Merchant Taylors’ School

ACCEPTABLE USE OF INFORMATION AND COMMUNICATION DEVICES WITHIN THE MTS COMMUNITY

Policy Custodian: Deputy Head Information Systems
Approving Body: MTS Senior Leadership Team
Approved: July 2021
(This policy does not apply to Merchant Taylors’ Prep.)

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 This privilege may, however, be withdrawn without notice at any time.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.

*In addition, these guidelines extend to <u>all</u> information and communication technology devices, including privately-owned 3G, 4G or 5G mobile phones, including but not limited to *iPhones, Androids, iPods*, ipads, smart watches, tablets, USBs, external hard drives, CDs, DVDs, social networking sites (e.g. *Facebook, FlickR*, Whatsapp, Instagram, Snapchat, Houseparty, Tiktok and Twitter).

- Access to the MTS network, Firefly VLE, the School’s Office-365 subscription and social networking community is a privilege, not a right: access entails responsibility and inappropriate use will mean loss of access.
- Pupils are responsible for the integrity of their digital devices. It is a condition of bringing a smart phone to School that the owner accepts full responsibility for everything done using that phone 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, CD/DVDs, USBs, *PSPs, iPods*, *iPhones,* games consoles, smartphones, 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 such as *Mozilla Firefox*). It is against school rules for any pupil to have *Ultrasurf* or any equivalent 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). Legitimate School societies supported by a named member of staff are welcome to use the School's own social networking space.
- 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 email/SMS/MMS messages/tweets/posts/images or equivalent they send out or those that are sent from their accounts or devices. Email/SMS/MMS messages/posts should be written carefully and politely; pupils cannot expect that email/SMS/MMS messages will always be private.
- Anonymous messages, spam, chain letters, prank messages, phishes, spoofs, 'joe jobs' and virals must not be sent or forwarded. All forms of cyber-beefing such as fraping are strictly forbidden.
- Emails/SMS/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.
- The use of computer 'chat' or 'messaging' over the school network in any form is not allowed without the express permission of a teacher, for a specific academic purpose.
- 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/SMS any private information concerning any other pupil, such as their address, email or telephone number. This includes adding the mail addresses of others to mailing lists.
- Pupils must not use camera/video facilities in mobile phones or other devices 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. All surfing and posting (whether using the school network or privately owned devices such as but not limited to 3G/4G/5G mobile devices, smart watches, ipads and other tablet devices) must be compatible with the high standards of behaviour expected of MTS pupils.

- Pupils must not post anything, including imagery or video/audio 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 even to private communities within social networking spaces, Blogs and Wikis: MTS is opposed to all forms of bullying and just as physical bullying remains bullying even if it is not conducted in a public space, the same is true for cyber-bullying. Pupils must not administer or 'lurk' in social networking groups that are in any way malicious or may be construed as bringing the school's good name into disrepute. The school reserves the right to treat with the utmost severity any posts that in our opinion constitute: "cyber bullying"; fraping; use inappropriate and offensive language; have malicious racialist or other content; or, in any way bring the school's good name into disrepute or provoke anti-social or violent behaviour. We expect, in such situations, that pupils will co-operate in providing details of relevant ISPs and IP addresses, so as to prevent "spoofing" and help us determine the facts of what has occurred. Spoofing (a situation in which one person or program masquerades as another) in any form of digital communication will never be accepted as acceptable behaviour. Pupils must be aware that the above activities may be considered incompatible with study at Merchant Taylors' School and that, in exceptional cases, the school may have a responsibility to involve Social Services or the Police.
- 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. Material submitted to the school website and social networking sites will conform to the aims above and to the normal school rules on the use of appropriate language and behaviour.
- Pupils must not violate copyright, or otherwise use another person's intellectual property without his or her 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 (via privately owned devices and storage media) through the school network or over the internet which constitutes an infringement of privacy, copyright or involves the transmission, distribution, or storage of information or data in breach of any law (including copyright).
- The school reserves its right to monitor the use of all relevant computer systems by electronic means without prior notification to the user. This will include: the monitoring of web and social networking sites; the interception of emails; the deletion of inappropriate materials in circumstances where the school believes unauthorised use of its computer system is or might be taking place, or the system is being used for wrongful purposes or for storing text or imagery which is unauthorised or unlawful.
- In effect, privately owned devices including but not limited to laptops, tablets, USBs, 3G/4G/5G-smart phones, *iPhones*, *iPods, ipads* etc. are containers, like rucksacks and may hold disturbing images, unauthorized copies of copyrighted material, offensive or threatening letters. Therefore 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 (as may happen on suspicion of other contraband material held against school rules, such as alcohol or tobacco).
- Such devices may be seized and removed for the purposes of such an examination: examination may include inspection, backing up, imaging or copying relevant parts of (and if necessary all) the hard drives of such devices, as well as obtaining print-outs of files, logs, caches and data on the device.
- Seizure and examination are carried out only with the Head Master's authority and with the co-operation of either 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 in this matter. 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 (Social Services, Police, etc.).
- 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.

Additional sanctions for inappropriate behaviour and communication shall be governed by the school's normal disciplinary procedures. Pupils must be aware that the above activities may be considered incompatible with study at Merchant Taylors' School and that, in exceptional cases, the school may have a responsibility to involve Social Services or the Police.

Before any pupil may use the school computers, the parent or guardian must sign the **Parental Consent Letter** *and return it by hand, via the pupil, to the Common Room Secretary in the School Administration Office, together with the* **Pupil Agreement Form**.

The Common Room Secretary will issue the pupil with login credentials when the form is returned. Pupils may not use the computer facilities in school until they return this form. Once issued with these login credentials, first login into the School network must be via a School terminal.

* Although devices, forms of cyber-bullying, internet and social networking sites specified in this policy are referred to by brand name for quickness of communication and ease of understanding, the policy should be understood as being agnostic with regard to brand and applicable to equivalent devices, websites, or forms of bullying regardless of manufacturer, internet services provider, or minor variation in bullying strategy.

Deputy Head Information Systems