GDPR Policy Overview

The Grand Union Multi-Academy Trust is the Data Controller and determines the purpose and means of processing personal data.

General Data Protection Regulations

Key roles

- Data Protection Officer – Kamal Thacker (policy implementation throughout MAT and liaison with governing body)
- Head of HR/HR officer – Harjinder Johal & Tina Bakhru (staff data)
- Acting Network Manager – Inderjeet Sohal (security of electronic data)
- Admin Manager – Sharan Sond (pupil data)
- SENCO – Alka Patel (SEND information)
- Senior Inclusion and child protection officer – Lewis Adams (safeguarding and other sensitive information).

Key Principles

Personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes that are explained to the "data subjects"
- Relevant and limited to what is necessary
- Accurate and where necessary, kept up to date
- Kept for no longer than is necessary, thereafter deleted or anonymised
- Secure.

Legal principles underpinning our need to process data:

- The data needs to be processed so that the school can fulfil a contract with (or a responsibility for) an individual.
- The data needs to be processed so that the school can comply with its legal obligations
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform an official task in the public interest
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

When you can share personal data:

- If there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- When we need to liaise with other agencies – we must seek consent as necessary before doing this

- When our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies
- When legally required to do so with law enforcement and government bodies – crime, tax, legal proceedings, safeguarding and statistical research.

Rights of access for data subjects:

- Confirmation that their personal data is being processed and why
- Access to a copy of that data on demand
- The categories of the personal data being held
- Who the data has been, or will be, shared with
- How long the data will be stored for
- The source of the data, if not the individual themselves
- Whether any automated decision-making is being applied to their data (profiling), and what the consequences of this might be for the individual
- Most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil (aged 13 or over). The data belongs to the pupil.

The rights of the individual (which must be exercised via the DPO):

- Withdraw their consent (if the consent had been sought) to the processing of their data at any time
- Ask us to rectify, erase or restrict processing of their personal data
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on any automated decision making
- Prevent processing that is likely to cause damage or distress
- Be notified of any data breach
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Parental requests to view educational records:

- Parents or carers, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Biometric Systems

- Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012
- Parents/carers will be notified and the school will obtain written consent from at least one parent or carer before we take any biometric data from their child and first process it
- Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We must provide alternative means of accessing the relevant services e.g., pupils can pay for school dinners using a PIN at each transaction if they wish
- Parents/carers and pupils can withdraw consent, at any time, and we must make sure that any relevant data already captured is deleted
- If a pupil refuses to participate in the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s)
- Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV

- We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras must be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Photographs and Videos

- We may take photographs and record images of individuals within our school
- We must obtain written consent from parents/carers, or pupils aged 18 and over
- We must clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

1. Within school on notice boards and brochures, newsletters, etc.
2. Outside of school by external agencies such as the school photographer, newspapers, campaigns
3. Online on our school website.

- Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further
- When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

How we must protect the data we hold

- Appointing a suitably qualified DPO and ensuring they have the necessary training and resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for a specific and valid purpose
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to the rights of privacy of individuals
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; keeping a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Keeping data secure from unauthorised or unlawful access, alteration, processing or disclosure; and against accidental or unlawful loss, destruction or damage:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- 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 e.g. RONI information shared with the LA.
- Data is not inadvertently shared – e.g. SIMS registers displayed on IWBs.

Disposal of Records

Personal data that is no longer needed will be disposed of securely.

Retention Schedule

Retention schedule – after which records should be disposed of:

Staff references	10 years
Student references	10 years
Appraisal documents	5 years
Internal Data	5 years
Public Exam Data	10 years
Behaviour and Attendance records	5 years
Photographs and images for publicity	To be stored securely until 1 year after the student has left FHS or if consent is withdrawn.

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 agreed procedure
- When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:
    1. A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
    2. Safeguarding information being made available to an unauthorised person
    3. The theft of a school laptop containing non-encrypted personal data about pupils.

Training

- All staff and governors 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.

Monitoring Arrangements

- The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and shared with the Curriculum Committee.

Updated January 2024