Merchant Taylors' School

ACCEPTABLE USE OF INFORMATION AND COMMUNICATION DEVICES WITHIN THE MTS COMMUNITY

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

1. Introduction

Merchant Taylors' provides pupils with access to its computer network, portals, email systems and connectivity. Pupils are responsible for good behaviour, whether on the school computer network or using their own devices or home connectivity. All pupils' behaviour within the MTS community, defined in its broadest sense, must be consistent with the educational objectives of the school and with these guidelines.

All reasonable attempts will be made to protect a pupil's right to privacy and – subject to their strict adherence to the school's acceptable use policy – pupils may enjoy the use of school networks and connectivity to enrich their studies without undue intrusion. This privilege may, however, be withdrawn without notice at any time.

This statement aims to protect pupils from carrying out activities that may be inappropriate. The school has a duty of care to its pupils and despite the immense educational potential of ICT, there is an unsavoury side to the internet and other current aspects of technology use on mobile devices, which it would be irresponsible to ignore.

We anticipate that, by making it clear to the pupils just how seriously we view misuse of the school's facilities, connectivity or privately-owned communication devices, we will protect the pupils, help them avoid problems and make their experience of ICT at MTS a happy and productive one. Failure to comply with this policy will constitute a disciplinary offence and will be dealt with under the School's Sanctions Disciplinary Procedures.

2. Scope and Definitions

This policy applies to the use of the School's ICT systems and connectivity and to privately owned mobile phones, tablets and laptops used within the MTS community.

The specific list of social media and messaging platforms, along with minimum ages, is maintained in Living Appendix A (Social Media Platforms & Minimum Ages). This appendix is updated at least annually and may be updated sooner if required.

3. Permitted and Prohibited Uses

Pupils are responsible for the integrity of their digital devices. It is a condition of bringing a device to School that the owner accepts full responsibility for everything done using that device and its connectivity: “I lent it to someone and they did this” is not an acceptable excuse.

Pupils are responsible for the security of their password, the integrity of their network area and the appropriate use of privately owned communication devices; they must keep their password secret. “Someone logged on as me” is not an acceptable excuse.

Pupils must not damage computers or the computer network; nor should they hack, vandalise, damage or disable the personal or intellectual property of another person or organisation.

Pupils must not pirate software, distribute already pirated software, compromise school licensing, debilitate or disable computers, systems or networks through the misuse or overuse of electronic distribution or the spreading of computer viruses through the inappropriate use of files, removable media or other mass storage devices.

Pupils must not place any unauthorised applications on the school’s network (*.exe – or equivalent).

Pupils must not compromise the security or integrity of any ICT systems, whether from inside or outside the school and whether that system is owned by the school or by other organisations or individuals.

Access to the school's computer system must be through a pupil's authorised account only; pupils must not give out or share their password.

Pupils must not use another person's password or trespass in another person's folders, work or files.

School computer and internet use should be appropriate to a pupil's education. Under no circumstances must pupils attempt to hack, crack or otherwise circumvent the school filter (e.g. by the installation of other browsers or plug-ins). It is against school rules for any pupil to have proxy/bypass applications on any device whatsoever within school.

Pupils must not gamble or access, upload, download, transmit, display, or distribute obscene material or material that in any way could be construed as bringing the school’s good name into disrepute. The use of obscene, abusive, or sexually explicit language is

not permitted on MTS electronic resources, privately owned devices used on the MTS campus or social networking spaces that are linked to or could be identified with the school. The use of the school computer system for political purposes or advertising is forbidden without the permission of a teacher, which will be given only for legitimate school activities (e.g., Amnesty, Young Enterprise).

Pupils must not transmit, re-transmit, distribute, publish, promote, market, or store material on or through the school network or the internet, which is threatening, abusive, hateful, obscene, indecent, or defamatory or involves or encourages conduct that may constitute a criminal offence.

Pupils are responsible for messages, posts, images or equivalent they send out or those that are sent from their accounts or devices. Electronic communications should be written carefully and politely; pupils cannot expect that messages will always be private.

Anonymous messages, spam, chain letters, prank messages, phishing, spoofing and virals must not be sent or forwarded. All forms of cyber-bullying are strictly forbidden.

Emails/social networking posts commenting on the appearance of other pupils/teachers are unacceptable.

Any unpleasant material or messages received or found in a pupil's area or on a pupil's mobile device must be reported. During school hours pupils should not use any other messaging software than Teams chat and the school email system; the use of these is only for discussion of school-related activities.

Pupils must not give out their home address or telephone number or arrange to meet someone online unless they have written permission from their parent, carer or teacher.

Pupils must not post any private information concerning any other pupil, such as their address, email or telephone number. This includes adding the email addresses of others to mailing lists.

Pupils must not use camera/video facilities in mobile phones, tablets or laptops to photograph other members of the school community without their express permission for a justifiable educational objective. They must under no circumstances post image/video files (or links to such files) of other members of the school community without their express permission.

Pupils must not post anything, including imagery or audio/video files, about any other member of the school community on any internet site that might be construed as defamatory, malicious, misleading, or serving to bring the school's good name into disrepute. This extends to private communities within social networking spaces, blogs and wikis. The school reserves the right to treat with the utmost severity any posts that in

our opinion constitute cyber-bullying; use inappropriate and offensive language; have malicious racial or other discriminatory content; or, in any way bring the school's good name into disrepute or provoke anti-social or violent behaviour.

Pupils must remember that not only the school website but also any social networking presence linked to the school presents the face of the school to the world. We insist on high standards of content, accuracy and presentation.

Pupils must not violate copyright, or otherwise use another person's intellectual property without prior approval or proper citation. Pupils must not attempt to pass off internet information as their own. Copying or downloading copyrighted materials from the internet is the same as copying from another pupil; it is cheating and intellectual theft and will be punished as such.

Pupils must not transmit, re-transmit, distribute, publish, promote, market, or store material on or through the school network which constitutes an infringement of privacy or copyright, or involves the transmission, distribution, or storage of information or data in breach of any law (including copyright).

4. Monitoring and Privacy

With the adoption of digital learning at MTS and safeguarding obligations, the School deploys monitoring software on pupil-facing School desktop PCs and on pupil personal devices used for School purposes. Monitoring is subcontracted to the SENSO Assisted Monitoring Service and operates 24/7 (incorporating weekends and holidays). This may include the triggering of alerts based on detection of particular keywords and the capture of screenshots. Monitoring data is held by SENSO and is retained as part of the MTS pupil record. Pupils who use inappropriate terms or indulge in inappropriate behaviour may be subject to School disciplinary procedures.

A non-exhaustive list of types of key-phrases that are monitored includes: very high risk items suggesting risk of immediate harm (e.g., suicide, self-harm, criminal activity, violence, terrorism, sexual abuse, grooming); high risk items (e.g., racism, homophobia, misogyny, bullying, pornography, illegal drugs, sexual harassment); and lower risk items (e.g., offensive language).

In addition to key phrase monitoring, SENSO also monitors

- **Browsing Activity**: Senso tracks websites visited, including timestamps and URLs, to monitor for inappropriate or harmful content.
- **Chat and Messaging**: The platform monitors chat messages, including those in Microsoft Teams, using AI and keyword algorithms to detect potential threats or concerning behaviour.

- **Screen content and Image Analysis**: Senso employs AI-driven visual threat analysis to inspect images for potential risks, such as explicit content or indicators of self-harm

5. Cooperation and Device Inspection

Personal computers and any mass-storage devices or media that are under the control or in the possession of pupils may be examined by staff, including ICT Technical Services staff, at any time on reasonable grounds of suspicion that a breach of school rules has occurred.

Such devices may be seized and removed for the purposes of examination, which may include inspection, backing up, imaging or copying relevant parts of the devices, as well as obtaining print-outs of files, logs, caches and data.

Seizure and examination are carried out only with the Head Master's authority and with the co-operation of the pupil or parent. At least two members of staff will be present throughout the examination; where possible the pupil will be invited to be present. The pupil must give account of any relevant logon names and passwords when these are requested.

Parents and pupils are expected to co-operate. Should co-operation be denied the school reserves the right to ban the machine from the MTS campus and – in cases where it believes that the law has been broken – to impound the machine and call the relevant authorities.

6. Parental Consents and Communications

Parents should be aware that occasionally, in order to advise of last minute changes, it may be necessary for staff leading trips to contact their son on his mobile. Where practicalities permit, we will also try to make contact by email.

New parents are issued with the Acceptable Use Policy prior to their son joining MTS. They are asked to consent to: direct contact on a pupil’s mobile device during a School trip, visit or other bona fide School activity; publication of pupil work on the school website; and publication of photographs that include their son, subject to the principle that photographs will be un-named. Parents confirm they have read and understood the School rules for acceptable use and give permission for internet access, noting that whilst the School takes all reasonable precautions to prevent access to inappropriate materials, it cannot be held responsible for the nature or content of materials accessed via the internet, nor liable for damages arising from use of internet facilities.

7. Social Media and Messaging Platforms

For clarity and future-proofing, references to specific platforms are replaced with categories such as: public social networking sites, private/direct messaging apps, media sharing platforms (video, image, livestreaming), and discussion forums. Pupils must adhere to the minimum age requirements set by each platform and to School rules at all times. The current list of commonly used platforms and their minimum ages is set out in Living Appendix A.

Use of Artificial Intelligence (AI) Tools (for further details read the School AI Policy)

New AI technologies are emerging at an unparalleled rate; therefore, this policy will be reviewed at least annually, and more frequently where significant changes occur. The list of AI tools and minimum ages in Living Appendix B is indicative, not exhaustive, and subject to change.

The focus of this policy is to ensure that students create and submit assessments in a manner that is fair and, where needed, transparent. MTS will follow JCQ guidance when dealing with assessments submitted by students where there are suspicions that unfair use of AI has occurred.

Students must explicitly acknowledge any use of AI tools in the final piece of work (including internal assignments, NEAs and other assessed work). Acknowledgement must specify the tool used, the date accessed, and the nature of assistance (e.g., idea generation, outline, code suggestion, translation). Where AI has been deployed, students must retain a non-editable copy (e.g., screenshot) of prompts and AI-generated content used for reference and authentication purposes.

Where concerns arise about authenticity, teachers may use AI-detection indicators, eg Turnitin and other methods (e.g., comparison with known work, supervised oral checks). Detection results will always be considered alongside other evidence; they are indicators, not determinations.

Examples of AI misuse include, but are not limited to: copying or paraphrasing AI-generated content without proper acknowledgement; using AI to complete parts of an assessment such that the work does not reflect the student's own analysis, evaluation or calculations; failing to acknowledge use of AI tools; or submitting work with intentionally incomplete or misleading references or bibliographies.

Staff will ensure that departments discuss acceptable and unacceptable use of AI in their subjects, including where limited, ethical use may be permitted for formative (non-assessed) learning activities (e.g., brainstorming, idea harvesting, language support, debugging concepts) provided such use is acknowledged in submitted work.

Students are expected to demonstrate their own knowledge, skills and understanding as required for the qualification in question. Any use of AI which means students have not independently demonstrated their own attainment is likely to be considered malpractice.

Refer to Living Appendix B for an indicative list of AI tools and stated minimum ages according to provider terms, which may change. Pupils in year groups below a platform's minimum age must not use that platform.

Living Appendix A – Social Media Platforms & Minimum Ages

Maintained by the Senior Master (or delegated role). Reviewed at least annually or sooner if required due to changes in platform availability or usage.

Last updated: 14 August 2025

Platform / Category	Example Services	Stated Minimum Age*
Public social networking	Facebook, X (Twitter), Threads, Bluesky	Typically 13
Private/direct messaging	WhatsApp, Telegram, Signal, Discord (DMs)	Typically 13–16**
Media sharing – video	YouTube, TikTok, Twitch	Typically 13
Media sharing – images	Instagram, Snapchat, Pinterest	Typically 13
Community/Forums	Reddit, Quora, Discord servers	Typically 13
Collaboration/Creation	Canva, Notion, Figma	Typically 13–16
Location-based/social discovery	BeReal, Yubo	Typically 13–16

*Based on provider terms as at the date above; platform terms change and may vary by jurisdiction.

**Some services may require higher ages or parental consent in specific regions.

Living Appendix B – AI Tools & Minimum Ages (Indicative)

Maintained by the Senior Master (or delegated role). Reviewed at least annually or sooner if required due to changes in tool availability or usage.

Last updated: 14 August 2025

Tool Category	Example Tools	Stated Minimum Age*
General-purpose chatbots (text)	ChatGPT, Claude, Gemini, Copilot	Typically 13–18**
Image generation	DALL·E, Midjourney, Stable Diffusion	Typically 13–18**
Writing assistants	Jasper, Writesonic, Grammarly	Typically 13–18**
STEM & learning aids	Khanmigo, Wolfram	Typically 13–18**
Coding assistants	GitHub Copilot, Codeium	Typically 13–18**

*Providers' terms vary and change frequently. This list is indicative, not exhaustive.
**Some tools or regions require age 18 or a legal contract capacity; parental consent may be required for under-18s.

Merchant Taylors' School

AI Usage Acknowledgement Form

Last updated: 14 August 2025

This form must be appended to any assessed work where AI tools have been used in any capacity. It ensures compliance with the School's Acceptable Use Policy and AI Policy.

Name: _____

Date: _____

Assignment Title: _____

AI Tool(s) Used (e.g., ChatGPT, DALL·E): _____

Date Accessed: _____

Description of Use (e.g., idea generation, outline, translation):
_____
_____

Evidence Provided (non-editable copy of AI output): Yes / No

Declaration: I confirm that this work is my own, and any AI use has been appropriately acknowledged above. I understand that undisclosed AI use may be treated as malpractice under School and JCQ rules.

Signature: _____ Date: _____

Merchant Taylors' School

Staff Quick-Guide – Acceptable Use & AI Policy

Last updated: 14 August 2025

This quick-reference guide summarises key responsibilities for staff regarding ICT acceptable use and AI policy.

- Key Points for All Staff:
    - Remind pupils: School rules apply to mobile phones, tablets, and laptops on campus.
    - Check that AI Usage Acknowledgement Form is attached to assessed work where AI has been used.
    - Ensure AI use is acknowledged in final work – specify tool, date, purpose, and evidence.
    - Do not rely solely on AI detection tools – combine with other evidence (e.g., previous work comparison).
    - Escalate suspected malpractice to SLT/Exams Officer promptly.
    - Reinforce digital respect and safeguarding expectations during lessons and online activities.
- Escalation Triggers:
    - Evidence or strong suspicion of undisclosed AI use.
    - Breach of acceptable use (e.g., cyberbullying, security compromise).
    - Inappropriate online behaviour linked to the school community.

Always refer to the full Acceptable Use Policy for complete guidance.

Merchant Taylors' School

Pupil-Friendly Guide – ICT & AI Rules

Last updated: 14 August 2025

- DOs:
    - Use your mobile, tablet, or laptop responsibly and for school work.
    - Keep your passwords private – you are responsible for your account.
    - Be polite and respectful in all messages, posts, and online content.
    - Report anything unpleasant or worrying to a teacher.
    - If you use AI for work, complete the AI Usage Acknowledgement Form and submit it along with your final assignment.
- DON'Ts:
    - Don't use other people's accounts or passwords.
    - Don't bypass school internet filters or use proxy apps.
    - Don't share personal information about yourself or others.
    - Don't post anything that could harm, upset, or embarrass others.
    - Don't copy AI-generated work without saying it's from AI.

Remember: Using technology at MTS is a privilege – use it wisely, respectfully, and safely.