MERCHANT TAYLORS' SCHOOLS

For Boys and Girls aged 4 to 18 years

ICT & Social Media Acceptable Use Policy - Staff

Title ICT & Social Media Acceptable Use Policy (Staff)	
Author:	DWI
Last Amended:	December 2018
Review:	December 2019

1. Introduction and Scope

To whom does this policy apply?

- All staff members of Merchant Taylors' Schools who may have access to a computer owned by the school, regardless of whether or not they use it in their day to day work routine.
- All staff members of Merchant Taylors' Schools who may be connecting their own personal ICT equipment to the school network, including e-mail and internet services.
- All visitors/guests/contractors/governors of Merchant Taylors' Schools who may be connecting to the school network, either via school equipment or their own personal equipment.

In this policy "staff" includes all teaching and non-teaching staff, including peripatetic, supply and volunteer staff.

2. Purpose

Merchant Taylors' Schools embrace the use of ICT to enhance teaching and learning, to simplify administrative tasks and to communicate with the world. All organisations, including schools, are required to have a policy such as this to outline the principles underpinning appropriate use of computer equipment. The purpose of this policy is to state clearly the obligations of staff and visitors and any other user in using the ICT facilities of Merchant Taylors' Schools (whether on School premises or accessed remotely), including acceptable access and use of the internet, and to ensure that users are fully aware of the consequences of not following this code of practice.

This Acceptable Use Policy (AUP) has been compiled to provide all users guidance on what is appropriate use of ICT within Merchant Taylors' Schools and draws upon information from:

- Computer Misuse Act (1990)
- Data Protection Act (1998)
- Copyright, Designs & Patent Act (1988)
- Health and Safety (Display Screen Equipment) Regulations (1992, amended 2002)
- Child Exploitation and Online Protection Centre (CEOP)
- The National Society for the Prevention of Cruelty to Children (NSPCC).

This policy should be read alongside the staff code of conduct and the Data Protection Policy.

3. Consequences of Unacceptable Use

Failure to abide by this AUP will be treated as a disciplinary offence for staff in the same way as any other misconduct issue (see Staff Handbook) – the ultimate sanction being dismissal. Suspected illegal activities will be reported to the police and, if necessary, the Local Safeguarding Children's Board.

4. Communicating this policy

The staff AUP is published on the Merchant Taylors' website and a copy is given to each member of staff when they join the School as part of their induction process. Each member of staff is required to sign the ICT AUP Agreement and return this to the Deputy Head of their School (for teaching staff) or Bursar/DFO (for support staff). These will then be held on the staff file, by HR. By signing, staff agree to abide by the principles laid down in this document and to all amendments which will be published on the Schools' website from time to time, unless the ICT Director is notified in writing by an individual and the departure from this agreement is agreed by the Deputy Head or Bursar/DFO.

Visitors must be advised of the ICT AUP when attending the School. A copy will be held in Reception.

5. General Computer Use

In general, use of ICT equipment, email and the internet within the School should primarily be to enhance teaching and learning or for administrative use for School business. It is understood that users may occasionally need to use ICT for personal reasons and this is permitted so long as such use does not have a negative impact on their work (or the work of others) or the efficient functioning of the ICT facilities and does not conflict with other aspects of this code of practice or the staff code of conduct. Such incidental personal use is a privilege and not a right and may be withdrawn if abused.

Use of School resources and facilities for business purposes not related to School activities or for personal gain is not permitted.

If necessary, routine communication with pupils about work, homework etc. will normally take place via the virtual learning environment, Firefly, or School email accounts.

All property belonging to the School should be treated with respect and reasonable care. Any faults or breakages must be reported to the ICT Department immediately.

The School reserves the right to keep a record of staff browsing histories.

6. Security

All staff are responsible for the care and safe-keeping of any School-owned ICT equipment issued to them. They also have an important role to play in maintaining the security of the School network. To that end, staff must:

- keep portable equipment such as laptops, iPads, Surface Pros etc. securely locked away when not in use
- only use the School network under their own username and password. Passwords should not be obvious to other users (e.g. name or birthday), and should be a mix of uppercase and lowercase letters, numbers and special characters (e.g. #, &, !) and be 12 characters or more in length. Passwords must never be shared with anyone else.

- not download or install software packages without the authority of the ICT Services Department
- comply with the Copyright, Designs and Patents Act 1988 by not installing unlicensed software on any School device and by not copying licensed software for installation on another machine
- take particular care of portable equipment when it is taken "off-site"
- pay particular attention to logging off/locking machines whenever they are left unattended, whether on School premises or offsite (e.g. at home).

7. Safety

Staff must:

- take care with liquids (drinks etc.) around ICT equipment and be aware of the risk posed by liquids to electrical equipment
- comply with the Health & Safety (Display Screen Equipment) Regulations 1992 (amended 2002) by ensuring that they:
    - are comfortable when using equipment
    - adjust keyboard and mouse to ensure comfortable and suitable data input positions
    - adjust the screen position, resolution contrast and brightness to enable easy reading
    - keep their screens clean
    - do not sit in the same position for many hours and take regular breaks.

If any user would like advice about their safety when using ICT equipment, they should contact the ICT Director.

8. Unacceptable Use

In general, it is unacceptable for users to engage in activity which is illegal, offensive or likely to cause the reputation and good name of the Schools to be undermined.

Activities prohibited under this policy include, but are not restricted to:

- Cyberbullying – the sending of unpleasant, abusive or aggressive messages via email, messaging service, any social media platform or any other electronic media
- Accessing sites which may be legal but are unacceptable for an educational establishment. They may include sites relating to or promoting pornography, radicalisation or extremist views, terrorism, racism, gambling or anything which may be offensive, violent, dangerous or inflammatory
- Hacking – attempting to gain access to folders, databases or other material on the School network or via the internet to which one is not entitled
- Communicating with pupils via personal email addresses and/or personal social media accounts.

It should be remembered that e-mails are subject to data protection in the same way as other forms of written word and are therefore potentially disclosable under a subject access request. Therefore, they should be treated in the same way as other forms of written communication and should not include

anything abusive, discriminatory or defamatory. E-mails are also disclosable as evidence in court proceedings and even if deleted, a copy may exist on a back-up system or other storage area.

9. Social Media

This policy differentiates between the staff use of social media for personal reasons and use on School business. School departments and clubs will often set up their own social media pages to update pupils with information – this is entirely acceptable. These accounts must allow access by all. The ICT Services Department and members of SMT reserve the right to access these accounts to monitor their use.

Many staff will have a personal online presence via networking sites such as Facebook, LinkedIn, Instagram, Twitter or similar, or via blogging sites or their own personal websites. Activity on these personal platforms must have regard to the spirit of this AUP and must never put the security or reputation of the Schools, pupils or employees under threat. Staff may find the following advice on their personal use of social media useful:

i. Staff are advised not to identify themselves as members of Merchant Taylors' Schools Crosby in their online profiles.

ii. Staff may not, under any circumstances, 'friend' a pupil via their personal social media. They should use professional judgment in relation to "friending" former pupils and parents.

iii. Staff should be aware that making extreme political, religious or philosophical comments on social media may attract unnecessary attention and require the Schools to intervene.

iv. Staff must not use social media to document or distribute evidence of activities in their private lives which might bring the Schools into disrepute.

v. School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

vi. Under no circumstances may staff upload to personal sites images or video of pupils or other staff without explicit permission.

vii. Staff must not use social media and the internet in any way to attack, insult, abuse or defame anyone who is a member of the Merchant Taylors' community nor to discuss personal information about them; such action will be taken very seriously. Where there is a suspicion of any illegal activity, the police may be informed.

viii. Under no circumstances may Merchant Taylors' logos, crests, typefaces or brands be used or published on any personal web space or on any online or offline medium without the prior agreement of the Director of Marketing.

10. Monitoring

The School regularly monitors and accesses the School IT system (hardware, software, e-mail account, telephone) for purposes connected with the operation of the School. The School reserves the right to use software which automatically monitors the School IT system (e.g. it would raise an alert if a member of staff visited a blocked site or sent an e-mail containing an inappropriate word). The purposes of such monitoring and accessing include:

i. To help the School with its day to day operations e.g. if a member of staff is off sick or on holiday their e-mail account may be monitored in case urgent e-mails are received.

ii. To check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations e.g. to investigate allegations that a member of staff has been using their e-mail account to send abusive messages.

Such monitoring is carried out by the ICT Department under instruction from the Head of the relevant School or Bursar/DFO. Anything so revealed is shared only with the Head or Bursar/DFO, unless suspected to be illegal in which case it will be referred to the police and/or Local Safeguarding Children's Board.

MERCHANT TAYLORS' SCHOOLS
STAFF ICT & SOCIAL MEDIA ACCEPTABLE USE POLICY
AGREEMENT

All staff are required to comply with the Merchant Taylors' Schools Staff ICT Acceptable Use Policy.

Please sign and return to the Deputy Head (teaching staff) or HR (support staff).

✂----------

MERCHANT TAYLORS' SCHOOLS
STAFF ICT ACCEPTABLE USE POLICY
AGREEMENT

I have read and understand and agree to be bound by the conditions of the Merchant Taylors' Schools Staff ICT Acceptable Use Policy.

NAME (please print): _____

DEPARTMENT: _____

Signed: _____

Date: _____

Please sign and return to your Deputy Head (teaching staff) or HR (support staff).