



Data Protection Policy

The Finance and General Purposes Committee is responsible for this policy

Last Reviewed: 1st September 2026

Purpose

Highfield Priory School and Nursery ("the School") is committed to protecting the privacy, confidentiality and security of the personal information entrusted to it by pupils, parents, staff, governors, volunteers, contractors and other members of the school community.

The School recognises that effective data protection is fundamental to maintaining trust, safeguarding individuals' rights and fulfilling its legal responsibilities. Personal data is processed only where necessary to support the School's educational, safeguarding, employment and operational functions.

This policy sets out how the School meets its obligations under data protection legislation and establishes the standards expected of everyone who processes personal data on behalf of the School.

Scope

This policy applies to:

- Governors
- Employees
- Agency workers
- Contractors
- Volunteers
- Students on placement
- External professionals working on behalf of the School
- Anyone processing personal information on behalf of Highfield Priory

It applies to all personal information regardless of format, including:

- paper records
- emails
- handwritten notes
- photographs
- CCTV images
- electronic files
- cloud-based storage
- databases
- audio recordings
- video recordings
- portable devices

Legislative Framework

This policy has been developed in accordance with:

- ✓ UK General Data Protection Regulation (UK GDPR)
- ✓ Data Protection Act 2018
- ✓ Data (Use and Access) Act 2025 (DUAA)
- ✓ The Data (Use and Access) Act 2025 amends and supplements the UK GDPR, Data Protection Act 2018 and PECR. The School will apply those requirements as amended and in force from 2026.
- ✓ Privacy and Electronic Communications Regulations (PECR)
- ✓ Human Rights Act 1998
- ✓ Freedom of Information Act 2000 (where applicable)
- ✓ Education legislation relating to the management of pupil records
- ✓ Relevant guidance published by the Information Commissioner's Office (ICO)

The School will also have due regard to guidance issued by the Department for Education, the Independent Schools Inspectorate and other relevant regulatory bodies where applicable.

Lawful Bases for Processing

The School will identify and document an appropriate lawful basis before processing personal data. Depending on the circumstances, this may include consent, contract, legal obligation, vital interests, public task or legitimate interests. Where applicable, the School may also rely on a recognised legitimate interest introduced by the Data (Use and Access) Act 2025 for a purpose specified in law, subject to the requirements and safeguards that apply.

Where special category data or criminal offence data is processed, the School will also identify an appropriate additional condition under the UK GDPR and Data Protection Act 2018.

Roles and Responsibilities

Governors

The Governing Board is responsible for ensuring that appropriate governance arrangements are in place to enable the School to comply with data protection legislation. This includes:

- approving this policy;
- receiving assurance regarding compliance;
- monitoring significant risks;
- ensuring sufficient resources are available to maintain compliance.

Headteacher

The Headteacher has overall operational responsibility for ensuring compliance throughout the School.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for:

- advising the School on compliance with data protection legislation;
- monitoring compliance;
- providing advice on Data Protection Impact Assessments (DPIAs);
- acting as the primary point of contact with the ICO;
- advising on data breaches;

- supporting staff with data protection matters;
- promoting awareness and training.

School Business Manager

The School Business Manager will support the implementation of this policy through the management of operational records, contracts, retention arrangements and information governance processes.

All Staff

Every member of staff is responsible for:

- protecting personal information;
- following this policy and associated procedures;
- reporting data breaches immediately;
- completing mandatory training;
- processing data only where authorised;
- maintaining confidentiality.

Information Security and Data Handling

Highfield Priory School and Nursery recognises that protecting personal data is fundamental to safeguarding individuals, maintaining trust and meeting its legal obligations. The School is committed to ensuring that all personal information is handled securely, responsibly and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and this policy.

Appropriate technical and organisational measures are implemented to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.

All members of staff are responsible for ensuring that personal information is handled securely at all times. Staff must:

- access personal information only where required for their role;
- only process personal data for legitimate school purposes;
- ensure information is accurate and kept up to date;
- keep paper records secure when not in use;
- lock computers when left unattended;
- use strong passwords and multi-factor authentication where provided;
- ensure confidential conversations cannot be overheard by unauthorised persons;
- securely dispose of confidential information using approved confidential waste arrangements;
- immediately report any actual or suspected data breach in accordance with the School's Data Breach Procedure.

Records Management

The School maintains records to support education, safeguarding, employment, finance and the effective operation of the School.

Records must be:

- accurate;

- relevant;
- appropriately classified;
- securely stored;
- readily retrievable where required;
- retained only for as long as necessary;
- securely destroyed when no longer required.

Staff must not retain duplicate records unnecessarily or maintain unofficial "shadow files" containing personal information.

Where information forms part of an official school record, it must be stored within the School's approved record management systems rather than solely within individual email accounts or personal folders.

The School's Data Retention Schedule (Appendix D) sets out the retention period for all categories of records.

Email and Electronic Communications

School email accounts are provided for official School business.

Users must exercise care whenever sending emails containing personal or confidential information.

Before sending an email, staff should:

- verify recipient addresses carefully;
- consider whether all recipients require the information;
- use blind carbon copy (BCC) where appropriate;
- minimise the amount of personal information shared;
- password-protect or encrypt attachments where appropriate;
- ensure the lawful basis for sharing information exists.

Personal information must never be sent to unauthorised recipients.

Where sensitive personal information is shared electronically, appropriate security measures must be used to protect confidentiality.

School email accounts remain the property of Highfield Priory School and Nursery.

When a member of staff leaves employment, their email account will normally be disabled immediately. The account and its contents may be retained for up to **six months** to facilitate operational continuity, retrieval of legitimate school records or to meet legal obligations, after which the account will be securely deleted unless there is a lawful reason for continued retention.

Safeguarding records must not be maintained solely within email accounts. Any safeguarding information received by email must be transferred promptly to the School's safeguarding recording system (CPOMS) and managed in accordance with the School's Safeguarding and Child Protection Policy.

Emails which form part of an official school record, including safeguarding records, complaints, disciplinary matters, contracts, personnel records and SEND documentation, must be transferred to the appropriate school record management system and retained in accordance with the School's Data Retention Schedule (appendix D)

Routine correspondence should not be retained indefinitely and will be managed in accordance with the School's records management procedures.

Portable Devices and Home Working

The School recognises that staff may occasionally undertake authorised work away from school premises. Where personal data is accessed or processed remotely, staff must ensure that:

- only School-approved devices are used unless expressly authorised;
- devices are password protected;
- devices are encrypted where appropriate;
- confidential information cannot be viewed by unauthorised persons;
- paper records are transported securely;
- information is not left unattended in vehicles or public places;
- confidential waste generated away from school is returned to school for secure disposal.

Personal information must never be stored permanently on personal devices.

Cloud Storage and Third-Party Systems

The School uses a range of secure cloud-based services to support teaching, learning and administration.

Before introducing any new system that processes personal data, the School will consider:

- the security of the system;
- the supplier's compliance with UK GDPR;
- contractual arrangements;
- data storage locations;
- international transfers;
- information security certifications;
- whether a Data Protection Impact Assessment (DPIA) is required.

Only systems authorised by the School may be used to store personal information. Staff must not upload School information to personal cloud storage accounts.

Data Processors

The School engages carefully selected third-party organisations ("data processors") to provide services on its behalf.

Examples include providers of:

- management information systems;
- payroll;
- educational software;
- online learning platforms;
- communication systems;
- IT support;
- payment systems.
-

Before sharing personal information with a processor, the School will ensure that:

- appropriate due diligence has been completed;
- a written Data Processing Agreement is in place where required;
- appropriate security measures are implemented;
- the processor only acts on the School's documented instructions.

The School remains responsible for ensuring that personal information processed by third parties is protected appropriately.

Artificial Intelligence (AI)

The School recognises that artificial intelligence (AI) technologies are increasingly used to support administration, education and productivity.

Any use of AI must comply fully with the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, safeguarding responsibilities, the School's AI Policy and the Acceptable Use Policy.

Staff must not enter confidential, personal or safeguarding information into publicly available AI tools unless:

- the system has been approved by the School;
- appropriate contractual safeguards are in place;
- the processing complies with UK GDPR;
- the information has been appropriately anonymised where required.

AI may be used to assist with drafting documents, lesson planning or administrative tasks where this does not compromise confidentiality or the rights and freedoms of individuals.

All significant decisions affecting individuals will continue to involve appropriate human oversight. For further information, refer to the School's AI policy.

Data Retention and Secure Disposal

The School will retain personal information only for as long as necessary to fulfil the purpose for which it was collected or where required by law.

Retention periods are detailed within the School's Data Retention Schedule (Appendix D).

At the end of the retention period, records will be securely destroyed or permanently deleted using methods appropriate to the type of information.

Secure disposal may include:

- confidential shredding;
- secure destruction by approved contractors;
- certified destruction of electronic media;
- secure deletion of electronic records;
- permanent removal from cloud storage where applicable.

The School will maintain appropriate records of secure destruction where required.

Data Sharing

The School recognises that the appropriate sharing of information is essential to safeguarding children, fulfilling its legal obligations and supporting the effective operation of the School.

Personal information will only be shared where there is a lawful basis to do so and where the sharing is necessary, proportionate and compatible with the purpose for which the information was collected.

Information may be shared with, but is not limited to:

- parents and carers;

- local authorities;
- safeguarding partners;
- health professionals;
- the police;
- the Department for Education;
- examination boards;
- regulatory bodies;
- professional advisers;
- insurers;
- third-party service providers acting on behalf of the School.

Before sharing personal information, the School will consider:

- the lawful basis for sharing;
- whether the information is necessary;
- whether the recipient has a legitimate need to know;
- whether the minimum amount of information is being shared;
- whether additional safeguards are required.

Information will not be shared with third parties for marketing purposes without an appropriate lawful basis.

Nothing within this policy prevents the lawful sharing of information where necessary to safeguard or promote the welfare of a child. Where safeguarding concerns exist, the safety and welfare of the child will take precedence, and information may be shared without consent where permitted or required by law.

Individual Rights

Under UK GDPR, individuals have a number of rights in relation to their personal information. The School is committed to ensuring these rights are respected and facilitated appropriately. These rights include:

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

These rights are not absolute and may be subject to exemptions or limitations provided by legislation.

Any request relating to an individual's data protection rights should be referred immediately to the Data Protection Officer (DPO).

Subject Access Requests

Individuals have the right to request confirmation that the School is processing their personal information and to obtain a copy of that information where appropriate. The School will respond to Subject Access Requests in accordance with UK GDPR and the Data Protection Act 2018.

Requests:

- do not need to refer to legislation;
- may be made in writing or verbally;
- will normally be responded to within one calendar month, calculated in accordance with current data protection law; may require reasonable identity information before the response period begins; may, where permitted by law, pause the response period while genuinely necessary clarification is sought from the requester; will require the School to carry out reasonable and proportionate searches for relevant personal information.
- are generally free of charge.

Where permitted by legislation, the School may:

- request proof of identity;
- seek clarification of the information requested;
- extend the response period where requests are particularly complex or numerous;
- refuse manifestly unfounded or excessive requests;
- charge a reasonable administrative fee where permitted by law.

Detailed guidance is contained within the School's Subject Access Request Procedure – Appendix E.

Data Protection Impact Assessments (DPIAs)

The School recognises that some processing activities present a higher risk to the rights and freedoms of individuals. Where required by UK GDPR, a Data Protection Impact Assessment (DPIA) will be undertaken before introducing new systems, technologies or processing activities that are likely to result in a high risk to individuals.

Examples may include:

- new management information systems;
- biometric technologies;
- large-scale CCTV developments;
- monitoring technologies;
- artificial intelligence systems;
- significant changes to existing processing activities.

The DPO will advise on whether a DPIA is required and will monitor the implementation of appropriate safeguards.

Privacy by Design and Default

The School is committed to embedding data protection into all new projects, systems and working practices. Privacy considerations will form part of planning and decision-making from the earliest stages of any project involving personal information.

The School will ensure that:

- only the minimum personal information necessary is collected;
- access is restricted to those who require it;
- security measures are considered from the outset;
- retention periods are identified;
- risks are assessed before implementation;
- appropriate safeguards are incorporated into new processes.

Personal Data Breaches

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. Examples include:

- sending personal information to the wrong recipient;
- loss or theft of paper records;
- phishing attacks;
- ransomware;
- cyber attacks;
- unauthorised access to systems;
- accidental deletion of records;
- loss of encrypted or unencrypted devices;
- inappropriate disclosure during conversations.

All actual or suspected breaches, regardless of severity, must be reported immediately to the Data Protection Officer and School Business Manager. The School will:

- investigate all reported breaches;
- assess the level of risk;
- take appropriate action to minimise harm;
- notify the Information Commissioner's Office where required;
- notify affected individuals where legally required;
- maintain a breach register;
- review incidents to identify learning and improve practice.

Detailed procedures are contained within the School's Data Breach Procedure.

International Transfers

Where personal information is transferred outside the United Kingdom, the School will ensure that the transfer complies with the UK GDPR as amended by the Data (Use and Access) Act 2025. The School will assess whether the destination provides a standard of protection that is not materially lower than the protection provided under UK data protection law and will put appropriate safeguards in place where required. This may include:

- adequacy regulations;
- the UK International Data Transfer Agreement (IDTA);
- approved contractual clauses;
- other lawful transfer mechanisms recognised under UK GDPR.

The School will ensure that any third-party suppliers processing personal information internationally provide an appropriate level of protection for that information.

Training and Awareness

The School recognises that effective data protection depends upon knowledgeable and well-informed staff. All staff will receive appropriate data protection training:

- as part of their induction;
- at regular intervals thereafter;
- whenever significant changes to legislation or School procedures occur.

Training will be proportionate to an individual's role and responsibilities and may include:

- information security;
- confidentiality;
- recognising and reporting data breaches;
- records management;
- safeguarding information sharing;
- cyber security awareness;
- use of artificial intelligence;
- handling Subject Access Requests.

The School will maintain records of staff training and may provide additional guidance or refresher training where required.

CCTV

Highfield Priory operates a Closed-Circuit Television (CCTV) system to support the safety, security and welfare of pupils, staff, volunteers, visitors and the School premises. The use of CCTV is carried out in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and current guidance issued by the Information Commissioner's Office (ICO).

The School is the **Data Controller** for all personal data processed through its CCTV system. The CCTV system is used only where it is necessary and proportionate to achieve one or more of the following legitimate purposes:

- safeguarding pupils, staff, volunteers and visitors;
- helping to prevent and detect crime and anti-social behaviour;
- protecting School buildings, property and equipment;
- supporting the investigation of accidents, safeguarding concerns, disciplinary matters and other incidents;
- assisting with the management of health, safety and site security.

The School does not use CCTV for any commercial purpose and does not routinely undertake covert surveillance. All fixed cameras are clearly visible, appropriate signage is displayed around the site and cameras are positioned to minimise intrusion into areas where individuals would reasonably expect privacy. The School will ensure that:

- CCTV is used only where it is necessary and proportionate;
- appropriate signage informs individuals that CCTV is in operation;
- access to live images and recorded footage is restricted to authorised personnel only;
- CCTV recordings are stored securely and protected from unauthorised access;
- recordings are retained only for the period specified in the School's Data Retention Schedule unless required for an ongoing investigation or legal proceedings;
- requests for access to CCTV footage are managed in accordance with UK GDPR, the Data Protection Act 2018 and the School's procedures for responding to Subject Access Requests and other lawful disclosures.

The CCTV system operates independently of the School's main network. Recorded footage is stored securely on a dedicated server located in a locked secure area. Access to the CCTV management software is limited to authorised devices and authorised personnel with appropriate administrative permissions. Where footage is temporarily copied for the purposes of an investigation, it will be stored securely and managed in accordance with this Policy and the School's Data Retention Schedule (Appendix D).

1	Entrance from In Drive	15	Main Entrance Nursery
---	------------------------	----	-----------------------

2	Front of School Parking	16	Nursery Courtyard
3	Exit Drive Entrance	17	Playground Nursery
4	Electric Gate	18	Playground Preschool
5	Entrance Hall and Reception	19	Preschool Courtyard
6	Playground 1 and 2	20	Plantroom External
7	Main Car Park	21	Back of Preschool
8	Infant Quad Playground	22	Back of Nursery
9	Side Staff Car Parking	23	WC Exit
10	Extended Side Staff Car Park	24	Main Entrance External
11	Rear Staff Car Parking	25	Nursery Courtyard 2
12	Early Years Play Area	26	Nursery Courtyard 3
13	Sports Pitch	27	Playground Nursery 2
14	IP Dome		

Further operational arrangements for CCTV, including authorised access, disclosure, retention, maintenance and Subject Access Requests, are governed by this Data Protection Policy, the Data Retention Schedule and the School's security procedures. A separate CCTV policy is not relied upon unless one is formally adopted by the School.

Photography, Video and Images

The School recognises the importance of celebrating pupils' achievements whilst protecting their privacy and safeguarding their welfare. Photographs and video recordings may be taken for educational, safeguarding, identification and promotional purposes where there is an appropriate lawful basis for processing. The School will:

- provide clear information to parents regarding the use of images;
- respect any recorded preferences regarding photography where appropriate;
- ensure images are stored securely;
- use photographs responsibly and proportionately;
- avoid unnecessary identification of pupils in published materials;
- regularly review storage arrangements for digital images.

Staff must only use School-approved devices and systems when taking, storing or sharing images of pupils. Images must never be stored on personal devices or uploaded to personal cloud storage accounts.

Staff must not send photographs of pupils via email unless this has been expressly authorised and appropriate encryption or other approved security measures are in place. All pupil images must be stored only on approved School systems, such as secure SharePoint servers or authorised encrypted storage devices. Portable storage devices, including memory cards, must be securely stored when not in use.

Where images are taken for safeguarding purposes, they will be managed in accordance with the Safeguarding and Child Protection Policy.

Further requirements are contained within this Data Protection Policy, the School's Acceptable Use Policy, e-Safety Policy and Safeguarding and Child Protection Policy. A separate Photography and Images Guidance document is not relied upon unless one is formally adopted by the School.

Website, Cookies and Online Services

The School's website processes limited personal information through its online services. Where cookies or similar technologies are used, the School will comply with the Privacy and Electronic Communications Regulations (PECR) and applicable data protection legislation.

The School will:

- provide clear information regarding the use of cookies;
- obtain consent where required by PECR, recognising that current law permits limited categories of cookies or similar technologies without consent where the relevant statutory conditions are met;
- explain the purpose of cookies through its website privacy information;
- provide users with appropriate choices regarding non-essential cookies.

Where third-party services are used through the School website, appropriate contractual and security arrangements will be maintained.

Further information is available within the School's Website Privacy Notice.

Children and Online Services

Where the School provides or commissions an online service that is likely to be accessed by children, the School will take the needs and rights of children into account when deciding how personal information is used. Privacy and security controls will be designed and reviewed with children's age, understanding and vulnerability in mind, in line with data protection by design and current ICO guidance.

Where educational technology or other online services are procured, data protection, safeguarding, security, age-appropriateness, supplier terms and the need for a DPIA will be considered before implementation.

Monitoring Compliance

The School is committed to maintaining effective information governance and continually improving its data protection arrangements.

Compliance with this policy will be monitored through:

- regular policy reviews;
- internal audits;
- data protection impact assessments;
- breach monitoring;
- staff training records;
- information security reviews;
- governor oversight;
- external advice where appropriate.

Any identified areas for improvement will be addressed through the School's compliance programme.

Roles of Governors

The Governing Board has overall responsibility for ensuring that effective arrangements are in place to support compliance with data protection legislation.

Governors will:

- approve this policy and any significant revisions;
- receive appropriate assurance regarding compliance;
- oversee strategic information governance;
- monitor significant risks;
- receive reports on serious data breaches where appropriate;
- ensure sufficient resources are available to support compliance.

The Finance and General Purposes Committee has delegated responsibility for monitoring the implementation of this policy.

Complaints

Individuals who have concerns regarding the way the School processes personal information should raise these with the Data Protection Officer in the first instance. The School will investigate all concerns promptly and fairly. Where an individual remains dissatisfied, they may make a complaint to the Information Commissioner's Office (ICO). Nothing within this policy affects an individual's statutory rights under data protection legislation.

Related Policies and Procedures

Individuals who have concerns about the way the School processes their personal information may make a data protection complaint to the School. The School will facilitate the making of complaints, including by providing an accessible electronic route for submitting them. Complaints will be referred to the Data Protection Officer and logged.

The School will acknowledge a data protection complaint within 30 days, investigate it appropriately, keep the complainant informed of progress where necessary, and communicate the outcome without undue delay.

Complainants are encouraged to raise the matter with the School first so that it has an opportunity to investigate and resolve the concern. This does not affect an individual's right to complain to the Information Commissioner's Office (ICO) or to exercise any other legal right or remedy.

Related Policies and Procedures

This policy should be read alongside the following documents:

- Acceptable Use Policy
- Artificial Intelligence (AI) Policy
- Bring Your Own Device (BYOD) Policy
- Confidentiality Policy
- Cyber Awareness Plan and Cyber Emergency Plan
- Data Breach Procedure
- Data Retention Schedule (Appendix D)
- Safeguarding and Child Protection Policy (including information-sharing arrangements)
- Privacy Notices
- Records management arrangements and Data Retention Schedule (Appendix D)
- Safeguarding and Child Protection Policy
- Subject Access Request Procedure (Appendix E)
- Visitor Privacy Notice
- Website Privacy Notice

Authority

The Full Board of Governors, by delegation to sub-committees, is responsible for formulating the policies and procedures that will ensure the school continue to achieve the aims of the overall school strategy. Hence, each sub-committee has Terms of Reference and assigned responsibility for policies within that scope. The sub-committees are: Audit and Compliance Committee, Education Committee, Finance and General Purposes Committee, Health, Safety and Wellbeing Committee, Safeguarding and Child Protection Committee and Sales and Marketing Committee.

Appendix A – Key Data Protection Principles

Everyone processing personal information on behalf of the School must ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- retained only for as long as necessary;
- processed securely using appropriate technical and organisational measures.

The School also recognises its accountability under UK GDPR and will be able to demonstrate compliance with these principles.

Appendix B – Key Responsibilities of Staff

Every member of staff is expected to:

- maintain confidentiality;
- protect personal information;
- follow School policies and procedures;
- complete mandatory data protection training;
- report suspected data breaches immediately;
- use School systems appropriately;
- challenge poor information handling practices where appropriate;
- seek advice whenever uncertain.

Failure to comply with this policy may result in disciplinary action and, where appropriate, referral to external authorities.

Appendix C – Definitions

Personal information (or personal data) - Any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.

Special Category Data - Personal information requiring additional protection under Article 9 UK GDPR, including information concerning health, ethnicity, religion, biometric data and other protected categories.

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

Data controller - An organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.

Data processor - An organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.

Processing - Virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

Special categories of personal data – Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

Appendix D – Data Retention Schedule

Where litigation, an insurance claim, a safeguarding investigation, an employment dispute, an Information Commissioner's Office (ICO) investigation or other legal proceedings are ongoing or reasonably anticipated, records must not be destroyed, even where the normal retention period has expired. Disposal should be suspended until the matter has been concluded.

Record Description	Category	Retention Period	Disposal Action
Governors' Minutes	Governance	Permanent	Archive
Annual Governors' Reports	Governance	Permanent	Archive
Headteacher's Log Books	Governance	Permanent (or archive if of historical value)	Archive
SMT Minutes	Governance	10 years	Secure Disposal
Professional Development Plans	Staff Development	6 years after superseded	Secure Disposal
School Development Plans	Governance	10 years	Secure Disposal
Staff Sign-In Book	Administration	3 years	Secure Disposal
Appointment of Staff Files (Unsuccessful Applicants)	Recruitment	6 months	Secure Disposal
Staff Personnel File	Employment	6 years after employment ends	Secure Disposal
Child Major Accident File	Health & Safety	Date of Birth + 25 years	Secure Disposal
Staff Accident File	Health & Safety	6 years from date of incident*	Secure Disposal
Hazardous Substance (COSHH) Records	Health & Safety	40 years	Secure Disposal
Primary Pupil File	Pupil Records	Date of Birth + 25 years	Secure Disposal

Record Description	Category	Retention Period	Disposal Action
Child Protection Information	Safeguarding	Date of Birth + 25 years	Secure Disposal
SEND Files	SEND	Date of Birth + 25 years	Secure Disposal
Attendance Registers	Pupil Records	6 years	Secure Disposal
School Trip Consent Forms (No Incident)	Educational Visits	End of the academic year	Secure Disposal
School Trip Records (Where an Accident Occurred)	Educational Visits	Date of Birth + 25 years	Secure Disposal
Inspection Reports	Governance	Permanent	Archive
Policies (Current and Superseded)	Governance	Current version plus superseded versions retained for 10 years	Secure Disposal / Archive where appropriate
Alumni File	Alumni	Review 25 years after pupil leaves the School	Secure Disposal
Staff Meeting Minutes	Governance	10 years	Secure Disposal
Headteacher Correspondence	Governance	Review after 10 years (archive where appropriate)	Secure Disposal / Archive
Timesheets	Payroll	7 years	Secure Disposal
Appraisal Records	Employment	6 years after employment ends	Secure Disposal
Allegations Against Staff	Safeguarding / Employment	Until normal retirement age or 10 years from conclusion of the allegation (whichever is longer)	Secure Disposal
SEND Correspondence	SEND	Date of Birth + 25 years	Secure Disposal
School Visit Risk Assessments	Health & Safety	3 years after the visit (or Date of Birth + 25 years if linked to an accident involving a pupil)	Secure Disposal

Appendix E - Subject Access Request (SAR) Procedure

I. Purpose

This appendix explains how Highfield Priory School and Nursery will manage Subject Access Requests (SARs) under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

The School is committed to responding to requests promptly, fairly and transparently while protecting the rights of all individuals whose information it holds.

II. What is a Subject Access Request?

A Subject Access Request is a request made by an individual seeking confirmation that the School processes their personal data and requesting access to that information.

A request:

- does not need to mention UK GDPR;
- does not need to use the words "Subject Access Request";
- may be made verbally or in writing;
- may be submitted by email, letter or in person.

All requests should be treated seriously and referred immediately to the Data Protection Officer (DPO).

III. Who Can Make a Request?

Requests may be made by:

- current or former pupils;
- parents or those with parental responsibility (where appropriate);
- current or former employees;
- governors;
- volunteers;
- applicants;
- any other individual whose personal information is held by the School.

Where a request relates to a child, the School will consider the child's age, maturity, understanding and best interests before deciding whether information should be disclosed.

IV. Receiving a Request

Any member of staff receiving a request for personal information must:

- immediately notify the Data Protection Officer;
- avoid promising immediate disclosure;
- preserve any relevant records;
- keep the request confidential.
- Where necessary, the School may request information reasonably required to confirm identity. The statutory response period will be calculated from the latest point specified by current data protection law, including receipt of any identity information reasonably required.

V. Timescales

The School will normally respond within one calendar month of receiving:

- the request; and
- any identification reasonably required.

Where requests are particularly complex or numerous, the response period may be extended by up to a further two months. The requester will be informed of the extension within the initial one-month period.

VI. Information Provided

Where appropriate, the School will provide:

- confirmation that personal data is processed;
- a copy of the relevant personal data;

- the purposes for processing;
- categories of personal data;
- recipients or categories of recipients;
- retention periods where possible;
- details of the individual's rights;
- information about the right to complain to the Information Commissioner's Office (ICO).

VII. Exemptions

The right of access is not absolute.

The School may withhold or redact information where permitted by law, including where disclosure would:

- reveal personal data relating to another individual;
- prejudice the prevention or detection of crime;
- breach legal professional privilege;
- disclose confidential references where an exemption applies;
- compromise safeguarding responsibilities;
- place another individual at risk of harm.

Each request will be considered individually.

VIII. Requests Relating to Pupils

When responding to requests concerning pupils, the School will carefully consider:

- parental responsibility;
- the child's age and understanding;
- whether disclosure is in the child's best interests;
- safeguarding considerations;
- any relevant court orders.

Where necessary, legal advice may be sought.

IX. Refusing a Request

The School may refuse a request where permitted by UK GDPR, including where it is:

- manifestly unfounded;
- manifestly excessive;
- repetitive without reasonable justification.

Any refusal will explain:

- the reasons;
- the right to complain to the ICO;
- the right to seek a judicial remedy.

X. Record Keeping

The Data Protection Officer will maintain a confidential log of all Subject Access Requests, including:

- date received;
- requester;
- identity verification (where required);
- actions taken;
- response date;
- exemptions applied;
- outcome.

This log forms part of the School's accountability obligations.