



EDGBASTON HIGH SCHOOL

Data Protection and Privacy Notice

Edgbaston High School complies with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. All staff have a part to play in ensuring the School complies with its legal obligations in respect of personal data, whether that personal data is sensitive or routine. The School ensures that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The UK GDPR sets out seven key principles for processing personal data:

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

Rationale

Data protection is an important legal issue for Edgbaston High School. This Notice is intended to provide information about how Edgbaston High School will collect, store and process personal information about individuals including:

- Current, past and prospective Staff and Governors
- Current, past and prospective pupils
- Parents, carers or guardians (referred to in this policy as "parents")
- Contractors and third party suppliers
- Visitors

This information is provided in accordance with the rights of individuals under Data Protection Law to understand how their data is used. Staff, parents and pupils are all encouraged to read this Privacy Notice and understand the school's obligations to its entire community.

This Privacy Notice applies alongside any other information the school may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This Privacy Notice also applies in addition to the school's other relevant terms and conditions and policies, including:

- any contract between the school and its staff or the parents of pupils;
- the school's policy on taking, storing and using images of children;
- the school's document retention schedule;
- the school's safeguarding, pastoral and health and safety policies, including as to how concerns or incidents are recorded; and

- the school's IT policies.

Anyone who works for, or acts on behalf of, the school (including staff, volunteers, governors and service providers) should also be aware of and comply with the information in this document.

Linked Policies

All staff have a responsibility to handle the personal data with which they come into contact fairly, lawfully, responsibly and securely and in accordance with the following School policies and procedures:

- Data Breach Management Policy
- Safeguarding Policy
- Taking and storing images of children Policy
- Document retention schedule
- Health and Safety Policy
- Social media guidelines
- eSafety Policy
- CCTV Policy
- Code of Conduct

Objectives

- To protect the rights, safety and welfare of individuals in relation to the use of personal data at the school;
- To help employees of the school understand what is required under data protection law; and
- To help employees understand their role in data compliance.

Success Criteria

- Staff understand that data protection is the responsibility of everyone
- Staff understand that data is protected in accordance with data protection law

Responsibility for Data Protection

Data Controller	Edgbaston High School
Headmistress	Mrs C Macro
Chair of Governing Body	Mr M Chitty
Data Protection Lead	Ms C Gregory

Personal Data

In order to carry out its ordinary duties to staff, pupils and parents, the school may process a wide range of personal data as part of its daily operation. Some of this activity the school will need to carry out to fulfil its legal rights, duties and obligations - including those under contract with its staff, parents or pupils. Other uses of personal data will be made in accordance with the school's legitimate interests or the legitimate interests of another. (Appendix A)

Special Category Data

In addition, the school may need to process special category personal data or criminal records information in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required (Appendix B).

The categories of sensitive data the school collects, processes and stores are listed in Appendix C.

We do not need consent if we use special categories of personal data in accordance with this written Privacy Notice to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach individuals for consent to allow us to process certain particularly sensitive data. If we do so, we will provide full details of the information that is required and the reason it is needed, so that individuals can carefully consider whether they wish to consent.

Lawful Bases for Processing Data

Processing Activity	Article 6 Basis	Article 9 Basis (if applicable)
Employment records	Legal obligation	Employment/social protection
Safeguarding	Legal obligation/public task	Substantial public interest
Medical information	Legal obligation/legitimate interests	Health or vital interests
Catering biometrics	Consent	Explicit consent

Collecting Personal Data

In most cases the school receives personal data from the individual directly (or sometimes in the case of pupils from their parents or teachers). This may be via a form or during ordinary communication (conversation, email etc.) However, in some cases, information may be supplied from third parties for example:

- Other educational establishments (previous schools, universities)
- Previous employment
- Regulatory bodies such as the Disclosure and Barring Service
- Occupational Health, NHS and Public Health agencies
- Children's Services
- Examination Boards

When the school collects personal data, if necessary a Data Protection Impact Assessment (DPIA) carried out and documented to ensure data protection risks are minimised.

Whom do we Share Personal Data with?

We routinely share personal data with:

- other educational establishments (pupils attend after leaving EHS)
- appropriate members of staff within the school (including relevant pastoral and academic information)
- Universities and Colleges Admissions Service (UCAS)
- Centre for Evaluation and Monitoring (CEM) at University of Durham
- third party software providers (WCBS, RM, Office 365, Evolve, educational applications)
- the local authority
- the Department for Education (DfE)
- the Governors of the school
- Examination boards
- Occupational Health services
- NHS services such as immunisation and public health reporting
- Regulatory bodies such as the Disclosure and Barring Service
- HM Revenue and Customs (HMRC)
- Payroll bureau

- Independent Schools Inspectorate (ISI)

Occasionally, the school will need to share personal information relating to its community with third parties, such as professional advisers (lawyers, accountants, HR advisors), debt collectors or relevant authorities (police or the LADO/local authority).

For the most part, personal data collected by the school will remain within the school, and will only be processed by appropriate individuals (i.e. on a 'need to know' basis). Particularly strict rules of access apply to special category data, for example:

- medical records
- pastoral or safeguarding files
- personnel files

Staff, pupils and parents are reminded that the school is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the school's Safeguarding Policy.

Finally, in accordance with Data Protection Law, some of the school's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

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

International Transfers of Personal Data

The School primarily stores and processes personal data within the United Kingdom. However, some of our third party service providers may process personal data outside the UK, including in countries that may not provide the same level of data protection as UK law.

Where personal data is transferred outside the UK, the School will ensure that appropriate safeguards are in place in accordance with UK data protection law. These safeguards may include:

- Transfer of personal data to countries that have been recognised by the UK Government as providing an adequate level of protection for personal data;
- The use of the UK International Data Transfer Agreement (IDTA) or the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses;
- Contractual obligations requiring service providers to implement appropriate technical and organisational security measures; or
- Other lawful transfer mechanisms permitted under UK data protection legislation.

The School uses a number of cloud-based systems and educational technology providers, including RMuNify, Microsoft 365, Cisco, MyConcern and other approved software applications. Where these providers process personal data outside the UK, the School undertakes appropriate due diligence and seeks assurances that personal data will be protected to standards equivalent to those required under UK data protection law.

Individuals may obtain further information about the safeguards applied to international transfers by contacting the Data Protection Lead using the details provided in this Notice.

Storing Personal Data

The school will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Details of the length of storage can be found in the document retention schedule (Appendix D).

Keeping in Touch and Supporting the School

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

- Share personal data about alumnae as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the EHS Parents' Association and the Laurels Association (alumnae).
- Contact alumnae (including via the organisations above) by post and email to promote and raise funds for the school and, where appropriate, other worthy causes.
- Should you wish to limit or object to any such use, or would like further information about them, please contact Mrs Emma Cove, Head of Marketing and Communications in writing. You have the right to object to processing carried out on the basis of legitimate interests and to opt out of direct marketing at any time.
-

Members of the Laurels Association have been contacted directly about communication preferences and details of this will be available on the OGA section of the school website.

Data Accuracy and Security

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

An individual has the right to request that any inaccurate or out-of-date information about them is erased or corrected (subject to certain exemptions and limitations under Act): please see above.

The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this Notice and their duties under Data Protection Law and receive relevant training. All staff are aware of the need to report any data breaches to the Data Protection Lead who will act accordingly. For details of the management of data breaches see the breach management policy.

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/guidance/complete-the-school-census>.

Requesting Access to your Personal Data

Under data protection legislation, pupils, parents and staff have the right to request access to information about them that we hold. To make a request for your personal information (subject access request), or be given access to your child's educational record, please contact Ms Corinna Gregory in writing: DataProtectionOfficer@edgbastonhigh.co.uk.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed, transferred to other organisations; and
- claim compensation for damages caused by a breach of the Data Protection regulations

The school will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time limits, which is one month in the case of requests for access to information. The school will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the school may ask you to reconsider or charge a proportionate fee, but only where Data Protection Law allows it.

You should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts, nor any confidential reference given by the school for the purposes of the education, training or employment of any individual.

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. While a person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child's by law. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf, and moreover (if of sufficient age) their consent or authority may need to be sought by the parent. Pupils aged 13 are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Children younger than 13 may be sufficiently mature to have a say in this decision. All subject access requests from pupils will therefore be considered on a case by case basis.

Where the school is relying on consent to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the school may have another lawful reason to process the personal data in question even without your consent.

In general, the school will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school may be under an obligation to maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example where the school believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Queries and Complaints

If you have a concern about the way we are collecting or using your personal data, you should raise your concern in writing to Ms Corinna Gregory in the first instance.

If you believe that the school has not complied with this Notice or acted otherwise than in accordance with Data Protection Law, you should utilise the school complaints procedure and should also notify the Headmistress. The Information Commissioner's Office (ICO) (www.ico.org.uk), can also be contacted, although the ICO recommends that steps are taken to resolve the matter with the school before involving

the regulator.

Monitoring

It is the responsibility of the Headmistress, Chair of Governors and Data Protection Lead to ensure this policy is implemented in compliance with data protection law. The Data Protection Lead maintains an audit of data used within the school and reviews it in conjunction with the IT network manager. Any questions should in the first instance, be referred to the Data Protection Lead.

Evaluation

It is the responsibility of all employees to evaluate the effectiveness of this Notice and employees should not be afraid to question current or old practices or raise any concerns with the Data Protection Lead.

Review

This Notice will be reviewed every two years by the HR and Compliance Officer.

Signed by the Headmistress:

CAMayo

Approved by
The Governing Body

Approved by the Governing Body:

Date:

10/12/24

Review date:

November 2026

Appendix A

Legitimate interests of the school

The School processes personal data where it is necessary for our legitimate interests in operating and managing the school, supporting pupils, maintaining security, communicating with parents and alumni, administering school activities, and protecting the welfare of pupils and staff, provided that such interests are not overridden by the rights and freedoms of the individuals concerned.

- For the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents);
- To provide education services and timetables, including musical education, physical training or spiritual development, career services, and extra-curricular activities to pupils;
- To monitor pupils' progress and educational needs;
- To fulfil safeguarding duties and provide appropriate pastoral care for pupils, in accordance with statutory guidance such as *Keeping Children Safe in Education (KCSIE)*;

To ensure the health and safety of pupils, parents, staff and visitors; To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;

- To maintain up-to-date contact with pupils, parents and staff including a database of emergency contacts;
- To communicate news and notifications to the school community;
- To maintain relationships with alumni, including direct marketing or fundraising activity;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- To enable relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's policy on taking, storing and using images of children;
- For the purposes of Safer Recruitment of new and prospective staff as well as staff training, including the training of student teachers and assessment of newly qualified teachers;
- To assist with disciplinary or grievance proceedings;
- To assist in civil litigation, including employment tribunal proceedings;
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT: acceptable use policy;
- For security purposes, including CCTV in accordance with the school's CCTV policy and Legitimate Interests Assessment;
- To maintain records of visitors to the site; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional and legal advice and insurance for the school and employees.

Appendix B

Special Category Data

The following data are processed for pupils and staff at our School, for the purposes of education, safeguarding, pastoral care, health and safety, human resources management and equality monitoring:

Health Data

- Medical conditions
- Allergies
- Disabilities
- SEND information
- Medication requirements
- Mental health information
- Dietary requirements linked to health needs
- Occupational Health referrals and absence monitoring
- Making reasonable adjustments
- Complying with Health and Safety obligations

Racial or ethnic origin

- Ethnicity data
- Nationality-related information

Religious or philosophical beliefs

- Faith affiliation
- Requests for religious observance
- Dietary requirements connected to religion

Biometric data

- Fingerprint recognition – the School uses a biometric recognition system to enable pupils to access the cashless catering service. The system stores an encrypted biometric template derived from a pupil's fingerprint and does not store an image of the fingerprint itself. Biometric templates will be retained only for as long as the pupil remains enrolled at the School and continues to use the service. Explicit parental consent procedures are in place to allow pupils to use this system. This is compliant with the Protection of Freedoms Act 2012 (Part 1 Chapter 2).
- Whilst the CCTV system captures video and still images of faces, this is not processed via specific technical processing to uniquely identify someone therefore it is not classes as biometric data.

Trade union membership

- Staff trade union membership

Data concerning sexual orientation

- Equality monitoring
- Welfare or safeguarding records
- Staff HR processes

Reasons for collecting special category data

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's

interests to do so: for example for medical advice, social services, insurance purposes or to organisers of school trips;

- To provide education services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;
- To ensure all health and safety obligations are met for all staff, pupils and visitors;
- In connection with safer recruitment and continuing employment of its staff, for example DBS checks, welfare or pension plans; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

Appendix C

The categories of personal data that we collect, store and process

Pupils, Parents and Staff:

- Personal contact details information (such as name, address, telephone number, email address)
- Characteristics (such as ethnicity, language, nationality, country of birth)
- Images captured by the school's CCTV system (in accordance with the school's CCTV system statement included in the taking and storing images of children policy)
- National Insurance Number

Pupils:

- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment data (such as baseline data, marks for homework, classwork, tests and examinations)
- Special Educational Needs and Disabilities information.
- Pastoral information (such as behavioural and safeguarding information)
- Higher education information (such as destinations of leavers)
- Medical information
- References given or received by the school and information provided to/from other educational establishments (e.g. academic or pastoral information)
- Birth Certificate for pupils in Westbourne
- External examination data including unique codes, examination entries and results

Parents:

- Financial information to be used for the provision of bursaries
- Where appropriate, information about individuals' health
- National Insurance Number
- Proof of address

Staff:

- Car details (use of car parking facilities)
- Where appropriate, information about individuals' health
- Contact details for next of kin
- Financial information (payroll)
- National Insurance Number
- Identity documents including but not limited to proof of address, copy of birth certificate, copy of passport and photo ID.
- Certificate number of DBS check
- References given or received by the school

Appendix D: Data Retention Schedule

STAFF

Document	Content	Retention Period	Disposal	Information Asset Owner
Absence and Attendance	▪ Annual leave record ▪ Absence record ▪ Sickness record	Current year + 6 years	Secure disposal by the School	HR & Compliance Officer
Discipline and Grievance	▪ Letters, reports and meeting notes relating to cases	Oral warning – Date of warning + 6 months Written warning (Level 1) – Date of warning + 6 months Written warning (Level 2) – Date of warning + 12 months Final warning – Date of warning + 18 months	Secure disposal by the School	HR & Compliance Officer
Evidence of Right to Work (Home Office)	▪ Evidence of Right to Work for successful candidates	Home Office requires documents are kept for duration of employment + 6 years	Secure disposal by the School	HR & Compliance Officer
Pre-employment vetting information	▪ DBS Checks ▪ Home Office Checks	The school should not keep copies of DBS certificates, but is permitted to note the certificate number and any relevant information regarding convictions. Retained for the duration of the employment + 6 years.	Secure disposal by the School	HR & Compliance Officer
Payslips	▪ Copies	Current + 6 years	Secure disposal by the School	Finance Director
Performance Assessment (annual appraisal/assessment records)	▪ Personal Development Record ▪ Promotion/regrading	Current + 6 years	Secure disposal by the School	Deputy Headteacher
Personnel Files	▪ Personal and sensitive data	Termination of employment + 6 years	Secure disposal by the School	HR & Compliance Officer
Recruitment and	▪ Candidate assessment/	All relevant information should be added to	Secure disposal by the School	HR & Compliance Officer

Selection	shortlisting notes Interview notes	staff personal file and retained for the duration of their employment plus 6 years.	School	
School Census Returns		Current year + 5 years	Secure disposal by the School	HR & Compliance Officer
Single Central Record	- Personal and sensitive data - DBS Checks - Medical Checks - Contact details - Courses and training	Entry in excel spreadsheet kept to reflect current workforce. If someone leaves, they move to the leavers tab. The record should be deleted date of leaving + 6 years	Not applicable	HR & Compliance Officer
Staff Development Plans	Courses and training	Life of the Plan + 6 years	Secure disposal by the School	Deputy Headteacher
Timesheets	Record of staff onsite (logging in and out)	Current + 3 years	Secure disposal by the School	Finance Director
Unsuccessful candidates	- Application forms - Interview notes - Right to Work evidence - DBS details	6 months	Secure disposal by the School	HR & Compliance Officer

SENIOR LEADERSHIP TEAM

Document	Content	Retention Period	Disposal	Information Asset Owner
Minutes of Senior Leadership Team & meetings of other internal	- Minutes of SLT - Minutes from internal meetings	Date of meeting + 3 years then review annually, or as required if not destroyed	Secure disposal by the School	School Secretary
School Development Plans		Life of Plan + 3 Years	Secure disposal by the School	Headmistress
Property Files	- Maintenance logs - Work carried out by contractors	These should be retained by the school whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold	Secure disposal by the School	Estates & Facilities Manager
Visitor Books and signing in sheets	- Name of individual - Company - Time of entry and departure - Vehicle Registration	Last entry in the visitor book + 6 years then review	Secure disposal by the School	Receptionist
CCTV	Images of pupils, workforce, visitors	Images will be retained for 30 days unless requested as part of an incident/investigation	Deleted electronically by Data Controller	Estates & Facilities Manager

PUPILS

Document	Content	Retention Period	Disposal	Information Asset Owner
Accident Reporting	Contains information relating to individuals	Adults and Children - Accident Book + 3 years after last entry (<i>e.g. if it takes 5 years to complete book must be retained for a further 3 years</i>)	Secure disposal by the School	Health Safety Officer
Admissions files (successful)	- Pupil data received and used at point of enrolment - Data used in MIS as a core record	Pupil at school + 1 year	Secure disposal by the School	Director of Admissions & Marketing Communications
Admissions files (unsuccessful)	Pupil data	Resolution of case + 1 year	Secure disposal by the School	Director of Admissions & Marketing Communications
Attendance Registers (Pupils)	Pupil attendance information	Date of last entry + 3 years	Secure disposal by the School	Data Manager
Behaviour Records (Pupils)		Pupil at school + 1 year	Secure disposal by the School	SENCo/Designated Safeguarding Lead
Biometric Data	Fingerprints to enable access to cashless catering payments system	Retained until: - the pupil leaves the School; - when the pupil or parent withdraws consent; - when the pupil ceases to use the biometric system; - when the biometric system is replaced; or - where the School no longer requires the biometric data for the purpose for which it was collected	Secure deletion from the payment system by the Data Controller	Catering Manager
Books (Pupils)	- Class Record Books - Mark Books - Records of Homework set - Student work	Current Year + 1 Year Where possible student's work should be returned to the students at the end of the academic year	Secure disposal by the School	Heads Of Departments
Educational Record (Prep School)	Pupil information	Retained whilst the child remains at the primary school. Transfer to receiving school	Common Transfer File by the Data Controller. Data	Administrative Manager

	Examination results (public & internal)	when child leaves the school. DOB of the child + 25 years.	at source will need to be disposed of in line with the appropriate retention period	
Educational Record (Senior School)	- Pupil information - Examination results (public & internal)	Record transferred from primary school to receiving school. Retained from DOB of the child + 25 year	Secure disposal by the School	Administrative Manager
Exclusions (pupils)		Pupil at school + 1 year. Exclusion data should be 'passed on' to subsequent settings. The school then has the responsibility for retaining the full history of the child. The school should already ensure that the LA has the exclusion data	Secure disposal by the School	Headmistress
EYFS	- Pupil information - Nursery register	Records should be retained for a reasonable period of time after children have left the provision (e.g. three years) or until the next Ofsted inspection after the child has left the setting (whichever is the soonest)	Common Transfer File by the Data Controller or Secure disposal by the School	Director of Admissions & Marketing Communications
Information apps, e.g., Purple Mash, Seesaw, etc	- Name of pupil - Class	For the duration of the pupil's time at school	Deleted electronically by the Data Controller	Director of Systems Innovation & Examinations Secretary
Medical Conditions	- Name of Pupil - Medical Conditions - Medicine administration	Medical conditions + ongoing management. Pupil at school + 1 year	Secure disposal by the School	School Nurse
MyConcern	Personal and sensitive data	Record transferred from primary school to receiving school. Secondary school to retain from DOB of the child + 25 years as part of Student Education Record	Common Transfer File by the Data Controller. Data at source will need to be disposed of in line with appropriate retention period	SENCo/Designated Safeguarding Lead
Parental consent forms for School Trips	Pupil name	Conclusion of the trip (or at the end of the academic year).	Secure disposal by the School	Administrative Manager

	Next of kin contact details				
Photo Consent Forms	- Name of parental responsibility - Signature	For the duration of the pupil's time at school	Secure disposal by the School	Director of Admissions & Marketing Communications	
Safeguarding Files	Personal and sensitive data	Record transferred from primary school to receiving school. Secondary school to retain from DOB of the child + 25 years as part of Student Education Record	Common Transfer File by the Data Controller. Data at source will need to be disposed of in line with appropriate retention period	SENCo/Designated Safeguarding Lead	
Special Educational Needs (SEND) Records	- SEND files - Education, Health, and Care Plans	Record transferred from primary school to receiving school. DOB of pupil + 31 years (EHCP is valid until individual reaches age of 25 + 6 years from end of plan in line with Limitation Act)	Secure disposal by the School	SENCo/Designated Safeguarding Lead	
Text/Communication app between parents & school	Name and contact details of those with parental responsibility	For the duration of the pupil's time at school	Deleted electronically by Data Controller	School Secretary / PA To Headmistress	