PRIVACY NOTICE

Policy Custodian: Senior Master
Approving Body: MTS Senior Leadership Team
Approved: June 2024
(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;
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

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
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.

kept safe and secure.
not transferred outside the UK without adequate protection.

T
data where there is no compelling reason for its continued processing.

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

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

3.2 Data Protection Protocols

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

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

3.4.2 There are exceptions where prior approval is not required:

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 wr0.t i/Lani802t required:

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

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

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
Accident / Incident reporting	
Child Protection files	

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.

Senior Master