

Leicester Preparatory School

Data Protection Policy

Date: September 2026

Date to be reviewed: September 2027

DATA PROTECTION POLICY

1. Policy Statement

Stoneygate College (Leicester Preparatory School) Ltd, operating Leicester Preparatory School of which Berties nursery is part, is committed to protecting the personal information entrusted to it by pupils, parents and carers, employees, prospective families, visitors, contractors and other members of the School community.

The School recognises that appropriate handling of personal information is essential to safeguarding children, maintaining trust and meeting its legal and regulatory responsibilities.

The School will process personal information lawfully, fairly, transparently and securely and will maintain appropriate systems to demonstrate compliance.

This policy applies to all personal information processed by or on behalf of Leicester Preparatory School.

2. Legal Framework

The School will comply with applicable data protection and privacy legislation, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations (PECR), where applicable;
- applicable education and safeguarding legislation;
- applicable employment legislation;
- guidance issued by the Information Commissioner's Office (ICO);
- relevant Department for Education guidance.

The School will keep this policy under review when legislation or regulatory guidance changes.

3. Data Controller

The data controller for the majority of personal information processed by Leicester Preparatory School is:

Stoneygate College (Leicester Preparatory School) Ltd

The School determines:

- what personal information it needs;
- why it is collected;
- how it is used;
- who it is shared with;
- how it is protected;
- how long it is retained.

The School will maintain appropriate documentation to demonstrate accountability.

4. Data Protection Principles

The School will comply with the data protection principles.

Personal data must be:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and kept up to date where necessary;
5. kept only for as long as necessary;
6. processed securely;
7. managed in a way that enables the School to demonstrate compliance.

The School will also apply appropriate accountability measures to its data processing

5. Personal Data

Personal data means information relating to an identified or identifiable living individual.

Examples within a school include:

- names;
- addresses;
- telephone numbers;
- email addresses;
- dates of birth;
- pupil records;
- attendance;
- assessment information;
- behaviour records;
- photographs and videos;
- safeguarding records;
- medical information;
- financial information;
- employment records;
- CCTV footage;
- IT and online identifiers.

6. Special Category Data

Special category data requires additional protection.

This may include information concerning:

- health;

- medical conditions;
- allergies;
- disability;
- special educational needs;
- racial or ethnic origin;
- religious or philosophical beliefs;
- biometric information used for identification.

The School will only process special category information where an appropriate lawful basis and additional condition applies.

Access will be restricted to those who have a legitimate professional need.

7. Children's Personal Data

The School recognises that children require particular protection when their personal information is processed.

Children have their own data protection rights.

The School will therefore:

- consider children's age, maturity and understanding;
- use clear and age-appropriate explanations;
- minimise unnecessary collection of information;
- protect children's information from inappropriate disclosure;
- consider safeguarding implications when using photographs and videos;
- consider children's rights when responding to data protection requests;
- ensure staff understand their responsibilities.

The School will not assume that parents automatically control all of a child's data protection rights. The child's age, maturity, understanding and the nature of the request will be considered

8. Lawful Bases for Processing

The School will identify an appropriate lawful basis for each significant processing activity.

These may include:

Legal obligation

Where the School is required to process information by law.

Contract

Where processing is necessary to enter into or perform a contract.

Legitimate interests

Where processing is necessary for the legitimate interests of the School or another party and those interests are not overridden by the rights and freedoms of the individual.

Where appropriate, the School will document a Legitimate Interests Assessment.

Recognised legitimate interests

Where applicable under the Data (Use and Access) Act 2025, the School may rely on the recognised legitimate interests lawful basis where the relevant legal requirements are satisfied.

Consent

Consent may be used where appropriate.

Consent must be:

- freely given;
- specific;
- informed;
- unambiguous;
- recorded.

Consent must not be used where it is inappropriate because the School has another more suitable lawful basis.

Consent must be capable of being withdrawn.

Vital interests

The School may process information where necessary to protect someone's vital interests.

Public task

Where applicable, the School may rely upon public task where the relevant legal requirements are satisfied.

9. Criminal Offence Data

The School may process information relating to criminal convictions and offences where permitted by law.

This may arise particularly through safer recruitment, DBS checks, safeguarding and employment processes.

Such information will be handled securely and only where there is an appropriate lawful basis and condition.

10. Data Minimisation

The School will only collect personal information that is adequate, relevant and necessary for the purpose for which it is required.

Staff must not collect information simply because it might be useful in the future.

Where information is no longer required, it should be securely deleted or destroyed in accordance with the School's retention arrangements

11. Accuracy

The School will take reasonable steps to ensure that personal information is accurate and up to date.

Parents, pupils and staff should notify the School of relevant changes to:

- address;
- telephone number;
- email address;
- emergency contacts;
- medical information;
- other important personal information.

12. Security

The School will implement appropriate technical and organisational measures to protect personal information.

These may include:

- secure passwords;
- access controls;
- role-based permissions;
- multi-factor authentication where appropriate;
- encryption;
- secure cloud systems;
- antivirus and security measures;
- secure backups;
- locked storage;
- secure disposal;
- staff training;
- appropriate physical security.

Staff must:

- keep passwords confidential;
- lock devices when unattended;
- use School-approved systems;
- not share confidential information through personal accounts unless specifically authorised;

- take particular care when working remotely;
- report suspected breaches immediately.

13. Paper Records

Paper records containing personal information must be stored securely.

Confidential documents must not be left unattended in:

- classrooms;
- corridors;
- reception areas;
- meeting rooms;
- vehicles;
- open offices.

Confidential paper records must be securely destroyed when no longer required.

14. Email and Electronic Communication

Staff must check carefully before sending personal information by email.

They must verify:

- recipient;
- email address;
- attachments;
- information being disclosed;
- whether the disclosure is necessary;
- whether additional security is required.

Sensitive information should be transmitted using an appropriate secure method.

Where several parents or carers are emailed, staff should consider whether BCC should be used.

15. Sharing Personal Information

The School may share information where there is a lawful basis and the disclosure is necessary and proportionate.

Recipients may include:

- Department for Education;
- local authorities;
- safeguarding agencies;
- children's social care;

- health professionals;
- emergency services;
- examination and assessment bodies;
- other schools;
- professional advisers;
- insurers;
- accountants;
- payroll providers;
- pension providers;
- IT providers;
- educational software providers;
- contractors and service providers;
- regulatory bodies;
- law enforcement agencies where legally permitted or required.

Before sharing information, staff should consider:

1. Is there a lawful basis?
2. Is sharing necessary?
3. Does the recipient need all the information?
4. Is the recipient authorised?
5. Can the information be shared securely?

The School will not sell pupil or family personal information.

16. Safeguarding and Information Sharing

Data protection law does not prevent appropriate information sharing to safeguard children.

Where there is a safeguarding concern, staff must follow the School's Safeguarding and Child Protection Policy.

Information may be shared without consent where necessary and where permitted or required by law.

Staff must not delay necessary safeguarding action because they are uncertain about data protection.

The DfE specifically recognises the importance of appropriate information sharing in safeguarding contexts

17. Department for Education

The School may be required to provide information to the Department for Education and other statutory bodies.

This may include information relating to:

- pupil characteristics;

- attendance;
- assessments;
- educational outcomes;
- special educational needs;
- safeguarding;
- other statutory data collections.

Where information is required by law, parental consent will not normally be required.

The School will explain relevant DfE data sharing in its pupil and parent privacy notice

18. Photographs and Videos

The School may use photographs and videos for legitimate educational, safeguarding, administrative and communication purposes.

Different uses will be considered separately, including:

- internal School records;
- displays within the School;
- newsletters;
- School publications;
- website;
- social media;
- promotional material;
- press coverage.

Where consent is the appropriate lawful basis, consent will be obtained and recorded.

The School will consider safeguarding, privacy and the child's best interests before publishing identifiable images.

19. CCTV

Where CCTV is operated, it will be used for legitimate purposes including:

- security;
- safeguarding;
- protection of pupils, staff and visitors;
- prevention and investigation of incidents.

The School will:

- provide appropriate signage;
- restrict access;
- maintain appropriate security;
- retain footage for an appropriate period;
- respond to legitimate requests for footage;
- review the system periodically.

20. Filtering and Monitoring

The School may use filtering and monitoring systems to support:

- safeguarding;
- online safety;
- network security;
- appropriate use of School systems;
- prevention of harmful or inappropriate content.

Monitoring information will only be accessible to authorised staff.

The School will document:

- what is monitored;
- why it is monitored;
- who can access alerts or reports;
- retention arrangements.

Where a new or substantially changed filtering or monitoring system is introduced, the School will consider whether a Data Protection Impact Assessment is required. The school currently uses Senso Coud as its monitoring and filtering system.

Current DfE guidance specifically requires schools to explain filtering and monitoring activities in their privacy information.

21. Artificial Intelligence and Educational Technology

The School may use educational technology and artificial intelligence tools.

Before introducing new systems involving personal information, the School will consider:

- lawful basis;
- data minimisation;
- security;
- processor arrangements;
- international transfers;
- retention;
- children's rights;
- transparency;
- whether a DPIA is required.

Staff must not enter confidential or personal pupil information into unauthorised AI systems

22. Data Processors

The School may appoint third-party organisations to process personal information on its behalf.

Examples include:

- management information systems;
- cloud storage;
- email systems;
- accounting systems;
- payroll systems;
- HR systems;
- safeguarding systems;
- educational platforms;
- website providers;
- IT support;
- payment providers.

Appropriate contractual arrangements will be put in place where required.

Processors will only process information in accordance with the School's instructions and applicable law

23. International Transfers

The School will ensure that any transfer of personal information outside the UK complies with applicable data protection requirements.

Where appropriate, the School will use:

- adequacy regulations;
- appropriate safeguards;
- contractual protections;
- other lawful transfer mechanisms.

24. Retention

The School will not retain personal information for longer than necessary.

Retention periods will be determined by:

- legislation;
- regulatory requirements;
- safeguarding requirements;
- contractual requirements;
- financial requirements;
- operational requirements.

The School will maintain a Data Retention Schedule.

Records will be securely destroyed, deleted or anonymised when the retention period expires.

DfE guidance recommends that schools document retention arrangements and review what information they hold at least annually.

25. Data Subject Rights

Individuals have rights under data protection law, subject to applicable exemptions.

These include:

- right to be informed;
- right of access;
- right to rectification;
- right to erasure;
- right to restrict processing;
- right to data portability;
- right to object;
- rights relating to automated decision-making and profiling.

Not every right applies in every situation.

26. Subject Access Requests

A person may request access to their personal information verbally or in writing.

All potential Subject Access Requests must be referred promptly to the DPO.

DPO: Francis Fernandes
Email: f.fernandes@leicesterprep.co.uk

The School will:

- verify identity where necessary;
- locate relevant information;
- consider exemptions;
- protect information about other individuals;
- respond within the applicable statutory timeframe.

27. Personal Data Breaches

A personal data breach includes:

- loss or theft;

- accidental disclosure;
- sending information to the wrong person;
- unauthorised access;
- hacking;
- malware;
- loss of a device;
- accidental publication;
- inappropriate access by staff.

All suspected breaches must be reported immediately to the DPO.

The School will:

1. contain the breach;
2. establish what happened;
3. assess the risk;
4. record the breach;
5. determine whether the ICO must be notified;
6. determine whether affected individuals must be informed;
7. implement measures to prevent recurrence.

The School will maintain a Data Breach Register.

28. Data Protection Impact Assessments

The School will consider and undertake a DPIA where processing is likely to result in a high risk to individuals.

Examples include:

- new CCTV systems;
- biometric systems;
- significant monitoring systems;
- new technologies involving children's data;
- large-scale processing of sensitive information;
- profiling or automated decision-making.

29. Records of Processing Activities

The School will maintain a Record of Processing Activities (ROPA).

The ROPA will identify, where appropriate:

- processing purposes;
- categories of personal information;
- categories of data subjects;
- lawful bases;
- special category conditions;
- recipients;

- retention periods;
- security measures;
- international transfers;
- processors.

The DfE identifies the ROPA as an important means of demonstrating accountability.

30. Data Protection Officer

The School will appoint a Data Protection Officer where legally required and/or use an appropriately qualified data protection lead.

The DPO will:

- advise the School;
- monitor compliance;
- support staff training;
- advise on DPIAs;
- advise on breaches;
- cooperate with the ICO;
- act as a contact point for individuals and the ICO.

31. Staff Responsibilities

Everyone working for Leicester Preparatory School is responsible for protecting personal information.

Staff must:

- follow this policy;
- complete required training;
- keep information confidential;
- use approved systems;
- report breaches immediately;
- only access information needed for their role;
- not disclose information without authority.

Failure to comply may result in disciplinary action

32. Training

All staff will receive appropriate data protection training.

Training will cover:

- data protection principles;
- confidentiality;

- secure handling of pupil information;
- email security;
- passwords;
- breaches;
- information sharing;
- safeguarding;
- photographs;
- subject access requests;
- secure disposal;
- use of IT and AI.

Training will be refreshed periodically and records retained.

33. Complaints

Anyone concerned about how the School processes personal information should first contact the School.

Data Protection Officer: Francis Fernandes
Email: f.fernandes@leicesterprep.co.uk
Address: 2 Albert Road, Leicester, LE2 2AA

The School will maintain an appropriate complaints process and respond promptly.

Individuals also have the right to complain to the Information Commissioner's Office.

34. Policy Review

This policy will be reviewed at least annually and sooner if:

- legislation changes;
- ICO or DfE guidance changes;
- the School introduces new processing;
- a significant breach occurs;
- an audit identifies a weakness;
- there is a significant change in School operations.

Next review: August 2027