Emerson Park Academy

DATA PROTECTION POLICY

Approved by Board of Directors

Review Date: October 2027

Contents

1. Aims
2. Legal framework
3. Definitions
4. Data Protection Principles
5. Roles and responsibilities
6. Accountability & Data Protection by Design
7. Lawful processing
8. Data Subject Rights & Subject Access Request (SAR)
9. Parental Requests & The Educational Record
10. Statutory Complaints Tracking
11. Privacy Notice for Pupils & Parents
12. Data Security
13. Data Breach Management Protocols
14. CCTV & Surveillance Operations
15. Automated Biometric Recognition Systems
16. Freedom of Information (FOI)
17. Storage, Retention and Disposal of Records
18. Monitoring, Training & Arrangements

1. AIMS

Emerson Park Academy (the Academy) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection legislation. This policy applies to all personal data, regardless of whether it is handled in paper or electronic format.

2. LEGAL FRAMEWORK

This policy satisfies the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025. It integrates statutory guidance published by the Information Commissioner's Office (ICO), including the ICO's statutory frameworks, code of practice for surveillance cameras, and model privacy infrastructure from the Department for Education (DfE).

In addition, this policy complies with the following legislative frameworks:

- The Freedom of Information Act 2000
- The Protection of Freedoms Act 2012 (governing biometric automated recognition data)
- The Education (Pupil Information) (England) Regulations 2005 (as amended), establishing parental rights of access to educational records
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Academy Standards and Framework Act 1998

3. DEFINITIONS

Personal Data: Any information relating to an identifiable, living individual who can be directly or indirectly identified, specifically via reference numbers, names, online identifiers (e.g., IP addresses), or pseudonymised criteria (key-coded).

Special Categories of Personal Data (Sensitive Data): Personal data that is inherently sensitive, requiring robust operational safeguards under UK GDPR Article 9. This explicitly includes racial/ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (processed for unique identification), physical/mental health data, or data concerning sexual orientation or criminal histories/convictions.

Processing: Any manual or automated operation performed on personal data, such as collection, recording, structuring, storage, alteration, retrieval, use, disclosure, dissemination, restriction, erasure, or secure destruction.

Data Subject: The living individual whose personal data is being held or processed.

Data Controller: The legal entity or organisation that determines the purposes and lawful means of processing personal data. Emerson Park Academy is the Data Controller.

Data Processor: A separate legal individual or external third-party entity (other than an employee of the data controller) processing data on behalf of the Data Controller.

4. DATA PROTECTION PRINCIPLES

Article 5 of the UK GDPR mandates that personal data must be:

- Processed lawfully, fairly, and in a transparent manner (Lawfulness, Fairness, Transparency).
- Collected for specified, explicit, and legitimate purposes and not further processed incompatibly (Purpose Limitation).
- Adequate, relevant, and limited to what is necessary (Data Minimisation).
- Accurate and kept up to date; inaccurate data must be erased or rectified without delay (Accuracy).
- Kept in a form permitting identification for no longer than necessary (Storage Limitation).
- Processed securely using technical or organisational measures against unauthorised access, accidental loss, damage, or destruction (Integrity and Confidentiality).

The Data Controller remains legally responsible for, and must be able to explicitly demonstrate, compliance with all the core principles listed above (Accountability Framework).

5. ROLES AND RESPONSIBILITIES

Governing Board: Holds overall statutory responsibility for ensuring that the Academy complies with data protection law.

Data Controller: Emerson Park Academy (EPA) is registered with the ICO as a data controller and maintains its registration annually.

Headteacher: Acts with delegated operational authority from the Data Controller to ensure day-to-day policy compliance.

Designated Data Protection Officer (DPO): Responsible for monitoring data compliance, conducting internal audits, delivering staff training, providing guidance on Data Protection Impact Assessments (DPIAs), and serving as the primary corporate contact point for the ICO and data subjects. The DPO can be contacted via info@emersonparkacademy.org.

All Staff Members: Accountable for collecting, storing, and processing personal data securely in strict compliance with this policy, and notifying the DPO immediately regarding data breaches or structural concerns.

6. ACCOUNTABILITY & DATA PROTECTION BY DESIGN

The Academy implements systemic technological and organizational measures to actively demonstrate regulatory compliance:

- Comprehensive internal Records of Processing Activities (ROPA) are maintained, tracking categories of data, purpose, recipients, retention schedules, and security protocols.
- Privacy by Design and Default metrics are standard operational protocol, incorporating pseudonymisation, encryption, and strict data minimisation across platforms.

- Mandatory Data Protection Impact Assessments (DPIAs) are conducted for all high-risk processing, including structural changes to the Management Information System (SIMS), the safeguarding management platform (CPOMS), or any automated biometric processing.

7. LAWFUL PROCESSING

The legal basis for processing personal data is formally documented prior to any operational execution. The Academy processes personal data under one of six core lawful bases:

- Public Task: The standard lawful operational basis for processing data necessary for the Academy's official educational mandate as a public authority.
- Legal Obligation: Necessary to comply with statutory statutory duties (e.g., safeguarding mandates, DfE censuses).
- Contractual Necessity: Necessary to fulfill or enter into a contract with an individual (e.g., employment contracts).
- Vital Interests: Critical processing required to protect an individual's life or safety.
- Consent: Freely given, specific, informed, and an unambiguous positive indication. For online information society services offered directly to pupils, parental consent is mandated for children under 13.
- Legitimate Interests: Relied upon only for non-public authority functions, provided individual freedoms override them.

8. DATA SUBJECT RIGHTS & SUBJECT ACCESS REQUESTS (SAR)

Individuals possess formal rights regarding their data: the right to be informed via transparent privacy notices, the right to rectification of inaccurate data, the right to erasure ('right to be forgotten'), the right to restrict processing, the right to data portability, and the right to object to processing.

Subject Access Request (SAR) Protocols

- Individuals can submit a SAR to gain a copy of their personal data to verify its lawfulness. Requests must be sent to the DPO at info@emersonparkacademy.org.
- Response Timeline: Handled without delay and at the absolute latest within 1 calendar month of receipt. For exceptionally complex or numerous requests, this may be extended by up to a maximum of 2 further months; the data subject must be formally notified within the original month with a justification.
- Fees: Information is supplied free of charge. However, if a request is manifestly unfounded, repetitive, or excessive, the Academy may charge a reasonable administrative fee or refuse to act. The data subject must be notified of their right to complain to the ICO within 1 month.
- Exemptions: The Academy will redact or withhold information if disclosure would cause serious harm to physical/mental health, compromise child safeguarding protections, reveal adoption or parental order data, or violate legal professional privilege.

9. PARENTAL REQUESTS & THE EDUCATIONAL RECORD

Personal data belongs to the child. A parent or carer may only make a SAR on behalf of their child if the child lacks capacity to understand their rights, or has granted express consent.

- Pupils Under 12: Generally presumed to lack sufficient maturity to understand data rights. SARs from parents or carers are typically granted without the explicit consent of the child, following a case-by-case capacity evaluation.
- Pupils Aged 12 and Over: Generally presumed mature enough to understand their rights. SARs submitted by parents/carers for children in this bracket will not be fulfilled without express permission from the pupil, unless special safeguarding or capacity metrics override this.
- Educational Record: Separate from a SAR, under the Education Regulations, parents possess a statutory right to view their child's official educational record free of charge within 15 school days of a written request.

10. STATUTORY COMPLAINTS TRACKING

To satisfy strict statutory transparency standards, the Academy enforces a formalized internal complaints log. If an individual believes their data rights have been infringed:

- They must submit a formal data protection complaint in writing to the Designated DPO.
- The DPO will record the complaint in the Academy's Central Data Protection Complaints Register, tracking the date, nature of the grievance, investigation parameters, and ultimate outcome.
- The Academy will deliver a formal internal review response within 30 days.
- Data subjects maintain an absolute right to escalate unresolved grievances directly to the Information Commissioner's Office (ICO) at any point, though the internal tracking process runs concurrently to ensure thorough organizational accountability.

11. PRIVACY NOTICE FOR PUPILS AND PARENTS

This section constitutes the text version of the Academy's Statutory Privacy Notice, written in plain language accessible to pupils and parents.

What Categories of Information We Collect and Hold:

- Personal identifiers and contact details (such as name, unique pupil number, contact details, and address).
- Characteristics and demographics (such as ethnicity, language spoken, and free school meal eligibility).
- Safeguarding and pastoral information (such as professional court orders, multi-agency case notes, and CPOMS records).
- Special educational needs (SEN) details (including evaluations, data profiles, and specific learning requirements).

- Medical and health infrastructure (such as physical health, mental health, dietary restrictions, and clinical alerts).
- Attendance and academic metrics (such as test scores, exam results, exclusions, and behavioral data).

Why We Collect and Use This Information:

We process pupil and parent data under the Public Task and Legal Obligation frameworks to fulfill our core statutory functions: supporting teaching and learning, monitoring and reporting on pupil progress, providing appropriate pastoral care, protecting vulnerable children (safeguarding), and assessing the overall quality of our services.

Who We Share This Information With:

We do not share data without appropriate justification. We routinely share data with the Department for Education (DfE) via statutory data collections, Local Authorities, the NHS and emergency medical teams, law enforcement bodies where required by law, and our secure verified cloud processors (such as SIMS and CPOMS) under strict data sharing agreements.

12. DATA SECURITY

- Confidential paper records must be maintained under lock and key within restricted-access storage cabinets or safe boxes. They must never be left unattended in general-access staffrooms or classrooms.
- All electronic endpoints and digital files must be encrypted, password-protected, or coded. Servers and core networks are backed up off-site automatically.
- Removable media and portable devices (laptops, USBs) containing personal data are strictly prohibited unless they are password-protected and fully hardware-encrypted.
- Staff and governors are strictly prohibited from using personal laptops or computers for Academy business. Any mobile phone endpoint used to access school infrastructure must maintain enterprise-grade security profiles.
- Emails containing sensitive or special category data must be password-protected or sent via secure encrypted mail clients. Bulk parental communications must be distributed via blind carbon copy (bcc).

13. DATA BREACH MANAGEMENT PROTOCOLS

A personal data breach involves any unauthorised security event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

- Immediate Reporting: Staff or data processors must immediately notify the DPO upon discovery of a confirmed or suspected breach.
- 72-Hour ICO Window: If a breach poses a risk to individual rights and freedoms, the DPO will formally report the incident to the ICO within 72 hours of identification.

- High-Risk Notification: If a data breach presents a severe, high-risk threshold to individual rights (e.g., identity theft, deep distress, or safeguarding exposure), the Academy will notify all affected data subjects directly and in writing without undue delay.
- Central Audit: Every single data breach, regardless of scale or reporting status, is recorded in the Central GDPR Audit Platform, tracking facts, causal links, remediation steps, and staff training updates.

14. CCTV AND SURVEILLANCE OPERATIONS

- The Academy operates internal and external closed-circuit television (CCTV) cameras to fulfill its statutory duty of care under health and safety legislation, protect property assets, deter crime/vandalism, prevent bullying, and ensure effective management.
- CCTV data constitutes personal data and is handled strictly under ICO video surveillance codes. Continuous performance monitoring of employees via CCTV is explicitly prohibited.
- Retention Limit: CCTV images are retained for a strict maximum period of 28 days, after which they are permanently overwritten, except where footage is preserved specifically for an ongoing formal legal investigation or prosecution.
- Disclosure Metrics: CCTV footage will only be released when authorised by the Headteacher/DPO after consultation with the Chair of Governors. Police requests must be made in writing, and the Academy will verify legal necessity or require formal warrants where appropriate.
- Notification & Signage: High-visibility, prominent signs are displayed at all entrances and near cameras, identifying the data controller and detailing the security and crime-prevention purposes of the recording.

15. AUTOMATED BIOMETRIC RECOGNITION SYSTEMS

The Academy operates an automated biometric recognition system (e.g., fingerprint scanning) solely for identification within the school catering and cashless cafeteria system. Biometric profiles are treated strictly as Special Category Data.

- Statutory Parental Consent: Under the Protection of Freedoms Act 2012, written consent from at least one parent or carer is mandatory prior to processing biometric data for any pupil under the age of 18. In no circumstances will data be captured without this.
- The Pupil's Absolute Right to Refuse: A pupil's objection or refusal to participate overrides parental consent. If a pupil refuses or parents object, the Academy must provide a reasonable alternative arrangement without any penalty. At Emerson Park Academy, students can access their catering accounts seamlessly by stating their full name to the operator at the till point.
- Data Deletion: Upon a pupil leaving the Academy, or if consent is formally withdrawn in writing, all associated biometric templates are immediately and permanently purged from the system database.

16. FREEDOM OF INFORMATION (FOI)

Emerson Park Academy fully complies with the Freedom of Information Act 2000. Members of the public, media, or organizations have a right to request access to recorded information held by the Academy.

- Timeline: The Academy will acknowledge requests and provide a complete response within 20 working days. If information is withheld under a legal exemption, a formal refusal notice explaining the public interest test will be issued within the same window.
- Data Formats: Where the requested data forms a distinct dataset, the Academy will provide it in an open, re-usable format (such as a CSV file) where practicable.
- Personal Data Boundary: FOI requests cover organizational and environmental information. Requests for personal data regarding the applicant or others will be completely excluded from FOI tracks and processed under strict DPA/UK GDPR Subject Access Request frameworks.

17. STORAGE, RETENTION, AND DISPOSAL OF RECORDS

- Retention Schedules: Personal and educational data are retained in accordance with statutory guidelines and the Academy's retention schedules. Data is never kept longer than necessary.
- Secure Disposal: Redundant physical documents are securely shredded or incinerated. Electronic records are permanently scrubbed, overwritten, or destroyed in full alignment with national technical standards and ICO guidance on IT asset disposal.
- DBS Data: Disclosure and Barring Service (DBS) certificates and tracking data are managed with the highest confidentiality. DBS certificate numbers are recorded securely, but copies of certificates are never duplicated or retained for longer than necessary to complete onboarding checks.

18. MONITORING, TRAINING, AND ARRANGEMENTS

- Mandatory Training: All staff members, members of the Senior Leadership Team (SLT), and governors are required to undergo comprehensive data protection training during induction, supplemented by mandatory annual refresher modules.
- Policy Review: The Designated DPO is responsible for reviewing and monitoring this policy every 2 years, or more frequently if required by legislative shifts, structural audits, or technological updates.

APPENDIX A: BIOMETRIC INFORMATION CONSENT FORM

Please complete and sign this form to indicate whether you consent to Emerson Park Academy storing data from your child's fingerprint profile for identification within the cashless school catering services.

In granting consent, you authorize the Academy to process this biometric data solely for this purpose until your child leaves the school. You retain an absolute right to withdraw consent at any time in writing.

[ ] I GIVE CONSENT for my child's fingerprint profile to be processed.

[ ] I DO NOT GIVE CONSENT for my child's fingerprint profile to be processed.

Pupil Name: _____

Parent/Carer Name: _____

Signature: _____ Date: _____

APPENDIX B: NON-DISCLOSURE AGREEMENT (NDA)

For use by casual staff, supply teachers, external contractors, and volunteers.

I understand that during my placement or work at Emerson Park Academy, I may have access to confidential or personal data regarding pupils, staff, parents, and contractors. I agree that:

- I will use this data strictly for authorised school purposes and maintain full confidentiality.
- I will not attempt to access systems without express authorisation.
- I understand that a breach of this confidentiality may result in immediate exclusion, civil prosecution, or criminal liability under the Data Protection Act and Computer Misuse Act 1990.

Name (Block Capitals): _____

Signature: _____ Date: _____

Authorised School Signature (DPO/Headteacher): _____