PRIORY SCHOOL
EDGBASTON

DATA PROTECTION

(STATUTORY)

Trustee Committee:	Risk & Compliance	
Date Approved:	November 2026	
Next of Review:	November 2027	
Member of Staff Responsible:	Nedal Al-Chamaa – Finance Director	
Trustee Overseer:	Stuart Brereton	
Intended Audience:	Options: Employees, Volunteers, Parents, Pupils and Visitors	
Relevance:	Whole School	Yes
	Early Years	No
	Preparatory	No
	Seniors	No
Access:	Website	Yes
	Internal	No
	Restricted	No

Our Mission Statement

Priory School is a thriving, co-educational independent school founded upon a rich Catholic heritage which welcomes those from all faiths and none.

In partnership with parents and guardians we provide a nurturing, family-based ethos, alongside high-standards of teaching and learning, enabling all pupils to achieve their potential.

We embrace diversity and interfaith understanding alongside awareness of environmental and global issues, in response to the needs of our time.

The Governors and staff at Priory School are committed to providing a fully accessible environment which values and includes all pupils, staff, parents and visitors, regardless of their education, physical, sensory, social, spiritual, emotional or cultural needs.

The Governors, staff and pupils are committed to the safeguarding and welfare of pupils and staff.

To meet the needs of our school community, all our policies, including this policy, can be made available on different formats such as different font sizes or styles, colour, or alternate languages.

The Governing Council understands it has responsibility for ensuring the effective oversight of this policy and will assess, evaluate and review as necessary.

Rationale

All schools process large amounts of "personal data" about current, past and prospective pupils, and their parents, carers and guardians. Under the Data Protection Act 2018 and UK GDPR the school must process such personal data "fairly". This includes telling pupils and parents how their personal data will be held and used by the school.

Please note, the Data (Use and Access) Act 2025 has been passed; this policy will be reviewed regularly to ensure updated guidance is appropriately reflected.

This Data Protection Policy is intended to help meet these legal requirements.

The School is required to process relevant personal data regarding pupils and their parents and guardians, staff, volunteers, contractors, Governors, and other data subjects as part of its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

This policy applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of personal data, including e.g., the school's policy on taking, storing and using images of children.

Anyone who works for, or acts on behalf of, the school (including staff, volunteers, governors and service providers) should also be aware of and comply with the school's data protection policy for staff, which also provides further information about how personal data about those individuals will be used.

In this Policy any reference to pupils includes current and past or prospective pupils.

GDPR – Privacy Notices

In accordance with GDPR, the data protection rights of parents, pupils, and staff are set out in a Separate Privacy Notice - which is published on the school's website.

Responsibility for Data Protection

In accordance with UK GDPR and DPA 2018, the school has notified the Information Commissioner's Office of its processing activities. The school's Information Commission registration number is Z5520548 and its registered address is 39 Sir Harry's Road, Edgbaston, Birmingham B15 2UR.

The School has a designated **Data Protection Officer (DPO)** (Mr Nedal Al-Chamaa) who is on the onsite contact and will endeavour to ensure that all personal data is processed in compliance with this Policy and with the Principles of GDPR and Data Protection Act 2018.

The school also works closely with - Shard Business Services to provide independent support and advice and the contact is Jo Cardwell (dpo@shardbusinessservices.co.uk)

The Governing Board has overall responsibility for overseeing data protection, monitoring compliance, and developing policies and procedures.

The headteacher acts as a representative of the school on a day-to-day basis.
All staff have a responsibility to comply with data protection legislation.

The Principles of Data Protection

The School shall so far as is reasonably practicable comply with the Data Protection Principles ("the Principles") contained in UK GDPR Article 5 to ensure all data is:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Personal Data

Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data of pupils, their parents or guardians as part of its operation. This personal data may include (but is not limited to); names and addresses, bank details, academic, disciplinary, admissions and attendance records, references, examination scripts and marks.

For a full list of personal data processed about a specific group, please refer to the school's suite of privacy notices

Processing of Personal Data

The school will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents;
- To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the school community.
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance.

- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils.
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school.
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips. To provide requested information to social services / related agencies/professionals to safeguard children effectively.
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT: acceptable use policy.
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's policy on taking, storing and using images of children. However, the School will not publish photographs of individual pupils with their names on the school website without the express agreement of the appropriate individual.
- For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

Lawful basis

There are 6 lawful bases identified in the UK GDPR. The School will only process personal data under the following:

a. The consent of the data subject has been obtained

b. Processing is necessary for a contract held with the individual, or because they have asked the School to take specific steps before entering into a contract

c. Processing is necessary for compliance with a legal obligation (not including contractual obligations)

d. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

e. Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone’s life

f. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

For special category data, the School must also meet an additional condition for processing, a full list of which is available here.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law, a full which of list is available here.

Where consent is used as a legal basis for processing, consent must be a positive indication and firmly expressed, and cannot be inferred from silence, inactivity, or pre-ticked boxes. Consent can be withdrawn at any time for any reason. Please contact reception to withdraw consent.

Sharing data

The School will only share personal data where there is a lawful basis to do so, and sharing is necessary and proportionate. For example, we will need to share information with our management information system in order to assist with our administrative duties.

Where permitted, personal data may be shared with:

- The Local Authority
- The Department for Education
- Safeguarding agencies
- Healthcare professionals
- External consultants and auditors
- Management information system and educational software

This list is not exhaustive.

We may also be required to share information with law enforcement and government bodies, including information required for the prevention/detection of a crime/fraud, to assist apprehension or prosecution of offenders, to assess tax owed to HMRC, or information required in connection with legal proceedings. Where required by law, we may share this information without consent.

Where the School engages third party processors, appropriate due diligence will be undertaken to ensure data protection and security risks are assessed and addressed and an appropriate Data Processing Agreement shall in place where required.

Keeping in touch and supporting the school

The school will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the school, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the school may also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the “Friends of Priory” and the Priory School Alumni organisation.
- Contact parents and/or alumni (including via the organisations above) by post and email in order to promote and raise funds for the school.

Should a parent or pupil wish to limit or object to any such uses, or obtain further information about them, they should advise the school through enquiries@prioryschool.net.

Special Category Data

The school may, from time to time, need to process "special category data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political opinions, religious beliefs, sex life, sexual orientation, trade union membership, genetic data, and biometric data. Special category data is entitled to further protection and will only be processed by the School where both a lawful basis under Article 6 of UK GDPR and a condition for processing under Article 9 UK GDPR or Schedule 1 of the DPA 2018.

Retention of Personal Data

The School will not retain personal data for longer than is required for the purposes for which it was collected, unless there is a legitimate reason to retain for a longer period, for example safeguarding reasons.

Records are disposed of in line with the Records Retention Schedule, which identifies how long specific categories of personal data are kept. This is determined in relation to UK GDPR and DPA 2018, the IRMS Toolkit, statutory limitation periods, and the operational needs of the school.

Paper records are securely destroyed in line with the retention schedule, and electronic records are securely deleted from school systems. Records shall not be retained by staff outside of approved and secure systems.

Rights of access to Personal Data (“Subject access request”)

Individuals have the right under UK GDPR and DPA 2018 to have access to personal data about them held by the school, subject to certain exemptions and limitations set out in the legislation. The School requests that any individual wishing to access their personal data should put their request in writing to the DPO.

The school will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within statutory time-limits, which is one calendar month. The School cannot typically charge for a request, unless a request is deemed unfounded or excessive, or additional copies of documents are required.

Subject access request should include the name of the data subject (or relationship to data subject if applicable), contact information, and details of the information requests.

The School may ask for photographic identification, where the requester is not known to the school, or may ask for a request to be clarified. The school may also extend the deadline by up to a further two months, where the request is deemed complex. The requester will be informed of this within one month of the request, and informed as to why an extension has been used.

Certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts (though examiners' comments may fall to be disclosed), nor any reference given by the school for the purposes of the education, training or employment of any individual, as all references given or received by the School are classed as confidential.

The School will also not disclose data where we believe it may cause serious harm to the physical or mental health of another individual or reveal that a child is a risk of abuse (where this disclosure is not in the interests of the child). The school will not share data where this is exempt under any exemptions found in the UK GDPR and Data Protection Act 2018.

If we refuse a request, we will inform the requester as to why and inform them of their right to complain to the Information Commission.

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. Pupils aged 12 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case-by-case basis.

If a pupil is deemed mature enough and a request is made on their behalf, pupil information will typically not be released without consent from the pupil.

A person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

Requests for pupil educational record

If a request is made under 'The Education (Pupil Information) (England) Regulations 2005', we are not obliged to fulfil this request, as this only applies to local authority schools and special schools. Independent schools, academies, and free schools are not obliged to respond to a request for access to a pupil's education record under this legislation. However, if we receive a request for a pupil's education record - we will treat the request as a subject access request and follow the School's procedure for this.

Other Rights of Individuals

In addition to the right of access (the right which allows an individual to make a subject access request), there are additional rights given to data subjects. These include:

- Withdrawing consent at any time
- Ask for data to be rectified, erased, or processing restricted, or object to the processing of it (in certain circumstances)
- Prevent their data from being used for direct marketing
- Object to decisions based solely on automated decision making or profiling
- Prevent processing likely to cause damage or distress
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the Information Commission.
- Ask for data to be transferred to a third party (in a commonly used format and in certain circumstances)

To exercise any of these rights, please contact the DPO.

Data accuracy and security

The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the School of any changes to information held about them via enquiries@prioryschool.net

An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the relevant legislation) and may do so by contacting enquiries@prioryschool.net

The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, for example by ensuring records are locked with limited access, and ensuring personal data is not shared with unauthorised people. All staff will be made aware of this policy and their duties under the relevant legislation.

Security measures include:

- Role-based permissions and access control
- Multi-factor authentication and strong password practice
- Encryption
- Secure and compliant backups
- Secure disposal of records and assets storing personal data

This list is not exhaustive.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the Surveillance Camera Code of Practice published for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the DPO.

Data Breaches

The School will take all reasonable steps to ensure there are no data breaches, including training staff, securing systems, and fostering a culture of awareness and caution.

Staff must immediately report any suspected data breach, including security incidents and loss of personal data.

In the event of a suspected data breach, the School will follow the Information Commission procedure set out in Appendix 1.

Where appropriate, we will report a data breach to the ICO within 72 hours and data subjects without undue delay. Breaches may be reported to the Information Comission and data subjects proactively, even if the threshold has not been met, as part of the school's approach to accountability.

Following a breach, an investigation will be undertaken to ensure that next steps are taken to prevent reoccurrence of similar breaches.

Record of Processing Activities

The School is required to maintain Records of Processing Activities. All members of staff are required to notify the relevant persons before they embark on any new processing activities so they can be adequately recorded on the RoPA, and the record will be reviewed periodically.

The ROPA will include, where relevant:

- Categories of personal data processed;
- Categories of data subjects;
- Purposes of processing;
- Lawful bases relied upon;
- Recipients of personal data;
- Details of international transfers;
- Data retention periods;
- Security measures applied to the processing.

Data Protection Impact Assessments

For certain types of processing or processing likely to result in a high risk to data subjects, the School will undertake a Data Protection Impact Assessment (DPIA). A DPIA is designed to help organisations analyse, identify, and minimise the data protection risk associated with specific processing.

This process will:

- Identify the purpose of processing
- Assess necessity and proportionality
- Identify risks to data subjects
- Consider mitigating measures where risks are identified
- Assess whether processing shall continue

Although a DPIA may not eliminate all risk, it assists in minimising this and determining whether the level of risk is acceptable.

Please see the Information Commission guidance for further information regarding DPIAs - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

Enforcement

If an individual believes that the School has not complied with this Policy or that it has acted otherwise than in accordance with the UK GDPR and Data Protection Act 2018, they should utilise the School Complaints Procedure, notifying the School in the first instance via enquiries@prioryschool.net

Complaints

To make a complaint regarding data protection, these can be submitted in line with the School's Complaints Policy.

You should include your name, contact details, a description of the issue, and any supporting evidence you wish to provide.

We will acknowledge your complaint within 30 days, and we will investigate without undue delay. In some cases, we may need to confirm your identity, and may also ask you to clarify your complaint, including what outcomes you would like. If your complaint is on behalf of another person, we will require evidence that you are authorised to act on the complainant's behalf. Any proof of identity or clarification required will be asked for at the earliest opportunity.

The investigation will be undertaken by an appropriate person such as the Data Protection Officer or Headteacher. The complaint will be investigated fairly and thoroughly, and without any bias. Where necessary, we will provide updates on the progress of the investigation, for example where an investigation is likely to take some time.

In response to a complaint, you will receive a written response, including findings, actions taken, and any remedy or apology offered. We will also provide you with information on how to escalate your complaint if you are unsatisfied with the outcome.

If you remain unhappy with the outcome of your complaint, you also have the right to complain to the Information Commission at https://ico.org.uk/make-a-complaint/

Training

All staff, governors, volunteers, and other individuals who have access to personal data on behalf of the School will receive appropriate data protection training, including information on their data protection responsibility, identifying and reporting breaches, recognising subject access requests, and handling data securely. Refresher training will be provided periodically.

Monitoring and review

This policy will be reviewed regularly and amended, as necessary, for any changes in legislation or other changes necessary for the efficiency and financial health of the school.

Appendix 1 – Personal Data Breach Procedures

This procedure is based on guidance on personal data breaches produced by the Information Commission.

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. So, a data breach has occurred if personal data has been lost, stolen, destroyed (accidentally or in error), altered (accidentally or in error), disclosed accidentally or in circumstances where it should not have been or otherwise made available to unauthorised people.

Step 1: On finding or having caused a data breach, staff members or third-party data processors must notify the Data Protection Officer immediately.

Step 2: The DPO must notify the Headteacher immediately when notified of a breach.

Step 3: The DPO will take all reasonable steps to contain the breach and minimise its effects as far as possible, requesting action from staff members and any third-party data processors that may be required.

- Can the data be retrieved or safely deleted/destroyed by any unintended recipient(s)?
- Are we certain we have identified all the data that was lost/mistakenly disclosed or altered etc?

Step 4: At the earliest possible time, the DPO will assess the potential consequences of the breach. The DPO should consider;

- How could it affect the data subject(s) involved?
- How serious will these effects be for the data subjects?
- How likely is it that the data subjects could be affected in this way(s)?

Step 5: The DPO must decide whether or not the breach must be reported to the Information Commission. Breaches must be considered on a case-by-case basis; however, a breach must be reported to the Information Commission if it is likely to result in any physical, material or non-material damage such as;

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation

- damage to reputation
- or any other significant economic or social disadvantage to the individual(s) concerned

If the breach is likely to affect anybody in any of the ways described above, and cannot be successfully contained or rectified, it must be reported to the Information Commission.

Step 6: The DPO will document the decision taken as to whether or not the Information Commission are notified of the breach. The school should keep a record of this decision in case it is challenged at a later date by any of the individuals involved or by the Information Commission. The school should keep a record of breaches whether or not they are reported to the Information Commission. This record should include:

- A description of the breach and how it occurred
- Details of the data involved
- A description of the potential consequences of the breach
- Details of how likely it is any individuals could be affected
- A description of measures taken to contain or rectify the breach
- Actions taken to avoid any repeat of errors that lead to the breach

Step 7: In cases where the breach must be reported to the Information Commission, the DPO (or another member of staff if they are not available) must do so within 72 hours of becoming aware of the breach. Such breaches are reported via the relevant page on the Information Commission's website.

Step 8: The DPO must decide whether or not the individual's affected by the breach must be notified. Again, the potential risks to any affected individuals (described in Step 5), the severity of any effects and the likelihood of them being affected must guide this decision-making process. If there is a high risk the DPO will notify, in writing, all potentially affected individuals. This notification will include:

- Contact details for the DPO
- A description of how the breach occurred and the data involved
- A description of the measures taken to contain or rectify the breach
- Any advice it is possible to provide in terms of how the individuals could be affected

Step 9: The DPO must ensure records of breaches and decisions taken relating to them are stored and accessible in the event of any subsequent investigation by the school or the Information Commission.