MALTMAN'S GREEN SCHOOL

Data Protection Policy – for Parents

This policy also applies to the EYFS

Updated	Reviewed By	Review Date	Version
November 2026	J Stevens	November 2028	2026.01

Data Protection Policy – for Parents

Maltman's Green School takes the security and privacy of data seriously and aims to ensure that all personal data collected about employees, pupils, parents, governors, visitors and other individuals (the School Community) is collected, stored and processed in accordance and compliance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance) of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy applies to current and prospective parents/carers. 'Data subjects' are current and former paid employees, pupils, current and prospective parents/carers, bursary applicants, volunteers, governors and contractors in regulated activity. Maltman's Green School is a 'data controller' for the purposes of personal data. This means we determine the purpose and means of the processing of personal data. This policy explains how the School will hold and process information and explains rights as a 'data subject' and obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of Maltman's Green School.

This policy does not form part of any contract with the School and can be amended by Maltman's Green School at any time.

For the purposes of this Code of Conduct, the term **"parent"** refers to any individual who has signed the Acceptance Form, as well as any person who has parental responsibility for a child attending the school, whether or not they are a signatory to the contract for educational services.

The Data Protection Lead ("DPL") is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The DPL is also responsible for updating the Governing Body about data protection responsibilities and any risks in relation to the processing of data and is contactable via email bursar@maltansgreenschool.com

Data Protection Principles

Personal data must be processed in accordance with the six 'data protection principles' meaning that data must:

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
- not be kept for longer than is necessary for the purposes for which it is processed
- be processed securely.

1. Definitions

Key data protection terms used in this data protection policy are:

- Data controller – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Personal information (or 'personal data'): any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.
- Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

2. How we define Personal Data and Special Category Data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data. This applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to Maltman's Green School by a parent/carer, or someone else (such as an employee, a pupil's previous school, doctor, or a credit reference agency), or it could be created by Maltman's Green School . It could be provided or created during the application process or during the course of the pupil's time at the School (or any other services provided under the School's terms and conditions) or after its termination. It could be created by employees of the School, external bodies or by other parents/carers.

The School, in the course of its daily operations will collect and use individual personal data. Special Category Data is personal data that needs more protection because it is sensitive.

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific and explicit purposes and only for the purposes it was collected for

- Relevant and limited to what is necessary for the purposes it is processed
- Accurate and kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a manner that ensures appropriate security of the personal data.

The UK GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments)
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

The School's Privacy Notice sets out the types of sensitive personal data it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

3. How we define Processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

4. How we 'process' Data

Maltman's Green School will process personal data (including special categories of personal data) in accordance with our obligations under the 2018 Data Protection Act. We will use personal data for:

- performing the contract of services between us
- complying with any legal obligation
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if data subjects' interests and rights do not override ours (or theirs). All data subjects have the right to challenge our legitimate interests and request that we stop this processing
- for the purposes of safeguarding and promoting the welfare of individuals who come into contact with the School Community.

We can process personal data for the purposes above without knowledge or consent. We will not use personal data for an unrelated purpose without prior notification and the legal basis that we intend to rely on for processing it. Should certain personal data not be provided, there may be implication on carrying out certain parts of our contract of services. For example, if financial records are not provided, we may be unable to consider eligibility for or apply any bursaries. Additionally, an absence of the specific data may prevent us from complying with certain legal obligations and duties which we have with the local authority for example.

5. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- there is an issue with a pupil or parent/carer that puts the safety of our employees at risk or puts the safety of the pupil, parent or carer at risk
- we need to liaise with other agencies – we will seek consent as necessary before doing this but this may not always be required in circumstances where we are legally obliged to report to external agencies
- we may share the personal data of our employees or contractors and, occasionally, the personal data of other pupils or parents/carers in our communication with parents/carers
- our suppliers or contractors need data to enable us to provide services to our employees and pupils – for example, IT companies. When doing this, we will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with Maltman's Green School.

We will share personal data with law enforcement and government bodies where we are legally required to do so:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

6. Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. In the unlikely event of a suspected data breach, we will follow the procedure set out in guidance on personal data breaches produced by the ICO.

The School has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the DPL will take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then the School will notify the Information Commissioner's Office within 72 hours.

In the event of becoming aware of a data breach, the DPL should be contacted immediately and any evidence in relation to the breach should be secured so the Bursar can handle it as per outlined above.

All members of the School community have the right to be notified of a data security breach concerning your personal data.

7. Parent/carer responsibilities

Parents/carers must treat all personal data received from the School as confidential and only use it for the purpose for which it was supplied.

Any questions in relation to this policy or data protection should be directed to the School's DPL.

Access to personal data covered by this policy is only authorised and should only be used for the specified lawful purpose for which it was obtained and the following should be ensured:

- Personal data is not shared informally
- Personal data is kept secure and not shared with unauthorised parties including on social media (Twitter/X, Facebook, TikTok, Instagram, Reddit or any other social media site) or via messaging apps, such as WhatsApp, Telegram or Signal
- Personal data provided to parents/carers under this policy should not be inputted into unsecured AI tools for any purpose
- Unnecessary copies of personal data are avoided and disposal of material is done securely.
- Strong passwords are used.
- Data is anonymised or separate keys/codes are used so data cannot be identified.
- Personal data to personal computers or other devices is not stored/saved.
- Personal data is never transferred outside the European Economic Area except in compliance with the law and authorisation of the DPL.
- Personal data is shredded and disposed of securely when it is finished with
- Help is sought from the DPL if unsure about data protection or any areas of data protection or security can improved upon.

Any deliberate or negligent breach of this policy may result in the School requiring removal of a pupil in accordance with the Parent Code of Conduct. It is a criminal offence to obtain or disclose personal data without the consent of the data controller (section 170 Data Protection Act 2018).

8. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our School.

We obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials and we clearly explain how photographs and/or videos will be used to both the parent/carer and pupil. Uses may include:

- within school on notice boards 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.

Consent can be refused or withdrawn at any time. If consent is withdrawn, photographs and/or images will be deleted and not distributed further.

When using photographs and videos in this way the School will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Further information is detailed in the Pupil Photographic Consent Statement 2022.

9. Data Protection by Design and Default

The School has measures in place demonstrating we have integrated data protection into all of our data processing activities, including:

- the appointment of a suitably qualified DPL, with the necessary resources to fulfil their duties and maintain expert knowledge
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- completing privacy impact assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPL will advise on this process)
- integrating data protection into internal documents including this policy, any related policies and privacy notices
- regularly training employees on data protection law, this policy, any related policies and any other data protection matters; we will also keep 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 DPL 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 held, maintaining an internal record of the type of data, data subject, data purpose, any third-party recipients, data storage purpose, retention periods and data security.

10. Data Security and Storage of Records

The School will continue to protect personal data and keep it safe 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 hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data are not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Encryption software is used to protect all portable devices and removable media, such as USB and hard drive devices.
- Employees, 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 the School needs 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.
- Where the School (or a member of the School Community) sends parents/carers the personal data of others for the purposes set out under this policy, parents/carers are expected to take reasonable care of this data and should not use it for their own purposes without the School's knowledge and consent.

11. 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 may use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

12. Training

All employees 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.

13. Associated School Policies and documents

The School policies and documents that should be read in conjunction with this policy are:

- Admissions, Attendance and Children Missing and Absent from Education Policy
- Anti-Bullying Policy
- Assessment and Recording Policy
- Bursary Policy
- Complaints Procedure for Parents
- Critical Incident Management Plan
- Data Retention Policy
- Behaviour Policy
- Early Years Foundation Stage Policy
- English as an Additional Language (EAL) Policy
- Equal Opportunities and Anti-Prejudicial Discrimination Policy,

- Health and Safety Policy
- Keeping Children Safe in Education (Sept 2025),
- Medical Policy
- Off-Site Visits Policy
- Personal, Social, Health and Education (PSHE) Policy
- Privacy Notice
- Pupil Photographic Consent Statement
- Safeguarding Policy and Child Protection Policy & Procedures
- SEND Policy
- Spiritual, Moral, Social and Cultural Development Policy,
- Supervision Policy
- Terms and Conditions
- Visitor and Visiting Speaker Policy