Emanuel School

Data Protection Policy

1. Introduction

The processing of personal data underpins almost everything the school does. The school collects, stores and uses personal information about staff, pupils, their parents, its contractors, governors and other third parties[1] for academic and administrative purposes, as well as to comply with statutory obligations.

Emanuel School is committed to safe, fair and lawful data protection practices in line with the Data Protection Act 2018 (DPA) and adhering to the principles of the UK General Data Protection Regulation (GDPR):

- Lawfulness/fairness/transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation (data retention)
- Integrity and confidentiality (data security)
- Accountability

The school is liable for the actions of anyone that processes personal data of which the school is a controller. All staff including temporary staff, governors and volunteers must be mindful of legal obligations and have a part to play in ensuring compliance with the data protection law.

This policy sets out the school's expectations and procedures with respect to processing any personal data/special category personal data and should be read in conjunction with the school's privacy notices and other associated guidance/policies which provide further detail and advice on practical application.

In addition, this policy represents the standard of compliance expected of those who handle the school's personal data as contractors, whether they are acting as 'data processor' on the school's behalf or as data controller responsible for handling such personal data in their own right.

Emanuel School is registered with the ICO (registration number Z6672867).

2. Data Protection Terminology

Key data protection terms used in this policy and associated policies are:

Criminal Offence Data – Data that is treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures. Emanuel School processes criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on staff, contractors and volunteers. This applies even though the check has not revealed any conviction.

Data Controller – A person or organisation that determines the purposes and the means of processing personal data and who is legally responsible for how it is used. Emanuel School processes personal data relating to pupils, parents, staff, governors, visitors and other third parties and is therefore a data controller.

Data Breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Processor – A person or organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services with whom personal data may be shared

[1] Third parties may include suppliers, volunteers, visitors, applicants, alumni and others. Staff, pupils, parents and other data subjects/third parties may include past, present or potential members of those groups.

but who is not authorised to make any decisions about how it is used *(see also the definition of 'Processing').*

Data Protection Impact Assessment (DPIA) – A DPIAs is a tool used to identify risks in data processing activities with a view to reducing them.

Data Subject – This is the person the data/information relates to, the identified/identifiable individual whose personal data is held or processed. Data subjects include pupils and former pupils (alumni), parents and carers, staff, non-employed staff, contractors, governors and trustees, visitors, volunteers, applicants.

ICO – The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights and the regulator for data protection. It can provide guidance to promote good practice and take enforcement action where there is a breach of data protection legislation.

Personal Data – Personal data is information that relates to an identified or identifiable individual. This may include but is not limited to:

- identity and contact details,
- information about pupil behaviour and attendance,
- exam results,
- staff development reviews,
- staff recruitment information,
- staff contracts.

Privacy by Design and Default – Integrating data protection concerns into every aspect of processing activities.

Processing – This involves any activity that involves the use of personal data. This includes but is not limited to obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties. Processing can be automated or manual.

Special Categories of Personal Data – This is personal data that is considered more sensitive and is given greater protection in law. Special category data includes:

- personal data revealing racial or ethnic origin,
- personal data revealing political opinions,
- personal data revealing religious or philosophical beliefs,
- personal data revealing trade-union membership,
- genetic information,
- biometric information (where used for identification purposes),
- data concerning health (for example, medical information),
- data concerning a person's sex life,
- data concerning a person's sexual orientation.
- sexual matters or sexual orientation.

3. Data Protection Responsibilities

Everyone at Emanuel School is responsible for protecting personal data. There are some key roles and responsibilities for data protection compliance.

For most of the personal data the school collects, stores and uses, Emanuel School is the data controller and is responsible under the data protection law.

3.1 Governor and Trustee Responsibilities

The responsibility and accountability for compliance with the UK GDPR and Data Protection Act 2018 sits with governors and trustees.

3.2 Data Protection Lead (Bursar)

At Emanuel School, the bursar is the data protection lead. The data protection lead and compliance manager form the data protection response team.

The bursar is responsible for:

- advising school leaders and staff about their data obligations,
- monitoring compliance,
- conducting regular data audits,
- developing and updating data protection policies and procedures,
- monitoring who in the school has access to personal data,
- advising when data protection impact assessments are needed,
- answering data protection enquiries,
- keeping records of personal data breaches, notifying the ICO of any significant breaches and responding to any requests that it may make for further information,
- supporting and advising staff who have data protection queries,
- promoting security awareness and ensuring staff understand its importance,
- reporting to the governing body about data protection,
- advising the governing body on data protection risks,
- advising on and co-ordinating responses to information rights requests,
- making sure all assets containing personal data are appropriately managed and secure,
- making sure any contract with third-party processors cover,
- making sure staff receive annual training on data protection, including specific school processes such as data breach reporting processes and the escalation of information rights requests.

The bursar delegates day to day responsibility for undertaking some of these responsibilities through line management and identified roles to the compliance manager and/or head of IT as appropriate.

3.3 Heads of Department (or equivalent) Responsibilities

Heads of departments are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

- new and existing staff, visitors or third parties associated with the department who are likely to process personal data are aware of their responsibilities under data protection legislation. This includes drawing attention of staff to the requirements of this policy and ensuring that staff who have responsibility for handling personal data have the time to complete data protection training as part of their induction programme and ongoing development,
- data protection requirements are embedded into systems and processes by adopting a 'privacy by design and default' approach and undertaking data protection/privacy impact assessments where appropriate,
- privacy notices are provided where data is collected directly from individuals,
- data sharing is conducted in accordance with the *Data Protection Guidance for Staff*,
- requests from the data protection response team for information are complied with promptly,
- departmental policies and procedures are adopted where appropriate.

3.4 Staff Responsibilities

Anyone who processes personal data as part of their role is individually responsible for complying with data protection legislation, this policy any other policy/guidance/procedure and/or training introduced by the school to comply with data protection legislation.

In summary, staff must ensure that they:

- only use personal data in ways people would expect and for the purposes for which it was collected.
- use a minimum amount of personal data and only hold it for as ling as is strictly necessary.
- keep personal data up to date.
- keep personal data secure, in accordance with the school's *Information Security Policy*.
- do not disclose personal data to unauthorised persons, whether inside or outside the school.
- complete relevant training as required.
- report promptly (within 24 hours) any suspected data breaches or near misses to the data protection response team using the *Data Breach Reporting Form* (Firefly). If the data breach is believed to be serious, they should contact the bursar without delay. Staff should not attempt to investigate the matter themselves.
- are aware of the individual's legal rights set out in this policy (*see 'Data Subject Rights'*) and what the process is for recognising and escalating information rights requests. All rights requests must be forwarded to the data protection response team immediately. Staff should refer to the *Data Protection Guidelines for Staff* and *Procedure for Responding to Subject Access Requests*.
- seek advice from the data protection response team where they are unsure how to comply with data protection legislation.
- promptly respond to any requests from the data protection response team in connection with subject access and other rights-based requests and complaints (and forward any such requests that are received directly to the data protection response team).

Staff are required to take regard of the *Data Protection Guidelines for Staff* that describe staff responsibilities in more detail.

4. The Data Protection Principles

The UK GDPR sets out seven key 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:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals and not further processed in a manner that is incompatible with those purposes (lawfulness/fairness/transparency).
2. Collected for specified, explicit and legitimate purposes (purpose limitation).
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation).
4. Accurate and, where necessary, kept up to date (accuracy).
5. Kept for no longer than is necessary (storage limitation).
6. Processed in a way that ensures it is appropriately secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational manners (integrity and confidentiality).
7. The accountability principle requires the school to be able to prove that it adheres to data protection law.

Emanuel School implements appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. This involves, but is not limited to:

- Keeping records of our data processing activities, by way of logs and policies,

- Documenting significant decisions and assessments about how we use personal data (incl. Data Protection Impact Assessments),
- Generally having an 'audit trail' regarding data protection and privacy matters.

5. Lawful Basis for Data Processing

The school must have a lawful basis to process the data about an individual. Our privacy notices set out how we use data.

Before the processing starts for the first time, the school will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. The school may only process a data subject's personal data if one of the following lawful bases are met:

- The data subject (or their parent as appropriate) has freely given clear **consent**.
- The data needs to be processed so that the school can **fulfil a contract** with the data subject/individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation**.
- 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 can perform a task in the **public interest** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party.

Where the school relies on consent as lawful basis for processing, it will adhere to the requirements set out in the UK GDPR. The school will keep records of consent obtained to demonstrate compliance with consent requirements.

For special category data and criminal offence data, the school will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018 and may include:

- The individual (or parent) has given **explicit consent**.
- It is necessary in order for the school to carry out its obligations under **employment, social security or social protection law.**
- It is necessary to protect the **vital interests** of an individual who cannot give consent.
- The information has already been **manifestly made public** by the individual concerned.
- It is necessary for **legal claims or judicial acts**.
- It is necessary for reasons of **substantial public interest**.
- It is necessary for assessing the working capacity of an employee.
- It is necessary for reasons of public interest and there is a basis in law (**public health** or **archiving/research/statistics**).

6. Specified/Explicit/Legitimate Purposes for Data Processing

The school will only collect/process personal data for specified, explicit and legitimate purposes. These include:

- Ensuring that the school provides a safe and secure environment,
- Providing pastoral care,
- Providing education and learning for children/pupils,
- Safeguarding and promoting the welfare of children,
- Providing additional activities for children and parents (e.g. activity clubs),
- Protecting and promoting the school's interests and objectives,
- For personnel, administrative and management purposes,

- Fulfilling the school's contractual and other legal obligations.

7. Sharing Personal Data

Personal data will not be disclosed to anyone within the school who does not have the appropriate authority to receive such information, irrespective of their role or their relationship to the data subject, unless they need to know it for a legitimate purpose.

Emanuel School will not normally share personal data with anyone outside of the school without consent but in certain circumstances, the school will need to share personal information with third parties, such as professional advisers (lawyers, insurers and accountants) or relevant authorities (DfE, Independent Schools Inspectorate, Independent Schools Council, the Charities Commission, HMRC, police or the local authority).

Before sharing personal data outside of the school, staff will:

- consider all the legal implications,
- make sure they are allowed to share it (see *Lawful Basis of Data Processing*),
- confirm who needs the data, what data is needed and what they will use it for,
- ensure adequate security,
- ensure that only the minimum amount of personal data required for the specific purpose is shared.
- make sure that the sharing is covered in the *Privacy Notice*.

Further details on sharing personal data can be found in the privacy notices.

7.1 Keeping Children Safe

Occasionally, the school will also share information where the disclosure is required to satisfy safeguarding obligations. The UK GDPR or the DPA 2018 does not limit the sharing of information for the purposes of keeping children and young people safe. The statutory DfE guidance *Working Together to Safeguard Children* states that "effective sharing of information is essential for early identification of need, assessment, and service provision to keep children safe".

The school follows the guidance *Information Sharing – Advice for Practitioners providing safeguarding services to children, young people, parents and carers (July 2018).*

Data protection legislation permits the sharing of special category personal data without consent where it is to keep a child or young person safe from neglect or physical, emotional or mental harm, or if it is to protect their physical, mental or emotional well-being.

The school will comply with the data protection principles when making a permitted disclosure.

7.2 Consent

The school will obtain written consent to share personal data in circumstances in which this is required. Individuals should refer to the school's privacy notices which inform with whom/which organisations data is shared and why it is shared.

In matters concerning a pupil aged about 13 years/ a pupil in year 8, the school will (as required) get the pupil's consent to share their data. If the child is younger than this, the school will only get consent from whoever holds parental responsibility for the child.

The school will not use pre-ticked boxes or disclaimers stating that by not responding the sharing of data has been agreed.

Consent for taking and using photographs and video is described in the *Photographic Image and Video Policy*.

8. Data Subject Rights

One of the aims of the UK GDPR is to empower individuals (data subjects) and give them control over their personal information. The UK GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right of erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The school's privacy notices make members of the school community aware of their data subject rights. Requests to invoke any of the rights listed above will be treated in the correct manner and individuals will be assisted accordingly.

1. The right to be informed – Individuals have the right to be informed about the collections and use of their personal data. This is a key transparency requirement under the UK GDPR. The school's privacy notices are written in clear, plain language that is concise, transparent and easily accessible.

2. The right of access – Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. The individual can make a subject access request which will be dealt with promptly in line with agreed procedures and legislation. Detailed information regarding an individual's right of access can be found in the school's privacy notices. Staff should refer to the *Procedure for Responding to Subject Access Requests*.

3. The right to rectification – Individuals have the right to have personal data rectified if it is inaccurate or incomplete.

4. The right to erasure – The right to erasure is also known as the 'right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. In a school context this right only applies in limited circumstances.

5. The right to restrict processing - Individuals have the right to 'block' or suppress the processing of personal data. When processing is restricted, the school is permitted to store the personal data, but not process it further. The school can retain just enough information about the individual to ensure that the restriction is respected in future.

6. The right to data portability – Individuals have the right to obtain and reuse their personal data for their own purpose across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another (i.e. another school) in a safe and secure way, without hindrance to usability.

7. The right to object – Individuals have the right to object (verbally or in writing) to processing based on legitimate interests or the performance of a task in the public interest, direct marketing and processing for purposes of scientific/historical research and statistics.

8. Individuals also have rights in relation to automated decision-making and profiling (i.e. where a significant decision is made about the individual without human intervention). In circumstances where the school would carry out automated decision-making and be challenged by an individual, an investigation would be performed.

9. Data Security

Emanuel School will 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 as required by legislation. Staff should be conscious of these requirements when reading and applying other school policies. Examples of security procedures are:

- Confidential paper records are kept in locked filing cabinets/drawers with restricted access.
- Access to digital files is on a need-to-know basis; files and folders have granular permissions based on roles. File access is monitored and reviewed.
- Staff and governors will not use personal email accounts or personal cloud storage for school business.
- Where a member of staff is permitted to take data offsite, it will need to be handled, used and stored in a secure manner.
- Where possible, mobile devices are enabled to allow the remote blocking or deletion of data in case of theft or loss.

Staff should be mindful of the increased data security risks associated with remote working.

Please refer to the *Information Security Policy* for further information.

10. Data Breach Response and Monitoring

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. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of staff to disclose personal information unlawfully which may result in disciplinary action).

Incidents must be reported to the data protection response team within 24 hours; serious incidents have to be reported to the bursar without delay.

10.1 Preventing Data Breaches

Protecting confidentiality, integrity and availability of personal data is a critical responsibility that the school takes very seriously. Emanuel School takes steps to reduce the possibility of personal data breaches occurring which include but are not limited to:

- Mandatory data protection training for all staff at induction that includes how to recognise and report a personal data breach.
- Refresher training at appropriate intervals.
- Having appropriate controls in place to protect personal data *(please refer to 'Data Security').*
- Ensuring staff have an awareness of common data breaches and how they can be avoided, such as by checking recipients and attachments are correct before sending emails (staff awareness training).

10.2 Assessing and Reporting Breaches

The school has procedures in place to assess the severity of data security incidents and to report relevant breaches to the Information Commissioner's Office (ICO) within the statutory time frame.

It is the school's priority to establish what has happened to the personal data and to take action to limit further impact. Where the school believes that the breach is likely to result in a high risk to the rights and freedoms of a data subject,

- the bursar will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the data breach, even if the school does not have all details yet.

- the data subject(s) concerned will be informed with undue delay as appropriate. If possible, the school will give specific and clear advice on the steps the individual can take to protect themselves, and what the school is willing to do to help them.
- the school will inform the Charity Commission as appropriate.

If the school concludes that a data breach does not need to be reported to the ICO, this will be documented in the data breach log to be able to justify the decision as required.

10.3 Data Breach Recording and Review

All data breaches and near misses, regardless of whether they need to be reported to the ICO, will be accurately recorded by the data protection response team. Facts regarding the breach, the number of data subjects affected, its effects and the remedial actions taken will be documented in the log.

Data breaches or near misses will be reviewed and analysed regularly to identify patterns/trends and to take action to prevent similar breaches from happening again.

Further details on data breach management and procedures can be found in the *Data Protection Guidelines for Staff.*

11. Processing of Financial/Credit Card Data

The school complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements.

Other categories of financial information, including bank details and salary, or information commonly used in identity theft (i.e. national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

12. CCTV

Closed-circuit television (CCTV) images that identify individuals are considered personal data. The school's processing includes the use of CCTV for the purposes described in the *CCTV Policy.* These include but are not limited to maintaining and monitoring the security of the premises, protecting personal safety, supporting the police and community in preventing, detecting crime and anti-social behaviour.

Camera locations have been carefully selected in areas inside and outside that the school reasonably believes require monitoring to fulfil the purposes Privacy rights and freedoms of individuals have been carefully considered. Adequate signage has been placed in prominent locations.

The school adheres to the *Surveillance Camera Code of Practice* and has a standalone *CCTV Policy*. The school's use of CCTV is also explained in the privacy notices which can be found on the school website.

CCTV image requests from a data subject (or representative, e.g. parent) are considered subject access requests and must be directed to the data protection response team immediately so that the legally defined response time can be met. The same applies to law enforcement requests or requests from other authorities.

Technical enquiries about the CCTV system should be directed to the IT department.

Where footage is required for incidents related to pupils, the head of year will discuss this with the deputy head: pastoral first.

Please refer to the *CCTV Policy* for further information on access to and disclosure of CCTV images.

13. Data Retention

Personal data will not be kept longer than is necessary for the purpose or purposes for which it was collected.

The school will take all reasonable steps to securely and confidentially destroy or erase from its systems/files, all information which is no longer required. Records containing personal information or sensitive information will be either made unreadable or in a way that it cannot be reconstructed.

Details of how long information will be retained are outlined in the school's *Data Retention and Disposal Policy*.

14. Associated Policies and Guidelines

The *Data Protection Policy* should be read in conjunction with the following policies and guidelines:

- CCTV Policy
- Communication with Parents Guidance
- Data Breach Procedure
- Data Protection Guidelines for Staff
- Data Retention and Disposal Policy
- DfE guidance Data Protection in Schools (February 2023)
- Disciplinary Procedure
- Information Security Policy
- Laptop and Mobile Device Policy
- Photographic Image and Video Policy
- Privacy Notice (staff, pupils, parents, alumni, governors, recruitment)
- Procedure for Responding to Subject Access Requests
- Recruitment Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Whistleblowing Policy

This list of policies is not exhaustive.

15. Policy Review and Approval

The policy will be reviewed and updated on a regular basis and at least annually to meet the requirement of accountability. Any key changes will be communicated to staff in such a way that it is clear what has changed.

Policy Owner	Bursar
Date of last review	July 2023
Approved by	Cabinet: September 2023 Full Governing Body:
Responsible Committee	Finance and Building
Date of next review	Summer 2024

Table of Key Changes

Date	Change
August 2023	Clear definition of roles and description of responsibilities in section 3 ('Data Protection Responsibilities') in line with DfE guidance.

16. Queries and Comments

Questions about this policy and data privacy matters in general should be directed to the data protection response team (data.protection@emanuel.org.uk).