Merchant Taylors' School

PRIVACY NOTICE

Policy Custodian: Deputy Head Information Systems
Approving Body: MTS Senior Leadership Team
Approved: July 2023
(This policy does not extend to Merchant Taylors' Prep.)

References

1.1 Legal and regulatory framework:

- The General Data Protection Regulation 2018
- Data Protection Act 2018
- The Privacy and Electronic Communications Regulations 2011
- The Protection of Freedoms Act 2012

1.2 Relevant Guidance and practice notes provided by the Information Commissioner's Office:
This **Privacy Notice also** applies in addition to the School's other relevant terms and conditions and policies, including:

- The ICO Guide to the Privacy and Electronic Communications Regulations:
- The ICO Guide to Direct Marketing:
- The ICO Code of Practice on Subject Access:
- The ICO Data sharing code:
- The ICO Code of Practice on CCTV:
- The ICO Code of Practice on Privacy Notices:
- The ICO sector-specific guidance for schools, universities and colleges:
- HM Government: Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (March 2015).
- Privacy Notices under the GDPR
- Direct Marketing Guidance (PECR) The ICO's Guide to Data Protection
- Overview of the General Data Protection Regulation
- DRAFT Consent Guidance for GDPR

1.3 Relevant School Policies:
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 CCTV policy;
- the school's safeguarding, pastoral, or health and safety policies, including how concerns or incidents are recorded;
- the school's policies, including its ICT Acceptable Use policy,

2. General Principles

2.1 General Data Protection Regulation 2018 ("the Act") protects an individual's rights in respect of their information. Merchant Taylors' School process large amounts of "personal data" about members of the school community. Under the Act, the school must process such personal data "fairly". This includes telling pupils and parents how their personal data will be held and used by the school. This data protection policy is intended to help meet that legal requirement. It should be noted, from the outset, that data protection should always take second place to safeguarding and child protection. If there is a potential conflict between these competing requirements, the welfare of the child is paramount.

2.2 This Policy

2.2.1 This policy is intended to provide information about how the school will use (or "process") personal data about individuals including current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents"), staff and visitors. It applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of personal data. The General Data Protection Regulation (GDPR) is an EU Regulation which was to replace the current Directive and be directly applicable in all Member States, from 25th May 2018 onwards without the need for implementing national legislation. These regulations have also been incorporated into English law via the Data Protection Act, 2018.

2.2.2 Anyone who works for, or acts on behalf of, the school (including but not limited to staff, volunteers, governors and service providers) should also be aware of and comply with this data protection policy, which also provides further information about how personal data relating to those individuals will be used. Further details are in Sections 3 and 4 of this policy.

***2*.3 Responsibility for Data Protection**

2.3.1 In accordance with the Data Protection Act 2018 ('the Act'), the school has notified the Information Commissioner's Office of its processing activities. The school's ICO registration number is Z1484349 and its registered address is ***Merchant Taylors' School Ltd***. The School Address is Sandy Lodge Lane, Northwood, Middlesex, HA6 2AT

2.3.2 Whilst ***Merchant Taylors' School*** is the Data Controller for the school, the School has appointed the Deputy Head Information Systems (DHIS) to ensure that all personal data is processed in compliance with this policy and the Act. In the event of any queries, the DHIS may be contacted at the School via email:info@mtsn.org.uk or telephone, 01923 820644 or via written communication sent to the Deputy Head Information Systems at the School postal address.

2.4 The Principles of the Act

2.4.1 Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully.
- used for limited, specifically stated purposes.
- used in a way that is adequate, relevant and not excessive.
- accurate.
- kept for no longer than is absolutely necessary.
- handled according to people's data protection rights.
- kept safe and secure.
- not transferred outside the UK without adequate protection.

2.4.2 Under GDPR, the following rights exist for individuals

- Right to be informed how data is used by the School (as set out throughout this Privacy notice).
- Right of access to personal data held by the School.
- Right of rectification where personal data can be rectified if it is inaccurate or incomplete.

- The “right of erasure” is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Right to restrict processing in order to ‘block’ or suppress processing of personal data in certain circumstances e.g. where the data is inaccurate or the processing was unlawful, so that particular data is merely held but not processed.
- Right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- Right to object to processing based on legitimate interests, direct marketing or processing for purposes of scientific/historical research and statistics.
- Right to object to decisions made automated individual decision-making (making a decision solely by automated means without any human involvement).

2.5 Types of Personal Data Processed by the School

2.5.1 The school may process a wide range of personal data about individuals including current, past and prospective pupil, their parents and employees as part of its routine operations including.

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (about those who use School car parking facilities);
- bank details and other financial information, e.g. about parents who pay fees to the school or payroll details for members of staff;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils as well as references supplied by previous employers of staff;
- academic and professional qualifications as well as relevant previous experience and annual reviews of employees;
- images of pupils (and other individuals) engaging in school activities, and images captured by the school's CCTV system (and the policy on taking, storing and using images of children);

2.5.2 Generally, the school receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.

2.6 Sensitive Personal Data

2.6.1 The school may, from time to time, need to process "sensitive personal data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, biometric data, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

Examples of data processing in this category may include:

- 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 educational services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;

- In connection with employment of its staff, for example DBS checks, welfare or pension plans;
- To run any of its systems that operate on biometric data, such as for security and other forms of pupil identification (e.g. registration, catering payments, library borrowing etc.); 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.

2.7 Use of Personal Data by the School

2.7.1 The school will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its "legitimate interest" operations, not limited to but including as follows:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents;
- For the purposes of staff selection and to confirm the identity of prospective members of staff (including statuary safeguarding checks);
- To provide education services (including support for Special Educational Needs), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the school community;
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, to allow participation in Nationwide vaccination programmes, insurance purposes, or to organisers of school trips;
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT acceptable use policies;
- 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 security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

2.8 Data Accuracy and Security

2.8.1 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 should notify the DHIS of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DHIS in writing. The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, ensuring that it is held in accordance with the Principles of the Act. All staff will be made aware of this policy and their duties under the Act.

2.9 Safeguarding Practice and Information Sharing

2.9.1 Whilst the General Data Protection Regulation places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm.
Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns. For further information, see HM Government's "*Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers*" (March 2015). The Local Safeguarding Children's Board (LSCB) or Safeguarding Partnerships can require an individual or body to comply with a request for information, as outlined in section 14B of the Children Act 2004. This can only take place when the information requested is for the purpose of enabling or assisting the LSCB or Safeguarding Partnership to perform its functions. Any request for information about individuals should be necessary and proportionate to the reason for the request and should be made to the Designated Safeguarding Lead who must discuss any such request with the Data Protection Officer.

Occasionally, the school will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants) or relevant authorities (HMRC, police or the local authority). The School also has to complete surveys issued by organisations to which it is affiliated to including the Department for Education, the Independent Schools Council, the Independent Schools Bursars' Association and the Large Independent Day Schools group. Much of the information supplied to these groups is anonymous in character. In order for School Trips to be safely and securely undertaken, it will be necessary to share limited pupil and parent data with Travel Companies, Insurers and Transport and accommodation providers. Individuals should note that this is highly likely to include copies of passports. In cases such as this, the individuals should consult the data protection policies of these companies.

Where there is an unexpected need to share pupil and parents' data with a third party, the individuals affected will be notified in advance.

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

- medical records which are held and accessed only by the School Surgery, or otherwise in accordance with express parental consent; and
- pastoral or safeguarding files.

However, a certain amount of any Special Educational Needs pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that this pupil requires.

Staff, pupils and parents are reminded that the school is under duties imposed by law and statutory guidance (including **Keeping Children Safe in Education** and the Prevent Duty) 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 or cloud based applications 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.

2.10 Rights of Access to Personal Data ("Subject Access Request")

2.10.1 Individuals have the right under the Act to access personal data about them held by the school, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DHIS. The school will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within statutory time-limits. If an individual believes that any information held on him or her is incorrect or incomplete, then they should write to the DHIS as soon as possible. The School will promptly correct any information found to be incorrect.

2.10.2 **Exemptions.** All members of the school community should be aware that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts (though examiners' comments may, in certain circumstances, be disclosed), nor any reference given by the school for the purposes of the education, training or employment of any individual.

3. Data Protection for Staff

3.1 The aim of this section is to detail how the data protection policy might affect pupils and parents of Merchant Taylors' School and should be read in conjunction with Section 2, General Principles.

3.2 Data Protection Protocols

3.2.1 The following Protocols must be adhered to at all times:

- Staff should only ever share information on a "need to know basis".
- Data protection should never be used as an excuse for not sharing information where necessary. The welfare of the child is paramount.
- Seniority does not give an automatic right to information.
- All emails may be disclosable.
- Only keep data for as long as is necessary.

3.3 Confidentiality

3.3.1 Any School information/records including details of pupils, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless written consent has been obtained from the data subject by the School. This requirement exists both during and after employment. In particular, such information for the benefit of any future employer.

3.3.2 The law states that where a teacher is facing an allegation of a criminal offence involving a pupil registered at the School, the teacher concerned is entitled to anonymity until the teacher is either charged with an offence or the anonymity is waived by the teacher. If publication is made on behalf of the School, the School, including senior management and governors could be prosecuted. If a teacher is charged with such an offence, all communication must be directed through the Head Master who will have authority to deal with the allegation and any enquiries to ensure that this restriction is not breached. If a member of staff is found to have breached (whether intentionally or otherwise) this duty, any accusations will be dealt with under the School's Disciplinary Procedure.

3.4 Off Site Access

3.4.1 The School is required to ensure 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. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove sensitive personal data [as defined in Section 2 of this Data Protection Policy] from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head Master or Bursar (for support staff). Where a member of staff is permitted to download data off site it will need to be password protected.

3.4.2 There are exceptions where prior approval is not required:

- iSAMS, the School's data management system, may be used on personal devices provided that the device is secure and password protected.
- Remote access to the School network, where employees may work from outside the School site as long as the documents processed are not stored on personal devices.
- For pupils on off-site trips, medical information and other relevant information (e.g. passport details) may be taken by the trip leader.

3.5 Taking Photographs in Schools

3.5.1 The General Data Protection Regulation and Data Protection Act 2018 is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- Photos taken for official school use may be covered by the Act as well as the School's Terms and Conditions. Pupils should be advised why they are being taken.
- Videography is at used at Merchant Taylors' to assist teacher training. The positioning of the video camera is such that the teacher is the focus of the footage and is chosen so that pupils cannot be identified unless the pupils actively choose to face the video camera. Pupils should notified that the filming is taking place in the lesson.

3.5.2 Personal use:

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
- Family members invited to the School Play or Concert where copyright restrictions do not apply and wish to video it. These images are for personal use and the Data Protection Act does not apply. (The video footage must not be uploaded into a publicly available part of the internet in order to avoid privacy and copyright violations).

3.5.3 Official school use:

- Photographs of pupils or employees are taken for building passes or identification on school coaches. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.
- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used. Permission is sought through the Parental contract, at which time parents are given the option to opt out. Information on who might have opted out is held by the Deputy Head Information Systems. Staff may ask for details of who is on the list at any time.

3.5.5 Media use:

- A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

3.6 What to do in the Event of a Suspected Data Breach

3.6.1 **What is a 'personal data breach'?** A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service". A personal data breach may mean that someone other than the

school gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within the school or if a member of staff accidentally alters or deletes personal data.

3.6.2 In the event of a breach, the member of staff must notify the Privacy Officer as soon as possible and certainly within 24 hours of becoming aware of the breach. This notification must include at least:

- your name and contact details;
- the date and time of the breach (or an estimate);
- the date and time you detected it;
- basic information about the type of breach; and
- basic information about the personal data concerned.

Under the terms of the Act, the School has a statuary duty to report the breach to the Information Commissioner's Office within 72 hours. In some circumstances, those people whose personal data has been unlawfully shared need to be informed too.

3.6.3 The DHIS will then make a judgement on the best course of action which is likely to include notifying the Head Master, plus the Designated Safeguarding Lead in the event that the data breach includes pupils' details, as appropriate.

4. Data Protection for Pupils and Family

4.1 The aim of this section is to detail how the data protection policy might affect pupils and parents of Merchant Taylors' School and should be read in conjunction with Section 2, General Principles.

4.2 Keeping in Touch and Supporting the School

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

- Share personal data about current and past parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the School Development Office and the Old Merchant Taylors' Society;
- Contact current and past parents and/or alumni by post and email in order to promote and raise funds for the school;
- Collect information from publicly available sources about current and past parents' and former pupils' occupation and activities, in order to maximise the school's fundraising potential.
- Occasionally carry out wealth screening using trusted third parties who review information which is in the public domain (for example, FTSE100 directorships, company directorships, property holdings, Forbes, rich lists, etc.) on our behalf. We never use the data produced by this exercise as the sole basis for sending out communications; it is a starting point for further research to identify whether someone may be interested in supporting the school, which includes considering any previous engagement with the school, philanthropic interests and previous donations. This research helps us to understand more about you as an individual so we can focus conversations we have with you about fundraising and volunteering in the most effective way.
- Use publicly available sources to carry out due diligence on donors in line with the school's Gift Acceptance Policy and to meet money laundering regulations.
- Should you wish to limit or object to any such use, or would like further information about them, please contact the DHIS in writing.

4.3 Subject Access Requests

4.3.1 In addition to the general principles outlined in Section 2:

- Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. Pupils aged 13 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis.
- A person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on his behalf.

4.4 Pupils' Rights

4.4.1 The rights under the Act belong to the individual to whom the data relates. However, the school will in most cases rely on parental consent to process personal data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted. In general, the school will assume that pupils consent to 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 will 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.

4.4.2 Pupils are required to respect the personal data and privacy of others, and to comply with the school's IT Acceptable Use Policy and the School rules

4.5 Queries and Complaints

4.5.1. If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school complaints procedure and should also notify the DHIS. The school will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

4.5.2 An individual can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel (01626) 545 700. However, the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator

5. Data Retention and Storage Guidelines

5.1 In these guidelines, "record" means any document or item of data which contains evidence or information relating to the school, its staff or pupils. Some of this material will contain personal data of individuals as defined in the Act: but not all. Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

5.2 Storage of Records

Records should be stored as follows:

5.2.1 Digital records.

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data - or any large quantity of data - should as a minimum be stored in folders where access has been restricted. Network passwords should be complex and subject to regular change. Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record. It is important to bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed - whether as a result of litigation or investigation, or because of a subject access request under the Act.

5.2.2 Paper records.
Paper records should be stored in dry, cool, reasonably ventilated storage areas. Under the Act, paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not. However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the Act.

5.3 Archiving and the Destruction or Erasure of Records.
Staff given specific responsibility for the management of records must ensure, as a minimum, the following:
5.3.1 That records - whether electronic or hard copy - are stored securely as above, where possible with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;

5.3.2 That important records, and large or sensitive personal databases, are not taken home or - in respect of digital data - carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary, in which case it should be subject to a risk assessment and in line with the eSafety policy (therefore written permission requested in advance less the exemptions listed);

5.3.3 That questions of back up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual ad hoc action;

5.3.4 That arrangements with external storage providers - whether physical or electronic (in any form, but most particularly "cloud-based" storage) - are supported by robust contractual arrangements providing for security and access;

5.3.5 That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and - in the case of personal data - necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and

5.3.6 That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely - with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them. For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information securely.

HOW LONG WE KEEP 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. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the school. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Deputy Head Information Systems at the School. However, please bear in mind that the school may have lawful and necessary reasons to hold on to some data.

5.4 Table of Recommended Retention Periods

Type of Record/Document	Recommended Retention Period
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	6 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	***NB – this will generally be personal data***
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
• Examination results (external or internal)	7 years from pupil leaving school
• Pupil file including: Pupil reports Pupil performance records Pupil medical and vaccination records	ALL: 28 years from date of birth (subject where relevant to safeguarding considerations). Any material which may be relevant to potential claims should be kept for the lifetime of the pupil.
• Special educational needs records • (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)

SAFEGUARDING	***NB – please read notice at the top of this note***
• Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
• Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]
	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely.
• Child Protection files	If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).

ACCOUNTING RECORDS	
• Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*)	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place
[NB specific ambit to be advised by an accountancy expert]	Internationally: can be up to 20 years depending on local legal/accountancy requirements
Tax returns	Minimum – 6 years
VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
CONTRACTS AND AGREEMENTS	
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement

INTELLECTUAL PROPERTY RECORDS	
• Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	***NB this will almost certainly be personal data***
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (not certificate)
• Contracts of employment	7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 6 years
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
• Immigration records	Minimum – 4 years
• Health records relating to employees	7 years from end of contract of employment
INSURANCE RECORDS	
• Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
• Correspondence related to claims/ renewals/ notification re: insurance	Minimum – 7 years

ENVIRONMENTAL & HEALTH RECORDS	
• Maintenance logs	10 years from date of last entry
• Accidents to children	25 years from birth (unless safeguarding incident)
• Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances	Minimum – 7 years from end of date of use
• Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.

Deputy Head (Information Systems)