

MERCHANT TAYLORS' PREP PRIVACY (TRANSPARENCY) NOTICE

*Merchant Taylors' Prep GDPR Privacy Notice
Applicable to all members of the school community (past and present)*

1. References

1.1 Legal and regulatory framework:

- The UK 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 safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded;
- the school's policies, including its ICT Acceptable Use policy and eSafety policies,
- the School's Data Protection policy for staff, contained within the Employment Manual

1.4 Retention of Records Policy:

Sections 5.3 and 5.4 of this policy constitute MTP's Retention of Records Policy.

2. General Principles

2.1 Introduction

2.1.1 UK General Data Protection Regulation 2018 (“the Act”) protects an individual’s rights in respect of their information. Merchant Taylors’ Prep 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.

2.1.2 Personal data is information that the School holds about you or your child and which identifies you or your child (either directly or indirectly).

2.1.3 Under the Act, personal data must:

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

2.2 This Policy

2.2.1 This notice is to help you understand **how** and **why** we collect personal data about you or your child and **what** we do with that information. It also explains the decisions that you can make about your or your child's personal data.

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 policy,

2.2.3 Versions of this policy are available specifically for parents/pupils and employees. Children are considered to have enough understanding to exercise their own data protection rights once they reach the age of 12.

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***, Sandy Lodge Lane, Northwood, Middlesex, HA6 2AT.

2.3.2 Whilst ***Merchant Taylors’ Prep*** is the Data Controller for MTP, the School has appointed the Senior Deputy Head (SDH) to ensure that all personal data is processed in compliance with this policy and legislation. In the event of queries about data processing at Merchant Taylors’ Prep, the SDH may be contacted at the School via email:office@mtpn.org.uk or telephone, 01923 825648 or via written communication sent to the Senior Deputy Head at the Prep School postal address, which is Merchant Taylors’ Prep, Moor Farm, Sandy Lodge Road, Rickmansworth, Hertfordshire WD3 1LW.

2.4 The purposes for which we use personal data and the lawful bases

2.4.1 The School uses child's and their parents' personal data, and the personal data of an employee, contractor or visitor, in all cases extending to applicants and former parents, pupils or personnel to:

1. Teach the child and our other pupils;
2. Monitor the behaviour of the child and others and to take action where appropriate;
3. Look after the child and other people;
4. Enable the School to comply with its legal obligations, to assist in the management and operation of the School and to advance and protect the School's interests, objects and reputation;
5. Fundraise, market and promote the School. For example, by using photos of our pupils in the School prospectus, on the School's website or on social media;
6. Form and maintain a contract between the employee and the School;
7. Comply with Safeguarding, Child Protection, Prevent and other laws and duties;
8. Comply with Health and Safety laws and duties;
9. Comply with Equal Opportunities monitoring, laws and duties; and
10. Comply with legislation regarding the right to work in the UK.

2.4.2 Under data protection law, the School can only use personal data if it has a lawful basis for doing so. The lawful bases that we are relying on when handling your child's personal data are as follows:

- **Legitimate interests:** This means that the School is using personal data where this is necessary for the School's legitimate interests or someone else's legitimate interests.
 - Specifically, the School has a legitimate interest in:
 - educating and looking after its pupils;
 - complying with its agreement with a parent for a child to be at the School;
 - investigating if something has gone wrong;
 - protecting, promoting and improving the School
 - This lawful basis only applies where our legitimate interests are not overridden by your or your child's interests, rights and freedoms. Legitimate interests applies to all of the 4 purposes listed above.
- **Public task:** This allows the School to use personal data where doing so is necessary in order to perform a task in the public interest or to exercise one of our functions or powers as a school. This basis applies to purposes 1, 2, 3 and 4 above. For example, when we teach and look after a child.
- **Legal obligation:** The School might need to use your or your child's personal data in order to comply with a legal obligation. For example, to report a safeguarding concern to Children's Services. Occasionally the School may have a legal obligation to share your or your child's personal data with third parties such as the court.

- **Vital interests:** In limited circumstances we may use your or your child's personal data to protect someone's vital interests. For example, to prevent someone from being seriously harmed or killed.

2.5 Detailed lawful bases for processing data

This section contains more detail about the purposes for which your or your child's personal data is used, the applicable lawful basis or bases as well as further information about sources and recipients. It does not say anything different to what's set out above but goes into more detail.

We have used a colour coded system so that you can see which bases we are relying on for each of the purposes described at paragraphs **Error! Reference source not found.** to 56 below. **LI** means legitimate interests, **PI** means public task, **LO** means legal obligation and **VI** means vital interests. So **(LI, PI)** means that we are relying on both legitimate interests and public task for that purpose.

2.5.1 Lawful bases for processing data for parents and children

Where a child is 12 years old and able to exercise their own data rights, please read 'your' for 'your child' throughout this section.

- 1 Our main reason for using your child's information is to provide your child and other pupils with an education (**LI, PI**).*
- 2 The School will also use your child's personal data to safeguard and promote your child's welfare and the welfare of others (for example, so that we can look after your child if they are hurt) (**LI, PI, VI**).*
- 3 We will use information about your child during the admissions process e.g. when assessing them and considering any information provided on the registration forms (**LI, PI**).
- 4 We may let your child's previous school know if they have been offered a place at the School. This is because they have a legitimate interest in finding out what happens to their former pupils as this will help them support their other pupils when they leave the school (**LI**).
- 5 The admissions forms which you complete give us personal data about your child, such as, their name, contact details, disabilities, learning disabilities, any particular difficulties they have with work, hobbies and interests, medical information (such as information about an allergy) and their family circumstances (**LI, PI**).
- 6 We get information from your child, their teachers and other pupils. Your child's old school also gives us information about how well your child did and any difficulties they had if we need this information to teach and take care of them (**LI, PI**).
- 7 Sometimes we get information from your child's doctor and other professionals where we need this to look after your child (**LI, PI**).
- 8 We need to tell all appropriate members of staff if your child has a health issue and use their medical information to look after them (**LI, PI**).
- 9 We will tell your child's teachers if your child has special educational needs or requires extra help with some tasks (**LI, PI**).
- 10 We will need to share information about your child (e.g. about their health and wellbeing) with the school Nurse and pastoral team (**LI, PI, VI**).

- 11 If we have information that your child suffers from an allergy we will use this information so that we can look after your child (LI, PI, VI).*
- 12 If we have information that your child has a disability we will use information about that disability to provide support for your child, adjust our policies and take it into account when we make decisions (LI, PI).*
- 13 Where appropriate, the School will have information about your child's religious beliefs or other beliefs and practices. For example, if your child does not eat certain foods (LI, PI).*
- 14 We will also hold information such as your child's religion or ethnic group] for the purposes of reporting census information and celebrating our communities (LI, PI, LO).*
- 15 We use CCTV to make sure the School site is safe. Images captured of your child via CCTV will be your child's personal data. CCTV is not used in private areas such as changing rooms (LI, PI).*
- 16 We will use your child's personal data to take other steps to make sure the school site and buildings are safe, for example, we keep a record of who is on the school sites at any given time (LI, PI).*
- 17 We may share information about your child with (and get information from) health authorities, providers of healthcare services and healthcare professionals, for example, in relation to pupil immunisations. (LI, PI).
- 18 We record your child's attendance and if he or she has time away from the School we record the reason(s) why (LI, PI).
- 19 We will need to share some of your child's information with regulators and with the government (e.g. the Department for Education). We will need to tell the local authority that your child attends the School, if your child leaves the School or let them know if we have any concerns about your child's welfare. The local authority may also share information with us for these reasons (LI, LO, PI).
- 20 We may need to share information about your child with the Health and Safety Executive (a government organisation) if there is a health and safety issue at the School (LI, LO).*
- 21 The School is a charity which means that in exceptional circumstances we may need to share your child's personal data with the Charity Commission e.g. in the event of a serious incident (LI, LO, PI).*
- 22 When we are inspected by the Independent Schools Inspectorate we will have to make your child's personal data available to the inspectors to assist them with their inspection (LI, LO, PI).*
- 23 If the School receives a complaint or grievance that involves your child we will need to use their personal data to deal with this appropriately. For example, if you make a complaint or if another parent complains about an issue which involves your child (LI, PI).*
- 24 The School may share information about your child with the local authority for the purpose of the preparation, implementation and / or review of your child's Statement of Special Educational Needs or Education Health and Care Plan (LI, PI, LO).
- 25 We may use your child's personal data in connection with legal disputes (LI, PI, LO).*

- 26 We are legally required to provide the Department for Education with certain information about your child. Some of this information will be stored on the National Pupil Database. Organisations can request information from the National Pupil Database which includes information about your child. But they are only allowed to do this for limited purposes and they must be very careful about how they use your child's personal data. More information can be found here - <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information> (LO).
- 27 We will need information about any court proceedings, court orders or criminal petitions that relate to your child. This is so that we can safeguard your child's welfare and wellbeing as well as other pupils at the School (LI, PI).
- 28 If your child is from another country we have to make sure that they have the right to study in the UK. Sometimes the government will ask us to provide information as part of our reporting requirements. In addition to this we have a duty to provide information about your child to UK Visas and Immigration who are part of the government (LI, LO, PI).
- 29 Additionally, if your child is sponsored by us under a Child Student or Student visa we will have to provide information about them to UK Visas and Immigration to comply with our duties as their sponsor (LI, LO, PI).
- 30 Depending on where your child will go when they leave us we will provide their information to other schools and colleges. For example, we will share information about your child's exam results and provide references. Any references that we provide will be confidential which means that you might not be provided with a copy (LI, **PError! Reference source not found.**).
- 31 If we hold safeguarding or child protection information about your child, we will share that with your child's next school (LI, PI, LO).
- 32 If your child has a safeguarding file, we are legally required to pass this file to their next school (LI, LO, PI).
- 33 If your child takes public examinations we will need to share information about them with examination boards. For example, if your child requires extra time in exams (LI, PI).
- 34 We may need to share information with the police (and/or other law enforcement agencies) and/or our legal advisers if something goes wrong or to help with an inquiry. For example, if one of your child's classmates is injured at School or if there is a burglary (LI, LO, PI).*
- 35 We use consultants, experts and other advisors to assist the School in fulfilling its obligations and to help run the School properly. We will share your child's information with them if this is relevant to their work (LI, PI).*
- 36 If your child has misbehaved in a serious way, we may need to share information with the police (and/or other law enforcement agencies) and we may need to use information about the action taken by the police (LI, LO, PI).
- 37 We may share some information with our insurance company to make sure that we have the insurance cover that we need or in connection with an actual or possible claim (LI, PI).*

- 38 If the School is dealing with a request for information, query, complaint or grievance (e.g. from a parent), we may need to share your child's information with other parties if it is relevant and appropriate to do so. For example, with the appropriate staff, pupil or parent involved and governors (LI, PI)
- 39 If one of your child's teachers is subject to an internal disciplinary case and this has affected your child, we may need to use your child's personal data to investigate. We may also need to share your child's personal data with the government and regulators if they become involved, for example, if they need to make a decision regarding the teacher's ability to teach (LI, PI, LO).
- 40 If you are based outside of the UK and have appointed an agent to act on your behalf during the admissions process (an overseas agent), then we may share information about your child with them. For example, we may send them the acceptance letter so that they can pass this on to you (LI).
- 41 We will share your child's academic and (where fair) their behaviour records with you so you can support your child's schooling (LI, PI). If your child has behaved badly in relation to one of their classmates (e.g. we suspect bullying) then we might share information with that pupil's parents (e.g. what sanction your child has been given) (LI, PI).
- 42 If ever in the future, we are considering restructuring the charity which operates the School, we may share your child's personal data with the other parties involved and with the relevant professional advisors (LI).
- 43 We will monitor your child's use of email, the internet and any internet based platforms, as well as mobile electronic devices e.g. iPads. *
- 43.1 In certain circumstances we will look at the content of your child's communications (e.g. emails and text messages) and their electronic devices. This is to check that your child is not misbehaving when using this technology or putting themselves at risk of harm.
- 43.2 If you would like more information about this you can read the IT Acceptable Use Policy or speak to the Senior Deputy Head or Director of Digital Learning. The monitoring we do is carried out using computer software which will automatically tell us if something isn't right. This software monitors all devices which in use at school, and we also monitor activity carried out elsewhere using school-provided IT accounts. (LI, PI).*
- 44 The School regularly publishes photos and images (including video recordings) of our pupils. If we take a photo or video of your child, we might put this on our website, on our social media pages or in our prospectus. We do this to show prospective pupils and parents what we do here and to advertise the School (LI). *
- 45 We will continue to use these photos and videos after your child has left the School (LI, PI).*
- 46 If we would like to use a photo or video in a more unusual or high-profile way (e.g. on a banner or billboard) we will talk to you about this first. *
- 47 Sometimes we use photos and videos for teaching purposes, for example, to record a drama lesson (LI, PI). *
- 48 If you have any concerns about us using photos or videos of your child please speak to the Senior Deputy Head.*

- 49 We publish our public exam results, sports fixtures and other news on the website and put articles and photos in the local news to tell people about what we have been doing (LI).
- 50 We will keep your child's contact details when they leave so we can keep them updated about what is happening at the School, to tell them about events and activities and find out how they are getting on.
- 51 The School must make sure that its computer systems are working well and are secure. This may involve information about your child, for example, our anti-virus software might scan files containing information about your child (LI).*
- 52 We may share your child's personal data with Merchant Taylors' School. For example, how well your child has behaved and their test results] (LI, PI).]
- 53 From time to time, we hire a third party to provide activities such as an external sports coach. We may share your child's personal data with them (LI, PI)].
- 54 Some of the records the School keeps and which contain your child's personal data may be used by the School (or by someone else such as the government) to check that the School has been a good school (LI, PI).
- 55 We also keep some information indefinitely for archiving purposes (this is known as "archiving in the public interest" under data protection law) and for historical research purposes.*
- 55.1 This includes the School's legitimate interest in research; supporting long-term accountability; enabling the discovery and availability of the School's and the wider school community's identity, memory, culture and history; enabling the establishment and maintenance of rights and obligations and of precedent decisions; educational purposes; and commercial and non-commercial re-use.*
- 55.2 For example, we keep some old photos so that we have a record of what the School was like in the past.
- 55.3 Information held in our archive may be made publicly available but this would only be done in compliance with data protection laws (LI, PI).*
- 56 We will share your child's personal data with the governors of the School if it concerns something they should know about or which will enable them to fulfil their role as a governor. For example, this will apply if your child has done something really well or if there is a problem at the School they need to know about (LI, PI).

As you will see from the information above, in some cases we will rely on more than one lawful basis for using your child's personal data.

We use service providers to handle personal data on our behalf for the following purposes:

- a) IT service providers who might access information about you when checking the security and functionality of our IT network;*
- b) On educational visits, caterers may have information about any food allergies or intolerances that your child has; travel companies may have a list of staff's and pupils' names; where international travel is required, travel companies will have a list of staff's and pupils' passport details;*

- a) We use various software, apps and websites to help us with teaching, and to help us provide pastoral support to our pupils. For example, we use Seesaw and Teams to allow pupils to access homework which has been set by their teachers; we use the TES Schoolcloud platform to organise parental consultations; we use Renaissance Learning to provide our Accelerated Reader service.*
- b) We use third party "cloud computing" services to store some information rather than the information being stored on hard drives located on the School site – for example we use ISAMS as our Management Information System, and we use the Office 365 system.*

2.5.2 Additional lawful bases for processing data for employees, contractors and visitors

Many of the lawful bases set out for processing the personal data of children and parents above in section 2.5.1 also apply to employees, contractors and visitors. They are marked with an *. There are some additional lawful bases for employees, contractors and visitors below:

1. We require sufficient information to form and maintain a contract between an employee and the School. For example, we will need bank details, details of qualifications held, etc. (LI, PI)
2. We need to comply with safeguarding, child protection, Prevent and other laws and duties. For example we need to check DBS records, training records etc. (LI, PI, LO).
3. We need to comply the other duties of employers, such as legislation regarding the right to work. For example we need to check identity documents, and where appropriate information about individuals' health records. (LI, PI, LO, VI).

2.5.3 Sensitive Personal Data

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, 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.

2.6 Sending information to other countries

When the School sends personal data outside of the UK, we have to consider if the other country has the same level of protection for personal data as there is in the UK. Some countries are considered by the UK Government to have adequate rules and this includes all of the European Union and some other countries, such as, New Zealand, Norway, Switzerland and Argentina. The School sends your child's personal data to countries with adequate rules when we:

- Go on a trip to France and share staff and pupil personal data with activity providers and the hotel]; and
- Store staff and pupil personal data in cloud computer storage with servers in Ireland.]

In certain circumstances, we will send your child's personal data to countries which do not have the same level of protection for personal data as there is in the UK. For example, we will:

- Store personal data in cloud computer storage with servers in the USA (this applies to some Seesaw data)

If necessary we will provide you with additional details about where we are sending your child's personal data, whether the country has an adequacy finding and if not the safeguards which we have in place outside of this privacy notice.

If you have any questions about the safeguards that are in place please contact the Senior Deputy Head.

2.7 What decisions can you make about your or your child's personal data?

- **Correction:** if personal data held by the School about is incorrect or incomplete you can ask us to correct it.
- **Access:** you can also ask what personal data we hold about you or your child and to be provided with a copy. This is commonly known as making a subject access request. We will also give you extra information, such as why we use this personal data about you or your child, where it came from and who we have sent it to.
- **Deletion:** you can ask us to delete the personal data that we hold about you or your child in certain circumstances. For example, where we no longer need the information.
- **Portability:** you can request the transfer of your or your child's personal data to you or to a third party in a format that can be read by computer in certain circumstances.
- **Restriction:** you can request that we restrict how we use your or your child's personal data in certain circumstances. Please contact the Senior Deputy Head if you would like to know more.
- **Object:** you may object to us using your or your child's personal data where:
 - we are using it for direct marketing purposes (e.g. to send you an email about a fundraising opportunity);
 - the lawful basis on which we are relying is either legitimate interests or public task. (See Section 2.5)
 - If we ever use your or your child's personal data for scientific or historical research purposes or statistical purposes.

The Senior Deputy Head can give you more information about your or your child's data protection rights. Please note that these rights don't apply in all cases and we won't always have to comply with your request.

Like other organisations we need to keep personal data safe, up to date, only use it for what we said we would, destroy it when we no longer need it and most importantly - treat the personal data we get fairly.

Please speak to the Senior Deputy Head if:

- you would like to exercise any of the rights listed above; or
- you have any concerns about how your or your child's personal data is used or shared.
- You have any out-of-the-ordinary requests for us to update the information we hold (you do not, for example, need to speak to the Senior Deputy Head if you have moved house: tell the Office).

For parents: if you or your child fails to provide certain information when requested, we may not be able to perform our obligations under the contract we have entered into with you. We may also be prevented from complying with our legal obligations (such as to ensure the welfare of your child and their classmates). Failing to provide information may also adversely affect the education and care we are able to provide to your child.

For employees, contractors and visitors: if you fail to provide certain information when requested, we may not be able to enter into a contract with you or facilitate a visit.

You have a right to make a complaint to the Information Commissioner's Office (ico.org.uk). If you do have any concerns about how we have handled your child's personal data we would kindly ask that you contact us in the first instance before you speak to the ICO so that we have an opportunity to put things right.

2.8 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 recording, retaining and sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm.

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). For further information about this, please view the school's Safeguarding Policy.

2.9. Obligations which apply to staff

Staff must comply with the Data Protection Policy set out in detail in the Employment Manual.

2.9.1 In particular, 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.

2.9.2 Confidentiality

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.

2.9.3 See also the School's eSafety Policy. The School must 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 from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or SDH. Where a member of staff is permitted to download data off site it will need to be password protected.

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 and/or Office 365 system, where employees may work from outside the School site as long as the documents processed are not stored on personal devices.
- For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader.

2.10 Obligations which apply to pupils

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

3. Photographs, videos and images in School

3.1 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.

3.2 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).

3.3 Official school use:

- Photographs of pupils or employees are taken for building passes and identification purposes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.
- For example, 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 SDH. Staff may ask for details of who is on the list at any time.

3.4 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.

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

4.1 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.

4.2 In the event of a breach, the member of staff must notify the Senior Deputy Head, or in their absence the Head, or in their absence any other Senior Leader, 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 statutory 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.

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

5. Further information

5.1 Alumni and fundraising

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 Crescunda 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 Terryers' Association;
- 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 SDH in writing.

5.2 Queries and Complaints

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 SDH. 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

5.3 Storage of Records

Sections 5.3 and 5.4 between them form the MTP Retention of Records Policy.

"Record" means any document or item of data which contains evidence or information relating to the school, its staff or pupils.

Digital records

Digital records can be lost or misappropriated in huge quantities very quickly. Sensitive data is stored in areas where access has been restricted. Network passwords are be complex and subject to regular change.

Paper records

Paper records are stored in dry, cool, reasonably ventilated storage areas. 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.

5.3.1 Archiving and the Destruction or Erasure of Records.

Staff given specific responsibility for the management of records must ensure, as a minimum, the following:

- 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;
- That important records, and large or sensitive personal databases, are not taken home or carried or kept on portable devices 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);
- That questions of back up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems);
- 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;
- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant, necessary, accurate and up-to-date;
- 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

5.4 Retention periods

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 SDH at the School. However, please bear in mind that the school may have lawful and necessary reasons to hold on to some data.

Table of Recommended Retention Periods

Type of Record/Document	Recommended Retention Period
<u>SCHOOL-SPECIFIC RECORDS</u> <ul style="list-style-type: none"> • Registration documents of School • Attendance Register • Minutes of Governors' meetings • Annual curriculum 	<p>Permanent (or until closure of the school)</p> <p>6 years from last date of entry, then archive.</p> <p>6 years from date of meeting</p> <p>From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)</p>
<u>INDIVIDUAL PUPIL RECORDS</u> <ul style="list-style-type: none"> • Admissions: application forms, assessments, records of decisions • Examination results (external or internal) • Pupil file including: <ul style="list-style-type: none"> Pupil reports Pupil performance records Pupil medical records • Special educational needs records • <i>(to be risk assessed individually)</i> 	<p><i>NB – this will generally be personal data</i></p> <p>25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).</p> <p>7 years from pupil leaving school</p> <p>ALL: 25 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.</p> <p>Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)</p>

<p><u>SAFEGUARDING</u></p> <ul style="list-style-type: none"> • Policies and procedures • DBS disclosure certificates (if held) • Accident / Incident reporting • Child Protection files 	<p><i>NB – please read notice at the top of this note</i></p> <p>Keep a permanent record of historic policies</p> <p><u>No longer than 6 months</u> from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.</p> <p>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</p> <p>If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely.</p> <p>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).</p>
---	---

<p><u>ACCOUNTING RECORDS</u></p> <ul style="list-style-type: none"> • Accounting records (<i>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</i>) <p>[NB <u>specific ambit to be advised by an accountancy expert</u>]</p> <ul style="list-style-type: none"> • Tax returns • VAT returns • Budget and internal financial reports 	<p>Minimum – 3 years for private UK companies (except where still necessary for tax returns)</p> <p>Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place</p> <p>Internationally: can be up to 20 years depending on local legal/accountancy requirements</p> <p>Minimum – 6 years</p> <p>Minimum – 6 years</p> <p>Minimum – 3 years</p>
<p><u>CONTRACTS AND AGREEMENTS</u></p> <ul style="list-style-type: none"> • Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>) • Deeds (or contracts under seal) 	<p>Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later</p> <p>Minimum – 13 years from completion of contractual obligation or term of agreement</p>

<p><u>INTELLECTUAL PROPERTY RECORDS</u></p> <ul style="list-style-type: none"> • Formal documents of title (trade mark or registered design certificates; patent or utility model certificates) • Assignments of intellectual property to or from the school 	<p>Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.</p> <p>As above in relation to contracts (7 years) or, where applicable, deeds (13 years).</p>
<ul style="list-style-type: none"> • IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents) 	<p>Minimum – 7 years from completion of contractual obligation concerned or term of agreement</p>
<p><u>EMPLOYEE / PERSONNEL RECORDS</u></p> <ul style="list-style-type: none"> • Single Central Record of employees • Contracts of employment • Employee appraisals or reviews • Staff personnel file • Payroll, salary, maternity pay records • Pension or other benefit schedule records • Job application and interview/rejection records (unsuccessful applicants) • Immigration records • Health records relating to employees 	<p><i>NB this will almost certainly be personal data</i></p> <p>Keep a permanent record of all mandatory checks that have been undertaken (not certificate)</p> <p>7 years from effective date of end of contract</p> <p>Duration of employment plus minimum of 7 years</p> <p>As above, but <u>do not delete any information which may be relevant to historic safeguarding claims</u>.</p> <p>Minimum – 6 years</p> <p>Possibly permanent, depending on nature of scheme</p> <p>Minimum 3 months but no more than 1 year</p> <p>Minimum – 4 years</p> <p>7 years from end of contract of employment</p>
<p><u>INSURANCE RECORDS</u></p> <ul style="list-style-type: none"> • Insurance policies (will vary – private, public, professional indemnity) • Correspondence related to claims/ renewals/ notification re: insurance 	<p>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.</p> <p>Minimum – 7 years</p>

<u>ENVIRONMENTAL & HEALTH RECORDS</u> <ul style="list-style-type: none"> • Maintenance logs • Accidents to children • Accident at work records (staff) • Staff use of hazardous substances 	10 years from date of last entry 25 years from birth (unless safeguarding incident) Minimum – 4 years from date of accident, but review case-by-case where possible Minimum – 7 years from end of date of use
<ul style="list-style-type: none"> • Risk assessments (carried out in respect of above) 	7 years from completion of relevant project, incident, event or activity.

Reviewed: Senior Deputy Head Sep 2024
Review Date: Sep 2025