Merchant Taylors' School

E-SAFETY POLICY

Policy Custodian: Senior Master
Approving Body: MTS Senior Leadership Team
Approved: January 2025
(This policy does not apply to Merchant Taylors' Prep.)

Contents

1. Introduction and Overview

Rationale. The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Merchant Taylors' School with respect to the use of ICT-based technologies and connectivity.
- Safeguard and protect the pupils and staff of Merchant Taylors' School
- Assist school staff working with pupils to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- Promote digital literacy and help foster a positive online environment.
- Outline the technological and procedural measures in place to comply with the filtering and monitoring obligations first outlined in KCSIE, September 2023.

The main areas of risk for Merchant Taylors' can be summarised as follows:

Content

- exposure to inappropriate content, including but not limited to online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- "lifestyle" websites, for example self-harm/suicide sites;
- hate sites, extremism and those aimed at radicalisation;
- misinformation and pupils not knowing how to validate online content.

Contact

- grooming;
- cyber-bullying in all forms;
- identity theft (including Social Media account hijacking)) and sharing passwords;.
- Radicalisation.

Conduct

- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online);
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) and use of AI to generate deep fakes;
- copyright (little care or consideration for intellectual property and ownership – such as music and film, still and video imagery).

Scope
This policy applies to all members of Merchant Taylors' School community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of School ICT systems and connectivity, both within and outside of the grounds of Merchant Taylors'.

The Education and Inspections Act 2006 empowers the Head Master to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school or bring the school into disrepute. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can be taken by the School as described in the Promoting Good Behaviour Policy.

Merchant Taylors' will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school, where we are aware of it.

Role	Key Responsibilities
Head Master	To take overall responsibility for e-safety provision; To take overall responsibility for data and data security; To ensure the school uses an approved, filtered Internet Service; To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant; To be aware of procedures to be followed in the event of a serious e-safety incident; To receive monitoring reports as required from the Senior Master and DSL; To ensure that there is a system in place to monitor support staff who carry out internal e-safety procedures.
Designated Safeguarding Lead (DSL) - Deputy Head Pastoral	To lead on safeguarding and online safety as detailed in the Keeping Children Safe in Education (KCSIE) 2024 statutory guidance and Meeting Digital and Technology Standards in Schools and Colleges (2022). This includes, among other duties: • checking relevant reports e.g. Senso logging • responding to safeguarding concerns identified by filtering and monitoring (individual or trends) • providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly • Making sure all staff, pupils, parents and carers are aware of the policy. • To communicate regularly with the Senior Master to review e-safety policies and procedures, and to audit filtering and monitoring provision at least annually • To liaise with the Head of PSHE and the Director of Digital Strategy to ensure e-safety education is embedded in the curriculum and is responsive to trends arising within the pupil community.

Role	Key Responsibilities
Senior Master	To take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies; To report any safeguarding issues that arise to the DSL; To promote an awareness and commitment to e-safeguarding throughout the school community; To communicate regularly with DSL and Director of Digital Strategy as required to discuss current issues, maintain monitoring and internet filtering logs; To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident; To facilitate training and advice for all staff; To be regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Director of Digital Strategy	To oversee the delivery of the e-safety element of the Computing curriculum; To liaise with the Senior Master regularly.
IT Manager	To report any e-safety related issues that arises, to the Senior Master; To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed; To ensure that provision exists for misuse detection and malicious attack e.g. keeping anti-virus protection up to date; To ensure the security of the school ICT systems; To ensure that access controls exist to protect personal and sensitive information held on school-owned devices; To ensure the school's policy on web filtering is applied and updated on a regular basis; To ensure that they keep up to date with the school's e-safety policy and technical developments in order to effectively carry out their e-safety role and to inform and update others as relevant; To ensure that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Senior Master/DSL/Head Master for investigation / action / sanction; To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster; To keep up-to-date documentation of the school's e-security and technical procedures.
IT Technical Support Team/DSL	To implement e-measures as required by the IT Manager and to assist with investigations and system updates; To assist DSL with termly reports run from SENSO which highlights all language of concern used by the students (and adult users) whilst using cabled networked school systems, personal Surface Tablet devices and within the cloud installation of MS-Teams deployed by the School. Report to be shared

Role	Key Responsibilities
	with DSL who analyses this with a view to enhancement of existing monitoring procedures. A regular report is to be shared with the Pastoral Committee, to monitor trends.
Database Administrators	To ensure that all data held on pupils on the School management system, iSAMS, have appropriate access controls in place.
Teachers	To embed e-safety issues in all aspects of the curriculum and other school activities; To monitor and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant); To be aware of the school filtering and monitoring policies and their obligations under KCSIE 2024 and MTS Safeguarding Policy to safeguard children using online technology, particularly knowing how to report concerns; To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All employees, volunteers and workers with access to the School ICT network	To read, understand and help promote the school’s e-safety policies and guidance; To read, understand, sign and adhere to the school staff Acceptable Use Agreement; To be aware of e-safety issues related to the use of smartphones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices; To report any suspected misuse or problem to the Senior Master or DSL (via CPOMS); To maintain an awareness of current e-safety issues, data protection issues and guidance e.g. through School-led INSET; To model safe, responsible and professional behaviours in their own use of technology; To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, smartphones etc.

Pupils	Read, understand, sign and adhere to the Pupil Acceptable Use Agreement; Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulation; To understand the importance of reporting abuse, misuse or access to inappropriate materials; To know what action to take if they or someone they know feels worried or vulnerable when using online technology; To know and understand school policy on the use of smartphones, digital cameras and hand-held devices including touch-screens, which are used by boys from Year 9 upwards; To know and understand school policy on the taking / use of images and on cyber-bullying; To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school; To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home; To help the school in the creation and review of e-safety policies.
Parents	To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images; to read, understand and promote the school Pupil Acceptable Use Agreement with their children.

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- IT Acceptable Use Policy for Staff to be part of school employment manual which is updated annually;
- Acceptable Use Agreements to be issued to whole school community on entry to the school;
- Signed Acceptable use agreements to be held in pupil and personnel files;
- Pupil policy available from the School Website. Staff policy is contained within the Staff employment manual.

Handling complaints and Pupil Misbehaviour:
The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The School cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.
Sanctions for pupil infringements that are available include:

- Formal sanctions, as laid out in Promoting Good Behaviour and the Serious Disciplinary Incidents Policy
- Restorative tasks/conversations with tutor / Head of Section / Senior Master / Head Master;
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework);
- Referral to the Police or other external agencies;
- Senior Master acts as first point of contact for any complaint detected by the IT Department; the DSL acts as first point of contact for safeguarding concerns detected by the school's monitoring system or reported by parents/carers, staff or pupils (Senso or CPOMS). Any complaint about staff misuse is referred to the Head Master;
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with School child protection procedures and the School Safeguarding Policy.

Review and Monitoring

The e-safety policy should be read in conjunction with school policies: Acceptable use of ICT Policy; Safeguarding Policy; Anti-Bullying Policy; Promoting Good Behaviour Policy; Serious Disciplinary Incidents Policy; Personal, Social and Health Education Policies.

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school;
- The e-safety policy has been written by the Senior Master and is kept up to in line with technical advances so it is appropriate for its intended audience and purpose.

2. Expected Conduct and Incident Management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems;
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;

Staff

are responsible for reading the school's E-safety Policy and using the school ICT systems accordingly, including the use of smartphones, and hand-held devices including touch-screen tablets issued to staff.

Pupils

should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. Pupils also need instructions to appropriate and inappropriate use of AI systems. As this is a rapidly emerging technology, the school is reviewing how pupils should be taught ethical and safe use of these and new tools. An additional complication emerges as the minimum use of application varies by application. A non-exhaustive, but indicative, list is presented below:

Chat GPT (minimum age 18)
Microsoft Co-Pilot (minimum age 13)
Google Gemini (minimum age 18)
Claude Anthropic (minimum age 18)
Deepseek (minimum age 18)

Canva (minimum age 13)
Grammarly (minimum age 16)
Khanmigo (minimum age 18)
Midjourney (minimum age 13)

In partnership with the student Whole School Council, the School has entered into discussion about the use of AI tools. These discussions address topics like how best to make use of AI to learn, acquire feedback from assignments, prepare revision materials, research credible sources. Other issues like excessive reliance on AI, use of AI to plagiarize or cheat in assignments, or spreading of false information have been discussion.

The School is presently looking at the use of plagiarism detection software for both assignments set internally and also those intended for submission to public Exam Boards

Parents/Carers

should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school and should be aware that the School may impose sanctions for misuse of ICT Systems.

As part of the School Terms and Conditions, the School may obtain and use photographs or images (including video recordings) of the Pupil for:
1. Use in the School's promotional material such as the prospectus, the website or social media;
2. Press and media purposes;
3. Educational purposes, as part of the curriculum or extra-curricular activities.

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions; the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed;
- monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders;
- parents are specifically informed of serious e-safety incidents involving young people for whom they are responsible;

• We will contact the Police if one of our staff or pupils receives online communication that we consider is sufficiently disturbing or breaks the law.

3. Managing the ICT infrastructures

Internet access, security (virus protection) and filtering

This school:
Has secure broadband connectivity supplied by Syscomm, a national provider of Internet services in education;
Uses a Fortinet filtering system which blocks sites that fall into content and web search categories including but not limited to:

- **Illegal:** content that is illegal, for example child abuse images and terrorist content
- **Bullying:** Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others
- **Child Sexual Exploitation:** Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.
- **Discrimination**: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
- **Drugs / Substance abuse:** displays or promotes the illegal use of drugs or substances
- **Extremism:** promotes terrorism and terrorist ideologies, violence or intolerance
- **Gambling:**
- **Malware / Hacking:** promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- **Pornography:** displays sexual acts or explicit images
- **Self Harm**: promotes or displays deliberate self-harm (including suicide and eating disorders)
- **Violence:** Displays or promotes the use of physical force intended to hurt or kill
- **Suicide**: Suggest the user is considering suicide

(Fortinet has been a member of the Internet Watch Foundation since 2007.)

Allows staff a less restrictive access than pupils to the Internet, whilst still being filtered. Sites which are initially blocked for pupils may be referred to IT Technical Services to be unblocked for pupil access. Pupils are also entitled to make requests to unblock sites which are required for educational purposes.
Ensures network is healthy through use of Crowdstrike, Watchguard anti-virus software; (Watchguard has been a member of the Internet Watchfoundation since 2017)
Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
Only unblocks other external social networking sites for specific purposes / internet literacy lessons. Records of requests to unblock sites are kept as well as details relating to the outcome of the request;
Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
Ensures all staff and students have signed an Acceptable Use Agreement Form and understands that they must report any concerns;

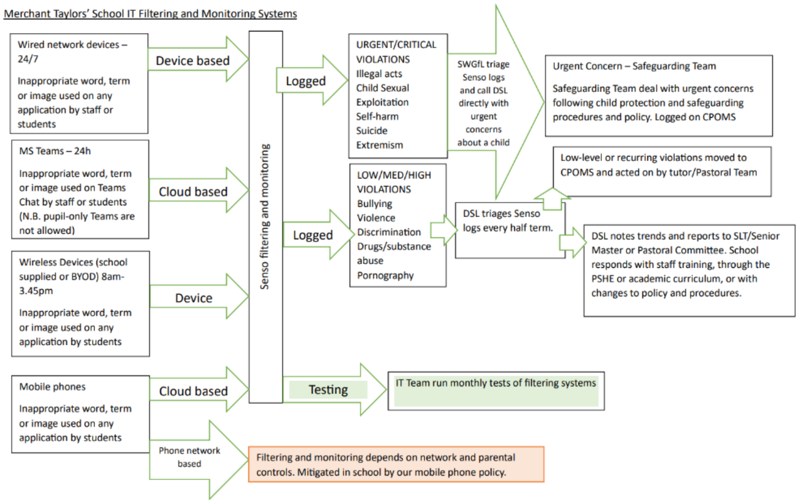
Requires staff to preview websites before use (where not previously viewed or cached) and encourages use of OneNote as a key way to direct pupils to age /subject appropriate web sites;
Is vigilant when conducting ‘raw’ image search with pupils e.g. Google image search;
Informs all users that Internet use is monitored and records of internet access are kept;
Informs staff and students that that they must report any failure of the filtering systems directly to the Senior Master;
Immediately refers any material found on School systems we suspect is illegal to the Police.
Tests both the main School filter and Wireless filters at least fortnightly. Central records are kept by the IT Technical Services and remedial measures to be taken as needed.

Commented [JB(IM1]: *changed from 'Firewall'

Network and Web-Based Monitoring

MTS uses individual, SENSO monitoring software for all pupil facing windows-based School desktops. This is a pro-active technology that actively monitors keystrokes and other activity across the network issuing alerts for the School to act on in the case of real or suspected network misuse. (SENSO has been a member of the Internet Watchfoundation since 2017). Experience has shown that the software is adept at detecting false positive results. As a result, the monitoring process has been sub-contracted out to the South West Grid For Learning Monitoring Service. Detection of high level, urgent or critical keywords requiring immediate action are escalated by SWFGL to the DSL as necessary and in turn dealt by the Safeguarding Teams. Incidents of this type are centrally recorded in CPOMS. The DSL periodically reviews the Senso logs and add lower-level safeguarding or pastoral concerns to CPOMS, to be followed up by the Pastoral Team. Trends from the Senso logs feed into Pastoral strategy, such as the PSHE curriculum.

A summary of the safeguarding protocols at MTS is illustrated below:


Merchant Taylors' School IT Filtering and Monitoring Systems
Wired network devices – 24/7
Inappropriate word, term or image used on any application by staff or students
Device based
MS Teams – 24h
Inappropriate word, term or image used on Teams Chat by staff or students (N.B. pupil-only Teams are not allowed)
Cloud based
Wireless Devices (school supplied or BYOD) 8am-3.45pm
Inappropriate word, term or image used on any application by students
Device
Mobile phones
Inappropriate word, term or image used on any application by students
Cloud based
Phone network based
Senso filtering and monitoring
Logged
URGENT/CRITICAL VIOLATIONS
Illegal acts
Child Sexual Exploitation
Self-harm
Suicide
Extremism
SWGfL triage Senso logs and call DSL directly with urgent concerns about a child
Urgent Concern – Safeguarding Team
Safeguarding Team deal with urgent concerns following child protection and safeguarding procedures and policy. Logged on CPOMS
Logged
LOW/MED/HIGH VIOLATIONS
Bullying
Violence
Discrimination
Drugs/substance abuse
Pornography
DSL triages Senso logs every half term.
Low-level or recurring violations moved to CPOMS and acted on by tutor/Pastoral Team
DSL notes trends and reports to SLT/Senior Master or Pastoral Committee. School responds with staff training, through the PSHE or academic curriculum, or with changes to policy and procedures.
Testing
IT Team run monthly tests of filtering systems
Filtering and monitoring depends on network and parental controls. Mitigated in school by our mobile phone policy.

MTS uses guest accounts for external or short-term visitors for occasional temporary access to appropriate services. The School requires MTS host to complete a visiting speaker form which requires notification in cases where a guest speaker uses a School guest account.

MTS Uses ‘remote’ management control tools for controlling workstations / monitoring user activity / setting-up applications and Internet web sites, where useful.
Storage of all data within the school will conform to the UK data protection requirements.
Pupils and Staff using mobile technology, where storage of data is online, will conform to guidance issued from HM Government.

As MTS has adopted digital learning via Surface tablets, SENSO monitoring software has been also installed on student touch screen devices to allow for teacher monitoring of pupil work during the School working day only, 8.00am-3.45pm. This allows teachers to assist pupil remotely and to ensure that the pupils are kept “on task” in class. Pupils are regularly screened to ensure they do not disable the Senso software and those found to have deliberately done so will have their internet access disabled until the software is reactivated. Teachers do not have the ability to monitor pupil devices at times such as evenings, weekends and during School holidays. Parents are reminded of this before each holiday period, and sent information to help support them in using parental safety control and internet filtering to keep pupils safe online outside of school.

MTS makes extensive use of Cloud-based Microsoft Teams. While the ability to for pupils to create Teams and Private Chat messaging within Teams has been disabled. Team messaging is monitored 24 hours a day and content of messages and pictures are automatically scanned. In the case of an “MS Team” with both adult and pupil membership at least two MTS adults should be owners or members of the team. MS–Teams monitoring is also subject to monitoring even in cases where a device not owned by the School or a pupil or is in use.

Content being looked for includes but is not limited to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Conduct being looked for includes but is not limited to: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, sharing other explicit images and online bullying.

Pupils will need frequent reminders that it can be illegal to discriminate against people because of

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion or belief
- gender
- sexual orientation

The School keeps a record of instances where attempted use of a VPN application is recorded by School systems. While such an application could be used by a pupil on holiday or by a pupil studying languages, it could be used by a cyber criminal as part of network hacking attempt as the application masks the location of the user. Records and outcomes are requested to unblock webs-sites are also recorded. Instances of unambiguous parental access to pupil email accounts are also recorded.

Network Security

The School:

Ensures staff and pupils read and sign that they have understood the school's IT Acceptable use Policy. Following this, they are set-up with Internet, email access and network access. Online access to the School network is through a unique, audited username and password;

We provide pupils with an individual network log-in username. They are also expected to use and protect a personal password which should not be shared with others (including parents);

All pupils have their own unique username and password which gives them access to the Internet, and *their own school approved email account*;

All email accounts are protected with Multi Factor Authentication;

Makes clear that no one should log on as another user and that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

Has a shared work area on the network for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

Requires all users to always log off when they have finished working or are leaving the computer unattended;

Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and automatically switches off all computers at 5.30 pm to conserve energy;

Has set-up the network so that users cannot download executable files / programmes;

Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities.

Maintains equipment to ensure Health and Safety is followed; equipment installed and checked by approved Suppliers;

Has integrated curriculum and administration networks, but access to the Management Information System (iSAMS) is set-up so as to ensure staff users can only access modules related to their role;

Ensures that access to the school's network resources from remote locations by staff is severely restricted and access is only through school-approved systems;

Does not allow any outside Agency to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or iSAMS Support, parents use a secure portals (ISAMS for academic data, VECTARE for the School Coach Service, SOCS for the Co-Curriculum programme, EVOLVE for School Trips) to access information on their child;

Provides pupils and staff with access to content and academic resources through SharePoint which staff and pupils and access using their username and password;

Has clear procedures for the daily back up of iSAMS and other important data and systems;

Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data;
Our wireless network has been secured to industry-standard Enterprise security level /appropriate standards suitable for educational use;
All computer equipment is installed professionally and meets health and safety standards;
Projectors are maintained so that the quality of presentations remains high;
Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private;

- From 2025, the School requires that an individual passwords must be 15+ characters long. Longer, stronger passwords offer better protection and reduce the need for frequent updates.
- Use a combination of words or a passphrase that you can easily remember but is hard for others to guess.
- Includes a mix of **letters, numbers, and symbols** if possible.
- Avoids using personal information such as names, dates, or common phrases.

For example, a strong password could look like: ***BrightBananaFootball1991!***

Password can be tested at: https://bitwarden.com/password-strength/

Users cannot use any of the last three passwords. It is the intention to only change passwords if there is a suspicion that a user account has been compromised.

E-mail

This school:

Provides staff with an email account for their professional use, and makes clear that personal email use should largely be through a separate account;
Does not publish personal e-mail addresses of pupils on the school website;
Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
Will ensure that email accounts are maintained and up to date;
Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police;
Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of cyber security technologies to help protect users and systems in the school, including Barracuda Total Email Protection, Watchguard AD360 EDR, Fortigate web filtering, plus direct Microsoft email filters. These are designed to block malware including viruses, Trojans, pornography, phishing and inappropriate language.

(Barracuda has been a member of the Internet Watchfoundation since 2009)
(Microsoft has been a member of the Internet Watchfoundation since 2001)

Personal Data

This School regularly scans user accounts for personal documentation of potential interest to cyber criminals. Where such documents are found, users are invited to remove them from School systems. MTS uses the Barracuda data Inspector tool.

Pupils

Pupils are introduced to and use e-mail as part of their routine way of working at Merchant Taylors'.

Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

KCSIE 2024 requires Filtering and Monitoring for all pupils devices brought into School. This would seem to include pupil smart phones to which the School does not have ready access. Safeguarding risks here are mitigated by School policy where pupils are not permitted to use their phones during the School day without the expressed permission of a member of staff. Pupils are permitted to connect their phones to the student wireless network which has the same filtering as the desktop devices. But the School cannot prevent a determined attempt to access a personal 4G or 5 G connection. The School walls are made of thick concrete and there are no mobile phone masts near the School site.

Parents:

Updated guidance to KCSIE first published in September 2023 onwards requires additional monitoring of School systems and internet filtering. In particular, parents are not subject to safeguarding DBS verification. They must understand that they do not have access to the email accounts provided to their sons by the School. This is because access to their son's email account provides potential access to other pupils at the School.

Staff

Staff should use the School e-mail systems for professional purposes and only use the School email system for personal matters sparingly;

Never use email to transfer staff or pupil personal data outside the School network;

Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

The sending of multiple or large attachments is limited to a file size of 30Mb, and may also be restricted by the provider of the service being used;

The sending of chain letters is not permitted;

Embedding adverts is not allowed.

School Website

The Head Master takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

Uploading of information is restricted to our website authorisers: Senior Master, Director of Marketing and Admissions and the IT Team;

Uploading of information can only take place via the School IP-address

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

Photographs and videos published on the web do not have full names attached;

Learning platform

Uploading of information on the schools' Teams and SharePoint system is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas. Many Teams are created automatically by Locker Connect, but all teams with pupil and teacher membership should have at least two teachers assigned.

Social networking

Teachers must not run social network spaces for student use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

School staff strongly recommends that in private use:

No reference should be made in social media to students / pupils, parents / guardians or school staff;

They do not engage in online discussion on personal matters relating to members of the school community;

Personal opinions should not be attributed to the School;

Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

It is now recommended practice for teaching staff to change their profile names on sites such as Facebook and for example if their name was Robert James Chadwick that they drop the surname Chadwick and just go by Robert James, making them a lot harder to find.

The appropriate use of social media by school staff is discussed as part of their Safeguarding Induction training and there are regular reminders to staff about how to protect themselves online by email or at Communications.

CCTV

We have CCTV in the school as part of our site surveillance for staff and pupil safety. We will not reveal any recordings (*retained by the School for 28 days*), without permission of all those who appear in the footage (and parents, for pupils) except where disclosed to the Police or other external agencies as part of a criminal investigation or following child protection procedures.

4. Equipment and Digital Content

Pupils use smartphones and mobile devices in School – Please refer to details contained in **MTS CODE OF USE FOR MOBILE TELEPHONES**

Staff use of personal devices

Staff are advised not to use their own smartphones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity (unless using a software-based phone system such as 3CX);

Staff should not ideally use personally owned devices, such as smartphones or cameras, to take photos or videos of pupils and should normally only use work-provided equipment for this purpose. Where circumstances require a member of staff to use their own smart phone to record

photographic or video footage, this material should be downloaded to the School network and deleted from the personal device as soon as is practical;
Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone can be provided and requested. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

We obtain parental / carer permission for the use of digital photographs or video involving their child as part of the school agreement form when their son joins the school;
We do not identify pupils full names of pupils in the credits of any published school-produced video materials / DVDs or advertising campaigns;
If specific pupil photos (not group photos) are requested for advertising purposes by third party organisations the school will obtain individual parental or pupil permission for its long-term use;
The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose; this extends to our obligations with regard to the Prevent Duty Guidance issued under section 29 of the Counter-Terrorism and Security Act, 2015. Following Home Office guidance about tackling radicalisation, MTS does not allow pupils independent access to Facebook, Twitter/X, YouTube, Ask.FM, Tumblr, Snapchat, Instagram, and Private messaging services, not limited to but including WhatsApp, Kik, Tik Tok Telegram and Viber, all of which are considered be potential sources of terrorist and extremist material.
As with AI tools, each application has a minimum age of use. For the each applications listed above, the current minimum ages are.
Facebook (13)
Twitter/X (13)
YouTube (13)
Ask.FM (13)
Tumblr (13)
Snapchat (13)
Instagram (13)
Whatsapp (13)
Kik (13)
Tik Tok (13)
Telegram (16)
Viber(13)
Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Senior Master
January 2025