GFM Data Protection and Processing Policy

Published Date:	01 September 2026
The Policy will be reviewed annually, or more regularly, in the light of any significant new developments. The next anticipated review date will be:	**01 September 2027**

This policy is applied at GFM alongside our school's vision, mission and values.

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UAE law and where possible, aligned to UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy is based on requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- UAE Federal Decree Law No. 45 of 2021 on the Protection of Personal Data (PDPL)
- MOE Code of Conduct
- UAE and Gems Company requirements

3. Definitions

Personal data: Any information relating to an identified, or identifiable, living individual. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. Special categories and data which are more sensitive and so need more protection includes: ○ Racial or ethnic origin ○ Political opinions ○ Religious or philosophical beliefs ○ Genetics ○ Biometrics (such as fingerprints, retina and iris patterns), where used for identification ○ Health – physical or mental
Processing: Anything done to personal data, such as collecting, recording, organizing,

structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject: The identified or identifiable individual whose personal data is held or processed.
Data controller: A person or organization that determines the purposes and the means of processing personal data.
Data processor: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

4. Roles and responsibilities

a. Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a Data Controller (DC). The school's **DC is the GFM IT Manager**

b. The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

c. The principal acts as the representative of the data controller on a day-to-day basis.

d. Staff are responsible for:

   i. Collecting, storing and processing any personal data in accordance with this policy

   ii. Informing the school of any changes to their personal data, such as a change of name/address/health status

5. Data protection principles

Our policy is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to necessary fulfil the purposes for which processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

6. **Collecting personal data**
    a. **Lawfulness, fairness and transparency**
        i. We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:
    b. **Limitation, minimisation and accuracy**
        i. We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
        ii. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
        iii. Staff must only process personal data where it is necessary in order to do their jobs.
        iv. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
        v. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

7. **Sharing personal data**

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies and other schools
- Our suppliers or contractors need data to enable us to provide services.

We will also share personal data with law enforcement and government bodies where we are legally required to do so. We may also share personal data with emergency services and external authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

8. **Responding to access requests**

When responding to requests, we:

- May ask the requesting individual to provide 2 forms of identification
- May ask the requesting company for the data protection policy
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)

- May provide the information free of charge

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- It would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- It would include another person's personal data that we can't reasonably anonymize, and we don't have the other person's consent, and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

9. Parental requests to see the educational record

Educational records are provided routinely to parents and legal guardians. If the request is for an additional copy of the educational record, the school may charge a fee to cover the cost of supplying it.

There are certain circumstances in which this right can be denied, such as if:

- releasing the information might cause serious harm to the physical or mental health of the pupil.
- releasing exam marks before they are officially announced.
- the parent has defaulted their contract with the company

10. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
Any enquiries about the CCTV system should be directed to the Operations Manager and principal.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. Written consent to share images is recorded on admission. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation and policy.

Where the school takes photographs and videos, uses may include:

- Within school on noticeboards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

12. Artificial intelligence (AI)

Artificial intelligence (AI) tools are used in constructive ways. GFM recognizes that AI has many uses to help pupils learn and produce useful information for the community.

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorized or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are locked when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Passwords are generated in line with school policy and IT team guidance and encryption used
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. We keep data in line with the timeframes as set in appendix 1.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the company procedure

16. Training

All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Appendix 1: Personal data breach procedure

An electronic/e-data breach would be dealt with at corporate level, in line with company policy and guidance. A local breach would be dealt with initially by line manager and Principal in line with disciplinary policy. The school will make all reasonable efforts to contain and minimize the impact of the breach, assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences. The school will investigate the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing data at risk and measures taken.

Emails are protected at corporate level. If an email is incorrectly sent the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence). In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator

to request that the information is removed from their website and deleted .

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead. This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Designation	Name	Signature	Date
Executive Principal/CEO/	**Akram Tarik**		**01 September 2026**
Principal	**Mia Chorfi**		**01 September 2026**

Next policy review date: 01 September 2027