HORLEY INFANT SCHOOL

DATA PROTECTION POLICY

Initially Approved On:	**Autumn 2019**
Reviewed On:	**Autumn 2019**
Staff Link:	**Jason Walters**
Next Review Date:	**Summer 2020**

Policy Status					
Statutory ✓	Non-Statutory (Work Programme)	Non-Statutory	Annual Review ✓	Bi-annual Review	Triennial Review

FGB Review (statutory/work programme policies only):	**Resources**
Link Governor (statutory/work programme policies only):	**Edward Oakes**

In order to minimize inconsistencies, discrepancies or inaccuracies within information, our school's Data Protection Policy is comprised of information from the following policies within separate sections:

- Data Protection Policy
- The school's compliance within GDPR guidelines
- Freedom of Information
- Biometric Data Policy
- Privacy Notice
- Appendices related to Data Protection

Contents

1. Aims

Our school 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 the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Mr Derek Mann and is contactable via Derek.Mann@caps-ltd.co.uk.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner

- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data through our induction packs and privacy notices.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- Will ask the requester to complete the Subject Access Request form in Appendix 2.
- Will ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request. (*Please note whilst we will make every effort to respond within one month, this may not be possible during times of school holidays when the school is closed.)*
- Will provide the information free of charge where it is reasonable to do so
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances

- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers various uses of photographs/videos throughout their child's time within school.

Uses may include:

- Within school on notice boards and in newsletters, etc.
- Outside of school by external agencies such as the newspapers
- Online on our school website

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will ensure the photograph is only used for what consent has been gained for or what is classed as a legitimate interest of the school.

When using photographs and videos in promotional/marketing, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our E-Safety and Acceptable Use Policy for more information on our use of photographs and videos.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online Safeguarding Policy and our Acceptable Use Policy.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full governing board.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of Information Policy (embedded within this policy)
- Biometric Data Policy (embedded within this policy)
- Privacy Notice (embedded within this policy)
- Online Safeguarding Policy
- Acceptable Use Policy
- Child Protection and Safeguarding Policy

HORLEY INFANT SCHOOL

FREEDOM OF INFORMATION PUBLICATION

(to be embedded within the Data Protection policy)

Initially Approved On:	**Autumn 2019**
Reviewed On:	**Autumn 2019**
Staff Link:	**Jason Walters**
Next Review Date:	**Summer 2020**

Policy Status					
Statutory ✓	Non-Statutory (Work Programme)	Non-Statutory	Annual Review ✓	Bi-annual Review	Triennial Review

FGB Review (statutory/work programme policies only):	**Resources**
Link Governor (statutory/work programme policies only):	**Edward Oakes**

Freedom of Information Publication Scheme

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- To specify the information which is held by the authority and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.

Classes of Information

Who we are and what we do.

- Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.

- Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.

- Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions

Our policies and procedures.

- Policy proposals and decisions.
- Decision making processes, internal criteria and procedures, consultations.
- Current written protocols for delivering our functions and responsibilities.

Lists and Registers.

- Information held in registers required by law and other lists and registers relating to the functions of the authority.

The Services we Offer

- Advice and guidance, booklets and leaflets, transactions and media releases.
- A description of the services offered.
- The classes of information will not generally include:
    - ❖ Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.

- ❖ Information in draft form.
- ❖ Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

- The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.
- Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.
- In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.
- Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.
- Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for Information published under this scheme

- The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum.
- Material which is published and accessed on a website will be provided free of charge.
- Charges may be made for information subject to a charging regime specified by Parliament.
- Charges may be made for actual disbursements incurred such as:
  - ❖ photocopying
  - ❖ postage and packaging
  - ❖ the costs directly incurred as a result of viewing information

- Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.
- If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Written Requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

Information to be published	How the information can be obtained	Cost
Class 1 - Who we are and what we do (Organisational information, structures, locations and contacts) This will be current information only	(hard copy and/or website)	
Who's who in the school	Prospectus (hard copy/website)	
Who's who on the governing body and the basis of their appointment	Prospectus (hard copy/website)	
Instrument of Government	Hard copy/website	
Contact details for the Head teacher and for the governing body (named contacts where possible with telephone number and email address (if used))	School contact information on website/Hard copy	
School prospectus	Hard copy/website	
Annual Report - Governors	Hard copy/website	
Staffing structure	Hard copy/website	
School session times and term dates	Hard copy/website	

Class 2 – What we spend and how we spend it (Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit) Current and previous financial year as a minimum	Hard copy	
Annual budget plan and financial statements	Hard copy	
Capitalised funding	Hard copy	
Additional funding	Hard copy	
Procurement and projects	Hard copy	
Pay policy	Hard copy/website	
Staffing and grading structure	Hard copy	
Governors' allowances - policy	Hard copy/website	

Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews) Current information as a minimum	Hard copy/website	
School profile • Government supplied performance data • The latest Ofsted report - Summary - Full report	N/a Hard copy/website Hard copy/website	

Performance management policy and procedures adopted by the governing body.	Hard copy/website	
Schools future plans	Hard copy/website	
Every Child Matters – policies and procedures	Hardy copy/website	

Class 4 – How we make decisions (Decision making processes and records of decisions) Current and previous three years as a minimum	(hard copy or website)	
Admissions policy/decisions (not individual admission decisions)	Hard copy/website/SCC website	
Agendas of meetings of the governing body and (if held) its sub-committees	Hard copy/website	
Minutes of meetings (as above) – nb this will exclude information that is properly regarded as private to the meetings.	Hard copy on request	

Class 5 – Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities) Current information only	Hard copy/website	
School policies including: • Charging and remissions policy • Health and Safety • Complaints procedure • Staff conduct policy • Discipline and grievance policies • Staffing structure implementation plan • Information request handling policy • Equality and diversity (including equal opportunities) policies • Staff recruitment policies	Hard copy/website	
Pupil and curriculum policies, including: • Home-school agreement • Curriculum • Sex education • Special educational needs • Accessibility • Race equality • Collective worship • Careers education • Pupil discipline	Hard copy/website	
Records management and personal data policies, including: • Information security policies • Records retention destruction and archive policies • Data protection (including information sharing policies)	Where applicable, hard copies by request	
Charging regimes and policies.	Prospectus/website	

This should include details of any statutory charging regimes. Charging policies should include charges made for information routinely published. They should clearly state what costs are to be recovered, the basis on which they are made and how they are calculated.		

Class 6 – Lists and Registers Currently maintained lists and registers only	Hard copy/website. Some information may only be available by inspection	
Curriculum circulars and statutory instruments	DfE website	
Disclosure logs	By inspection	
Asset register	By inspection	
Any information the school is currently legally required to hold in publicly available registers (THIS DOES NOT INCLUDE THE ATTENDANCE REGISTER)	By inspection	

Class 7 – The services we offer (Information about the services we offer, including leaflets, guidance and newsletters) Current information only	Hard copy/website, some information may only be available by inspection	
Extra-curricular activities	Hard copy/website	
Out of school clubs	Hard copy/website	
School publications	Hard copy/website	
Services for which the school is entitled to recover a fee, together with those fees	Hard copy/website	
Leaflets books and newsletters	Hard copy/website	

Additional Information This will provide schools with the opportunity to publish information that is not itemised in the lists above		

Contact details: Headteacher, 01293 782263 or email info@horley.surrey.sch.uk

SCHEDULE OF CHARGES

This describes how the charges have been arrived at and should be published as part of the guide.

TYPE OF CHARGE	DESCRIPTION	BASIS OF CHARGE
Disbursement cost	Photocopying/printing @ 10p per sheet (black & white)	Actual cost *
	Photocopying/printing @ 20p per sheet (colour)	Actual cost
	Postage	Actual cost of Royal Mail standard 2nd class
Statutory Fee		In accordance with the relevant legislation (quote the actual statute)

* the actual cost incurred by the public authority

HORLEY INFANT SCHOOL

BIOMETRIC DATA POLICY

(to be embedded within the Data Protection policy)

Initially Approved On:	**Autumn 2019**
Reviewed On:	**Autumn 2019**
Staff Link:	**Jason Walters**
Next Review Date:	**Summer 2020**

Policy Status					
Statutory ✓	Non-Statutory (Work Programme)	Non-Statutory	Annual Review ✓	Bi-annual Review	Triennial Review

FGB Review (statutory/work programme policies only):	**Resources**
Link Governor (statutory/work programme policies only):	**Edward Oakes**

Table of Contents

Key Points

Horley Infant School does not currently collect biometric data of pupils. However, if biometric data is to be collected in the future, all related policies would be updated and the following guidance followed:

- Schools and colleges that use pupils' **biometric data** must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations (GDPR) 2018.

- Where the data is to be used as part of an **automated biometric recognition system,** schools and colleges must also comply with the additional requirements in sections 26 to 28 of the **Protection of Freedoms Act 2012**.

- The school must ensure that each parent of a child is notified of the school's intention to use the child's **biometric data** as part of an automated biometric recognition system.

- The written consent of at least one parent must be obtained before the data is taken from the child and used ie, **'processed'**. This applies to all pupils in schools and colleges **under the age of 18.** In no circumstances can a child's biometric data be processed without written consent.

- Schools and colleges must not process the biometric data of a pupil (under 18 years of age) where:

    a) The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

    b) No parent has consented in writing to the processing; or

    c) A parent has objected in writing to such processing, even if another parent has given written consent.

- Schools must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

1. What is biometric data?

1.1 *Biometric data* means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.

1.2 The Information Commissioner considers all biometric information to be sensitive personal data as defined by the **GDPR 2018**; this means that it must be obtained, used and stored in accordance with that Regulation.

1.3 The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR 2018.

2. What is an automated biometric recognition system?

2.1 An *automated biometric recognition system* uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order

to recognise or identify the individual.

2.2 Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1.1 above.

3. What does processing data mean?

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

a) Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) Storing pupils' biometric information on a database system; or

c) Using that data as part of an electronic process**,** for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

Frequently Asked Questions

What information should schools provide to parents/pupils to help them decide whether to object or for parents to give their consent?

Any objection or consent by a parent must be an informed decision – as should any objection on the part of a child. Schools should take steps to ensure parents receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

What if one parent disagrees with the other?

Schools will be required to notify each parent of a child whose biometric information they wish to collect/use. If one parent objects in writing, then the school will not be permitted to take or use that child's biometric data.

How will the child's right to object work in practice – must they do so in writing?

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case the school will not be permitted to collect or process the data.

Are schools required to ask/tell parents before introducing an automated biometric recognition system?

Schools are not required by law to consult parents before installing an automated biometric recognition system. However, they are required to notify parents and secure consent from at least one parent before biometric data is obtained or used for the purposes of such a system. It is up to schools to consider whether it is appropriate to consult parents and pupils in advance of introducing such a system.

Do schools need to renew consent every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be

overridden, at any time if another parent or the child objects to the processing (subject to the parent's objection being in writing). When the pupil leaves the school, their biometric data should be securely removed from the school's biometric recognition system.

Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using iris or retina scanning, then schools will have to meet the notification and consent requirements for the new system.

Can consent be withdrawn by a parent?

Parents will be able to withdraw their consent, in writing, at any time. In addition, either parent will be able to object to the processing at any time but they must do so in writing.

When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a pupil objects, the school must not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

Will consent given on entry to primary or secondary school be valid until the child leaves that school?

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent. If any such objection is made, the biometric data should not be processed and the school must, in accordance with the GDPR, remove it from the school's system by secure deletion.

Can the school notify parents and accept consent via email?

Yes – as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

Will parents be asked for retrospective consent?

No. Any processing that has taken place prior to the provisions in the Protection of Freedoms Act coming into force will not be affected. Any school wishing to continue to process biometric data must have already sent the necessary notifications to each parent of a child and obtained the written consent from at least one of them before continuing to use their child's biometric data.

Does the legislation cover other technologies such a palm and iris scanning?

Yes. The legislation covers ***all*** systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems which use palm, iris or face recognition, as well as fingerprints.

Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools must continue to comply with the requirements in the GDPR 2018 when using CCTV for general security purposes or when using photographs of pupils

as part of a manual ID system or an automated system that uses barcodes to provide services to pupils. Depending on the activity concerned, consent may be required under the GDPR before personal data is processed.

The Government believes that the GDPR requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems, where a pupil's photo is scanned automatically to provide them with services, would come within the obligations on schools and colleges under sections 26 to 28 of the Protection of Freedoms Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Is parental notification or consent required if a pupil uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school. If a school wishes to use such software for school work or any school business, then the requirement to notify parents and to obtain written consent will apply. However, if a pupil is using this software for their own personal purposes then the provisions do not apply, even if the software is accessed using school equipment.

Associated Resources

- ICO guide to data protection
- ICO guidance on data protection for education establishments
- British Standards Institute guide to biometrics

HORLEY INFANT SCHOOL

PRIVACY NOTICE

(to be embedded within the Data Protection policy)

Initially Approved On:	**Autumn 2018**
Reviewed On:	**Autumn 2019**
Staff Link:	**Jason Walters**
Next Review Date:	**Summer 2020**

Policy Status					
Statutory ✓	Non-Statutory (Work Programme)	Non-Statutory	Annual Review ✓	Bi-annual Review	Triennial Review

FGB Review (statutory/work programme policies only):	**Resources**
Link Governor (statutory/work programme policies only):	**Edward Oakes**

HORLEY INFANT SCHOOL

Lumley Road, Horley, Surrey RH6 7JF
Tel: 01293 782263 Fax: 01293 822425
Email: info@horley.surrey.sch.uk Web: www.horley.surrey.sch.uk
Headteacher: Mr Jason Walters

Privacy Notice (for pupils)

We, Horley Infant School are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about you from your previous school and the Learning Records Service.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as Early Year Profile, Phonics screening check, Standardised Assessment Tasks)
- Relevant medical information (such as allergies)
- Special Educational Needs information (such as multi-professional team assessments, Educational Health Care Plans (EHCP)
- Exclusions/behavioural information (such as exclusion documentation, bullying, racial incidents)
- Photographs

Why we collect and use this information

We use the pupil data:
to support pupil learning
to monitor and report on pupil progress
to provide appropriate pastoral care
to assess the quality of our services
to comply with the law regarding data sharing
to protect pupil welfare

The lawful basis on which we use this information

We are required by law, to provide information about our pupils to the Department for Education (DfE) as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the National Pupil Database (NPD). The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

If you need more information about how the Local Authority and DfE store and use your information, go to:

NPD – www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information
DfE – for information about the departments data sharing process – www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information (and for which project) please visit the following website – www.gov.uk/government/publications/national-pupil-database-requests-received

To contact the DfE – www.gov.uk/contact-dfe

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

Please refer for further information to the School website www.horley.surrey.sch.uk for all pupil data which is created during the time a pupil spends at Horley Infant School. We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We follow the guidance in the *Information and Records Management Society's toolkit for schools* for how long we keep information about pupils.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- the National Health Service
- the School Nurse
- the Multi-Professional Team (such as Educational Psychologist, Learning and Language Support Teachers)

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so. Where it is legally required or necessary (and it complies with data protection law) we may also share personal information about pupils with:

- The pupil's family and representatives – to meet our legal obligations to share certain information with it, such a progress and attainment and additional learning support

- Our regulator, Ofsted, to meet our legal obligations to share certain information with it such a pupil attainment, safeguarding records
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations – to meet our legal obligations to share certain information with it such as the delegated budget
- Central and local government – to meet our legal obligations to share certain information with it such as progress and attainment data
- Health authorities – to meet our legal obligations to share certain information such as safeguarding concerns
- Security organisations - to meet our legal obligations to share certain information such as safeguarding concerns
- Health and social welfare organisations - to meet our legal obligations to share certain information such as safeguarding concerns
- *Professional advisers and consultants* - to share certain information with it such as progress and attainment data
- Police forces, courts, tribunals - meet our legal obligations to share certain information such as safeguarding concerns
- Professional bodies - to share certain information with it such as progress and attainment data

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census. Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research. The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards. The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data. For more information, see the Department's webpage on how it collects and shares research data. You can also contact the Department for Education with any further questions about the NPD.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them. Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer.

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please complete the Subject Access Request form and return to the school office.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our administrative team who may refer it to our DPO if necessary.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Headteacher:

Mr. J Walters (info@horley.surrey.sch.uk)

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored electronically in a file held on the school's admin computer & in a paper file held in the School Office
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored in a file held on the school's admin computer & in a paper file in the School Office
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- Care will be taken to ensure that no pupil premium interventions for named children are published on the school website. The pupil premium information required to be published on the school website will be shared with the DPO prior to publication to ensure there are no breached.
- The clerk/DPO will have sight of any data/documents to be shared with governors and will be able to check that any information on results is anonymized
- *Staff are aware they should not store any personal data on their laptops. They will have direct password-protected access to the school server for storage of data. Staff must also only store personal data on an encrypted USB stick (the IT technician can encrypt memory sticks if required)*

HORLEY INFANT SCHOOL

Lumley Road, Horley, Surrey RH6 7JF
Tel: 01293 782263 Fax: 01293 822425
Email: info@horley.surrey.sch.uk Web: www.horley.surrey.sch.uk
Headteacher: Mr Jason Walters

Subject Access Request Form

(An editable version of this form is located on our website in the GDPR section)

Part A: Information about a Subject Access Request (SAR)

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school/academy holds about them, and can make a Subject Access Request (SAR). The Data Controller within school has been designated as the person who will coordinate the response to a SAR; they may also liaise with other school staff and the school's Data Protection Officer (DPO). The requestor will be asked to complete this form and can return it either electronically to the email address above or by handing it to the school office.

The school is required to provide the individual with the data it holds on them within one calendar month. An extension of up to one calendar month can be granted if a school closure period is scheduled to occur during the initial one calendar month response time.

The response to the SAR will either be provided in an electronic form or through a hard copy; typically the information will be provided free of charge. However, there may be a cost if there is a large amount of data to be collated. The requester will be informed of this at the earliest opportunity and the school does not need to complete the request until the fee has been received. Similarly, the school can refuse to comply with a request which is manifestly unfounded or excessive.

We may ask the requester to be more specific about the information that is required in order to ensure that the information they are provided with meets their requirements rather than providing lots of information that may not be relevant to their query. Evidence of the identity of the person making the request and their relationship to the pupil must be gained prior to any disclosure of information. This should be recorded on the SAR Log by a member of school staff.

Part B: Data Subject's Details (person whose information you are requesting)

Title & Full Name	
Date of Birth	
Address	
Year Group (if pupil at school)	

Please turn over

Part C: Requestor Details

Title & Full Name	
Address	
Phone number	
Email address	
Status of requester	☐ Data Subject ☐ Parent or person with parental responsibility ☐ Other (please detail):
Preferred format of information requested	☐ Paper copy (please note there ***may*** be a charge for this) ☐ Electronic format (please provide an encrypted memory stick) ☐ Email (this will be sent to the email address above)

All requesters must provide two types of proof of photo ID alongside this request as well as when collecting e.g. passport / driving license. Copies can either be sent in electronically and will be deleted/shredded once checked or shown to school staff and 'ticked off' when handing this form in.

Part D: Requestor Details

Details of data being requested (please be as specific as possible with regards to the dates, content and types of data that is being requested)	

Part E: Declaration

Please complete either Section A **or** Section B	
Section A	Section B
I hereby request that Horley infant School provide the data requested about me.	I hereby request that Horley Infant School provide the data about the data subject in Part B on the basis of the authority that I have
Name/data subject: Signature: Date:	Name/requester: Child/data subject: Signature: Date:

Part F: To be completed by school staff

☐ ID 1 checked when receiving SAR	Staff member:	Date:
☐ ID 2 checked when receiving SAR	Staff member:	Date:

Appendix 3 – Storing Pupil Data

Basic File Description	Operational / Retention Period Where stored	Action at end of administration life
Pupils Educational Records		
Pupils Educational Record required by the Educational (Pupil Information)(England) Regulations 2005	Retained while child is at Horley Infant School Headteacher's office	The file should follow the pupil to: - Another school - Pupil referral unit - If a pupil dies the file should be returned to the Local Authority - Transfer to an independent school/home schooling/ leaves country – file to Local Authority - Signature of receipt required
Examination Results		
e.g. SATs EYFS, Phonic Screening	Information added to pupil's blue file – Headteacher's office Composite record for comparison to be kept for current year plus 3 years (Attic)	The file should follow the pupil to: - Another school - Pupil referral unit - If a pupil dies the file should be returned to the Local Authority Transfer to an independent school/home schooling/ leaves country – file to Local Authority
Child Protection		
Child Protection information held on pupil file	Blue file should have a white sticker to indicate a CP file (Headteacher's office) Retained while child in School, transferred in a double envelope by hand where practicable signature of receipt required	The file should follow the pupil to their next school

Child Protection information held in separate file	Records kept by HSLW retained while child at Horley Infant School (locked filing cabinet) Records kept by Secondary School until child is 25 years old	Secure disposal
Attendance		
Attendance Registers	Entry data kept for three years after date entry made (Attic)	Secure disposal
Correspondence relating to authorised absence	Current academic year plus 2 years (Attic)	Secure disposal
Special Educational Needs		
Special Educational Needs – files, reviews, individual education plans	Date of birth of child plus 25 years (retained on blue pupil file) (Headteachers office)	The file will follow the pupil. This is the minimum retention period. (Some LAs keep for longer to defend themselves against "failure to provide a sufficient education case".)
Statement maintained under Section 234 of the Education Act 1990 and any amendments made to the statement (EHCP)	Date of birth of child plus 25 years (retained on blue pupil file) (Headteachers office)	Secure disposal unless subject to a legal hold
Advice and information provided to parents regarding educational needs	Date of birth of child plus 25 years (retained on blue pupil file) (Headteachers office)	Secure disposal unless subject to a legal hold
Accessibility Strategy - for individual pupil	Date of birth of child plus 25 years (retained on blue pupil file) (Headteachers office)	Secure disposal unless subject to a legal hold
Curriculum Management		

Curriculum Returns	Current Year plus 3 years	Secure disposal
Published Admission Number (PAN) reports	Current Year plus 6 years	Secure disposal
Value added and contextual data	Current year plus 6 years	Secure disposal
Self-evaluation forms	Current year plus 6 years	Secure disposal
Implementation of the Curriculum		
Schemes of Work	Current year plus 1	Review records at end of each year and allocate a further retention period or secure disposal
Timetables	Current year plus 1	
Class record books	Current year plus 1	
Mark books	Current year plus 1	
Record of homework set	Current year plus 1	
Pupils' work	Where possible pupils work should be returned to the pupil at the end of the academic year, at most plus 1	Secure disposal
Childrens' Photographs	Current year plus 3 years	Secure disposal – delete
Extra-Curricular Activities		
Records relating to Educational visits outside the classroom	Date of visit plus 14 years	Secure disposal
Parental consent forms for school trips where there has been no major incident	Conclusion of trip	Requirement is low for retention Secure disposal
Parental consent forms for a school trip where there has been a major incident	Date of Birth of pupil plus 25 years. Retain to ensure rules followed by all pupils	Secure disposal
Walking Bus Registers	Date of register plus 3 years – takes account of incident accident reporting	Secure disposal Electronic back up destroyed

Home School Link Worker		
Day Books	Current year plus 3 years then review	Secure disposal
Reports from outside agencies – on case file	Whilst child in school – pass on to next school	Secure disposal
Referral forms	While referral is current	Secure disposal
Contact data sheets	Current year – review - destroy if contact no longer needed	Secure disposal
Contact database entries	Current year, review, destroy if no longer needed	Secure disposal
Group registers	Current year plus 2 years	Secure disposal
Central Government and Local Authority		
Common Transfer forms (CTF)	Current year plus 2 years	Secure disposal
Attendance Returns	Current year plus 1	Secure disposal
School census returns	Current year plus 5	Secure disposal