected and that manual records are kept in a secure location where they cannot be accessed by unauthorised personnel. Manual records that are no longer required will be disposed of as confidential waste and shredded.
- We will ensure that personal data is not disclosed to unauthorised third parties and that caution will be exercised when including personal data within reports or listings.
- We will ensure that when personal data must be disclosed to authorised third parties, it is sent using a safe and secure method. When sending personal data to authorised third parties in an electronic format, it will be sent using strong encryption.
- We will not use personal data for direct marketing purposes or provide data to unauthorised third parties.
- If data is to be entered onto third party databases for legislative or funding requirements, permission will be requested from individuals prior to doing so.

## Data Protection Risks

This policy helps to protect GMS from data security risks, including but not limited to:

- **Breaches of confidentiality.** E.g., information being released inappropriately.
- **Failure to offer choice.** E.g., all individuals about who we hold data should be free to choose how we use data relating to them.
- **Reputational damage.** E.g., we could suffer harm if data is hacked or otherwise breached electronically, and access is gained to sensitive information or data relating to GMS.

## Responsibilities under the Data Protection Act & GDPR

GMS acts either as or both the data controller and processor, dependent upon the context.

A Data Protection Officer has been appointed who is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the Company.

The Directors, Senior Management Team, and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within their teams.

Compliance with data protection legislation is the responsibility of all members of the Company who process personal information. Members of the Company are responsible for ensuring that any personal data supplied to the Company are accurate and up to date.

# Data Protection – Staff Responsibilities

Employees will routinely process data regarding learners for example when marking registers, writing reports, updating databases or in an academic supervisory role. GMS will ensure through the learner registration procedures that all learners give consent to these kinds of data processing and are informed of the various categories thereof as required by the DPA & GDPR.

Types of data that employees will routinely process includes (but is not limited to) details such as:

- Personal details such as name and address, date of birth etc.
- National Insurance Number
- Previous Qualifications
- Class attendance records
- Course work and associated comments
- Personal supervision related notes e.g., behaviour and discipline matters

Each member of staff needs to be aware of the following aspects related to their responsibilities:

- Data should not be shared informally. When access to confidential information is required, employees can request from their line manager.
- GMS will provide training guidelines to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and should never be shared.
- Personal data should not be disclosed to unauthorised persons, either internally or externally.
- Data held should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of permanently.
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.
- Employees must not disclose personal data to a learner (unless for normal academic purposes) without authorisation or agreement.
- Employees shall not disclose personal data to other staff members unless authorised by the individual concerned or the HR Manager.

# Data Storage

When data is stored on paper, it should be kept in a secure place where unauthorised persons cannot see it.

These guidelines also apply to data that is held electronically but has been printed out:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees must ensure that paper and print outs are not left where unauthorised people could see them, e.g., on the floor or on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are regularly changed and never shared between employees. (See GMS Office 365 User Guidelines Section 7)
- Data should not routinely be stored on removable media, and only in the event of absolute necessity should it be ***temporarily*** stored (e.g., USB Stick). Such media should be kept locked away securely when not being used and the data deleted at the earliest possible opportunity.
- Data should only be stored on designated drives and servers – for GMS Data this means using the approved Office 365 platform – SharePoint and OneDrive. (See GMS Office 365 User Guidelines Section 12)
- Data should not be routinely stored on a PC or other local device – no data should be stored only on a local device – everything must be saved either to SharePoint or Cidori OneDrive accounts.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should not be saved directly to mobile devices such as tablets and smart phones.
- All servers and computers containing sensitive data should be protected by approved security software and firewall.

All employees should understand their responsibilities for data protection and security when dealing with personal data on computers or in files away from GMS offices/learning centres or by means of logins to the GMS server from home or away from the GMS environment:

- If the computer belongs to GMS, then it is not to be used by other household members.
- Only equipment designed to be portable is taken from GMS premises.
- If computer is owned by employee, then GMS data must not be accessible to anyone else i.e., password protected, and all files are deleted when no longer needed.
- Anti-Virus and Anti-Malware protection is in place.
- Any printouts are stored and disposed of carefully utilising services provided.
- Suitable transport is provided between home and work so that equipment data and manual files remain secure whilst in transit. Any loss, unauthorised destruction, or disclosure of data will be a potential disciplinary offence.
- Computer files brought to work from outside the GMS environment are virus checked before loading onto GMS computer equipment or the GMS server.
- No personal files can be taken from the GMS environment without the express permission of the line manager.
- Personal data in whatever format must under no circumstances be left unattended e.g., laptops in vehicles or elsewhere.
- Personal data files must not be left unattended at any time except when locked in a filing cabinet drawer or similar equipment.

## Data Use & Processing

GMS seeks to protect against unauthorised access to and use of personal data. Loss of data, corruption or theft of data are ever present dangers that all staff need to be aware of.

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, care must be exercised when sending by email and data of a sensitive or personal nature should be sent in a password protected or encrypted document.
- Personal data must not be transferred internationally unless appropriate safeguards, adequacy regulations, or approved transfer mechanisms are in place in accordance with UK GDPR and the Data (Use and Access) Act 2025.
- Any international transfer of personal data will be risk assessed and approved through appropriate contractual, organisational, and technical safeguards
- GMS may rely on recognised legitimate interests as a lawful basis for processing personal data where permitted under UK GDPR and the DUAA, including where processing is necessary for safeguarding, fraud prevention, information security, or emergency response purposes.
- All processing activities will continue to be assessed for necessity, proportionality, and fairness.

GMS understands that all organisations will need to be confident, for example, that personal and transactional data can be located and anonymised or erased, in order to respond to requests to delete, rectify, transfer, access or restrict the processing of data.
Customers and suppliers should contact their account manager to understand what features are available to enable this, from data cleansing and subject access reports to specific data retrieval and disposal tools which create efficiencies by allowing organisations to locate, anonymise and remove data with minimal administrative effort and to enable a quick and efficient response to information requests.

## Automated Decision-Making and Profiling

Where GMS uses automated systems or profiling processes that may significantly affect individuals, appropriate safeguards will be implemented in accordance with UK GDPR and the DUAA.
Individuals will be informed where significant automated decision-making is used and may:

- Request human intervention;
- Express their point of view;
- Contest a decision.

GMS will ensure that any automated processing involving special category data is subject to enhanced protections and appropriate lawful bases.

## Cryptography/Encryption

We will ensure that robust cryptography/encryption processes exist within our systems and platforms.

## My Learning Portal

This is our MS Azure based online learning platform which uses Transparent Data Encryption.

For details of the Transparent Data Encryption included in the Azure SQL managed platform, please see (https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tdeoverview?view=azuresql&tabs=azure-portal).

# Microsoft 365

Microsoft 365 uses email Encryption which is the process by which information is encoded so that only an authorized recipient can decode and consume the information. Encryption helps ensure that only authorized recipients can decrypt our content. Content includes files, email messages, calendar entries, and so on.
Encryption is part of a larger information protection strategy for our organization. By using encryption, we help ensure that only authorized parties can use the encrypted data.

With Microsoft 365, our data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).

Microsoft 365 uses encryption in two ways: in the service, and as a customer control. In the service, encryption is used in Microsoft 365 by default. Microsoft 365 uses Transport Layer Security (TLS) to encrypt the connection, or session, between two servers.

TLS email encryption:
A message is encrypted, or transformed from plain text into unreadable ciphertext, either on the sender's machine, or by a central server while the message is in transit.
The message remains in ciphertext while it's in transit in order to protect it from being read in case the message is intercepted.
Once the message is received by the recipient, the message is transformed back into readable plain text in one of two ways:
- The recipient's machine uses a key to decrypt the message, or
- A central server decrypts the message on behalf of the recipient, after validating the recipient's identity.

## Data Accuracy

DPA & GDPR requires that GMS take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees to take reasonable steps to ensure this happens.

- Data will be held in as few places as necessary.
- Staff should not create unnecessary additional data sets.
- Staff should take every opportunity to ensure that data is updated.
- Data should be updated as inaccuracies are discovered. E.g., incorrect email address or telephone number of learners.

## Subject Access Requests

All subject access requests (SAR) should be referred to the company Data Protection Officer.

All individuals who are the subject of personal data held by GMS are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to the information.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligation.

If an individual contacts the company requesting this information, such requests can be made by email, addressed to the Data Protection Officer, David Murfitt at: (dmurfitt@cidori.co.uk).

UK GDPR and the DUAA require GMS to respond to Subject Access Requests without undue delay and generally within one calendar month of receipt.
Where clarification or additional information is reasonably required to identify the requester or locate the requested information, GMS may pause (‘stop the clock’) on the response timeframe until the necessary information has been received.
GMS will conduct reasonable and proportionate searches when responding to Subject Access Requests.
The Data Protection Officer will always verify the identity of anyone making a subject access request before complying with the request.

## Data Protection Complaints

Individuals have the right to raise concerns or complaints regarding how GMS collects, stores, processes, or shares personal data.

Complaints may be submitted via email, online form, or in writing to the Data Protection Officer.

GMS will:

- Acknowledge complaints within 30 days where applicable;
- Investigate complaints fairly and without undue delay;
- Communicate the outcome of the complaint to the individual;
- Maintain records of complaints and resolutions.

Individuals also retain the right to complain directly to the Information Commissioner's Office (ICO).

## Retention of Data

GMS will retain some items of data for longer periods than others. Constraints on storage space determine that information about learners cannot be kept indefinitely unless there are specific requests to do so.

In general, information about learners held in manual files will be kept for a maximum of five years after the learner has left their GMS course programme. This will include:

- Name and address.
- Academic achievements including any relevant auditable course work and records.
- Copies of any references given.

Other information kept on computerised systems will be held for a minimum of three years after the course has ended and the learner has left their GMS course.

GMS will need to keep information about staff - in general terms all information will be kept for seven years after a member of staff leaves GMS.

However, some information will be kept for much longer; this will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment and information required for job references.

GMS will maintain appropriate records of processing activities, retention schedules, data sharing arrangements, complaints, and security incidents to demonstrate accountability and compliance with UK data protection legislation.

## Conclusion

Compliance with the DPA & GDPR is the responsibility of GMS.

Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken or access to GMS facilities being withdrawn and even criminal prosecution.

- In addition to this Policy please also note and be aware of the following related GMS resources:

GMS Office 365 User Guidelines (SharePoint)
GMS GDPR Guidelines (SharePoint)
GMS Learner Confidentiality Policy
GMS Document Retention Policy
GMS Acceptable IT Use & Cyber Awareness Policy
GMS (Trading as Cidori) Privacy Policy: https://www.cidori.co.uk/privacy-policy/