ICT Acceptable Use Policy - Pupil

ICT Acceptable Use (Pupil)
Applicable To: Whole School
Author: Chief Operating Officer
Last Amended: September 2021
Review: September 2022

ICT ACCEPTABLE USE POLICY – Pupil

1.   Introduction

The ICT Service Department, its resources and its staff are committed to providing an excellent service to staff and pupils. The facilities exist to support the aims and objectives of the Schools and as such must be treated with respect at all times. In particular, the ICT Service staff seek to support the acquisition of knowledge and skills and to support the development of initiative, confidence, independence, self-discipline and a strong sense of values.

This document defines the Merchant Taylors' Schools' policy in respect of the acceptable use of their information and communication (ICT) facilities and all pupils must make themselves familiar with this policy as violations may lead to disciplinary action.

2.   Purpose

The ICT Service Department is responsible, on behalf of the Schools, for providing a safe environment in which to learn and achieve educational objectives. In so doing, the ICT Service Department will seek to provide a first-class service whilst at the same time minimising and containing potential risks to the Schools and their members.

The purpose of this policy is therefore to state clearly both pupils' obligations in using these facilities and the ICT Service Department's responsibility and authority in taking action of safeguard them.

2.1   Personal Responsibility

Pupils, staff and all other users of the ICT system must accept personal responsibility for using the ICT facilities with respect and in accordance with this policy. It is the responsibility of all pupils to report any misuse of the network to a staff member. Misuse may come in many forms but it may commonly be viewed as information on the computer system which suggests:

- pornography
- unethical or illegal requests
- racism
- sexism
- inappropriate language
- any material which may be likely to cause offence.

Misuse of the network may also involve the deliberate streaming of large data files or any other practice which will deliberately slow down the network speed.

Merchant Taylors' Schools make no warranties of any kind whether expressed or implied for the network service they are providing. The Schools will not be responsible for any damages suffered whilst using the system, including loss of data as a result of delays, non-deliveries, mis-deliveries nor service interruptions caused by the system or elements of it, or your errors or omissions. Use of any information obtained via the network or other information systems is at your own risk. Merchant Taylors' Schools specifically deny any responsibility for the accuracy of information obtained via its Internet services.

ICT Acceptable Use Policy (Pupil)

3. Policy Statements

3.1 General

It is the policy of the Schools to:

- provide a working environment that encourages access to knowledge and sharing of information

- maintain ICT facilities for academic and administrative purposes which provide access to their communities for local, national and international sources of information

- ensure that the security, safety and reputation of the Schools and their members are protected from harm through the use or misuse of ICT.

3.2 Software and Hardware

This policy covers the use of the Schools' ICT networks and the Internet, irrespective of the means by which they are accessed. The policy applies to pupils who are using the following methods of access whilst working under the auspices of the School:

- wired connections via a School machine
- wireless (WiFi) connections
- cellular connections (3G / 4G) on their own device

The Schools invest in a range of software and maintain this software to prevent unauthorised/inappropriate access to the Internet and to monitor email. Software is also used to detect viruses and to monitor and control the use of all computer facilities. It remains the responsibility of the pupil, however, to treat all resources, facilities and services with respect and to adhere to this policy.

Access to educational Internet-based games may be allowed with some discretion. Pupils will ensure that such games are quiet, cause no disruption and contain suitable age-appropriate content. Strict priority is given to anyone wishing to complete schoolwork.

Pupils will not unplug, insert or disconnect any cabling relating to ICT equipment, nor interfere with projectors unless they have been given direct permission to do so.

ICT Acceptable Use Policy (Pupil)

3.3 Acceptable use

It is the policy of the Schools that:

- the ICT facilities are provided in support of teaching and learning, research and administrative activities
- pupils are expected to conduct themselves in an orderly manner and respect the rights of others when using the facilities
- only designated pupils or those given permission are permitted to use the facilities.

3.4 Network Etiquette and Privacy

Rules for using the computer facilities / own devices include, but are not limited to the following:

- pupils will not post nor upload any information, pictures or video to any website/app (including video and photo sharing websites/apps) that may be deemed unsuitable, offensive or annoying to others. In addition, pupils agree neither to post nor upload any material which identifies the Schools, its staff or its students from any device whether within the Schools or elsewhere.
- publishing documents or photographs relating to the Schools or their pupils without express permission is prohibited.
- pupils consent to access and review by the ICT Service Department of all materials created, stored, retrieved sent or received using the Schools' ICT resources.
- pupils must use appropriate language in all communications
- pupils must keep personal data private (e.g. home address / telephone number)
- pupils must not use the facilities in any way that would disrupt the use of the service by others
- pupils should take care to avoid excess printing (be brief, proof read work for mistakes before printing, avoid printing entire articles if an extract is all that is needed etc.)
- pupils should remember that humour and satire can often be misinterpreted
- pupils must cite references for any facts which they state
- pupils must respect the rights and beliefs of others
- pupils must be polite

3.5 Distance Learning & Live Lessons

Distance learning requires teachers and pupils to adapt normal classroom routines to the online world, but the normal high expectations of conduct and behaviour will remain. The following directions **must** be followed:

- the recording of still images, filmed images or audio of staff or other pupils without permission, and the distribution of such images, is strictly forbidden.
- you must log in to any Office365 programme (including Teams) with **your** school email and password. Impersonating someone else or trying to access the school system via a different email is strictly prohibited.
- making inappropriate, offensive or unkind comments, including through emojis and/or images, will not be tolerated.
- any visual or audio file shared with others must be appropriate to the learning task.

- pupils must not interfere with another pupil's work without their permission, whether it is work submitted on a platform or shared work in a collaboration space (such as in OneNote).

ICT Acceptable Use Policy (Pupil)

- there is an expectation that pupils will engage in online collaborative work when requested by their teacher, work in a respectful and helpful manner, following instructions carefully.

- when submitting academic work, students must adhere to the usual standards of academic honesty and be careful not to plagiarise work, avoiding copying off the internet and submitting as their own assignment work, or submitting work as their own without reference to co-authors if the work was generated collaboratively.

- pupils are expected to take reasonable steps to complete learning tasks in the timescales set by teachers so as to maintain progress in their studies. Distance learning requires greater self-management of task completion by pupils, given the absence of physical face-to-face teacher pupil contact. Timely communication of expected/experienced delays to work submission, and an openness of both parties to listen and adapt to the dynamic challenges collectively faced, are key to maintaining strong teacher-pupil learning relationships and academic progress. If you are struggling, please do contact your teachers, they want to help.

- pupils should store their electronic work in an organised fashion – using their My Documents folder on a home computer (which could be ordered by subject), their cloud-based OneDrive (available at www.office.com – and sign in with school credentials) or in the usual way expected by their class teacher (e.g. Class Notebook).

Relating specifically to live lessons:
- pupils should wear headphones during live lessons or tutorial sessions
- it is expected that pupils will engage in lessons and tutorials in a manner as similar to regular classroom learning as possible. This includes: making sure no music is on in the room; mobile phones are not to be used during the lesson unless directed by the teacher, nor are other functions on computers; pupils should have all their equipment ready before the lesson.
- behaviour when working as part of an online lesson should be as expected in normal classroom learning: quietly attentive; prepared to ask and answer academic questions; attempt learning tasks in good faith, whatever the challenge; engage respectfully with others when collaborating.
- parents should not be participating/be present in lessons except where this is requested by the School due to the age of the pupil or due to an SEN need.
- recording or taking screenshots in online classes is strictly forbidden.
- pupils should have the option to have cameras on and should be aware that it could be possible to be seen on a display screen if they have a camera on. This is more manageable if 'lecture theatre' view is used by the teacher.

3.6   Security

All use of the School systems must be under your own username and password unless specifically directed otherwise by a member of staff. Remember to keep your password to yourself and do not share it with your friends. If you think that someone else has access to your account, contact a member of the ICT Service Department immediately.

If a pupil takes home any School owned property then they are responsible for it. It will be necessary to check home and personal insurance policies to ensure that the risks of damage or theft to the Schools' equipment are covered. It is important that pupils are aware of their own personal security when transporting expensive and 'desirable' equipment between

ICT Acceptable Use Policy (Pupil)

home and school. This equipment should not be left unattended. Pupils should be discreet when travelling on public transport or walking to or from the Schools.

3.7   Personal Use

The Schools accept that pupils will want to use the computer system for their personal use. Provided that this use is occasional, reasonable and does not interfere with or detract from everyday work and commitments, it will normally be tolerated. Pupils are able to use the facilities in this way at lunch times and at break times as well as occasionally in lessons. Personal use during lesson times must be directed by a member of staff.

3.8   Unacceptable Use

The ICT Service Department will prohibit the use of its facilities when used intentionally in contravention of the principles outlined in this policy. The activities prohibited under this policy include (but are not restricted to) those listed below. Pupils must not:

> i.   cause the good name and reputation of the Schools to be undermined
>
> ii.   deliberately access, create, store, download or transmit any material that the Schools may deem to be threatening, defamatory, abusive, obscene, racist or otherwise offensive or access any age-restricted material classified above their actual age
>
> iii.   send or partake in unwanted email, chain letters, pyramid letters or similar schemes
>
> iv.   gain unauthorised access to facilities or services
>
> v.   behave in a way, or use the facilities in such a manner, that violates any other School policy
>
> vi.   pretend to be someone else or give false information about themselves
>
> vii.   transmit, store or download any material in violation of any UK or other national laws. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws
>
> viii.   engage in cyber-bullying – the use of technology to tease, intimidate or threaten
>
> ix.   make malicious use of any instant messaging platform over the school network
>
> x.   connect their personal device to any switch or hub linked to the school wired network
>
> xi.   use any VPN/proxy sites. Use of such sites/networks will be considered a direct attempt to compromise the security of the Schools' network and will result in disciplinary action
>
> xii.   overuse, hack or back up the school network or use it in such a way that would deliberately slow down access for other users, e.g. by streaming or downloading movies

ICT Acceptable Use Policy (Pupil)

3.9   If pupils have any concerns during the school day, or at any other time, they must raise them immediately with an appropriate member of staff (Form Tutor, Head of Year or Deputy Head). These may include:

- a concern that their network security has been compromised
- any worry that there has been attempt by someone older from outside the Schools to contact them (e.g. grooming, trying to discover personal details, travel plans etc)
- any accidental access to a restricted site or one which has inappropriate content.

3.10   Prevention and investigation of misuse

The Schools reserve the right to access all information held on their facilities, including monitoring and intercepting any system logs, web pages or email messages. This is for the purpose of preventing and detecting misuse. It is the policy of the Schools to:

- promote their Acceptable Use Policy to all their members and provide advice on acceptable use when asked
- undertake a full and continual audit of all Internet activity to ensure pupils adhere to the detail and the spirit of the Acceptable Use Policy
- take swift action against anyone found to be misusing the Schools' ICT facilities.

If it is suspected that a pupil's personal device is being used in an unacceptable way whilst on the school site or away from the site on school business, including the use of their own cellular data access, a member of staff will confiscate the device and ask the permission of pupil to gain access in order to investigate. If the pupil refuses to give permission for the member of staff to gain access, the device will be held until the pupil's parents can be contacted so that device can be accessed in their presence. The full cooperation of the family is expected in these circumstances.

3.11   Health and Safety

Merchant Taylors' Schools have a separate ICT Health and Safety Policy. By agreeing to this Acceptable Use Policy you agree to follow the Health and Safety rules which govern use of ICT facilities. In particular, if you have a medical condition such as epilepsy which may be affected by the use of computers then you must inform your School and a member of the ICT Service Department.

The Schools cannot guarantee the safety of personal chargers which may be brought in to charge personal devices. As a result, it is the responsibility of pupils to ensure that their own devices are fully charged before they are brought into School. The use of personal chargers is forbidden on the School sites.

3.12   Occasionally, the Schools will want to share information with parents relating to changes to this policy, new online threats or trends which may affect pupils etc. This will usually be done via the weekly email bulletin to parents.

3.13   Disciplinary Action

Breaches of the School's ICT Acceptable Use Policy will be dealt with in line with the Behavior Policy (Including Rewards and Sanctions).

3.14   Cyberbullying

Cyberbullying is defined as *the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else.*

Cyberbullying can take different forms:

- Threats or intimidation
- Harassment or stalking
- Manipulation
- Vilification and defamation
- Ostracism and peer rejection
- Impersonation
- Forwarding or publicly posting private information or images

Cyberbullying can be characterized in several specific ways that differ from face-to-face bullying:

- The profile of the person carrying out the bullying
- The location of the online bully
- The potential audience
- The perceived anonymity of the person carrying out the bullying
- The motivation of the person cyberbullying
- The digital evidence of the bullying activity

As with other types of bullying, cyberbullying is unacceptable in the School community. Appropriate sanctions will be applied, in line with the Behaviour (Including Rewards and Sanctions) Policy.

What to do if you are the victim of cyberbullying:

- Report it – tell your parents and your Form Tutor. Remember, you have not done anything wrong, and you deserve support
- Keep evidence – take screenshots, keep a timeline of what has happened
- Block the bully – block the account from which the bullying originates. You can also request that they delete the offending content
- Report it – report the account to the messaging service provider or to CEOP

ICT Acceptable Use Policy (Pupil)

What the School will do:

- Provide support for the person being bullied, involving them in the decision-making process
- Record the incident
- Work with those involved towards removing the upsetting material
- Inform parents
- Work to restore the relationships between the victim and the bully

If there is evidence of illegal activity, the School will co-operate fully with the police and follow their advice on securing evidence. The School will refer incidents about which they are aware to the police where they:

- Involve illegal contact between adults and children
- Involve coercion or blackmail
- Are extreme in their nature or violent
- Place a child at immediate or significant risk of harm.

The School provides information about staying safe online and dealing with cyberbullying through its Cornerstone Curriculum (PSHE) and ICT lessons.

ICT Acceptable Use Policy (Pupil)

ICT Acceptable Use Policy

This is a summary of the Merchant Taylors' Schools' ICT Acceptable Use Policy. The full policy can be found on the School Website or a hard copy can be obtained on request.

Purpose
The purpose of this policy is to state clearly both pupils' obligations in using ICT facilities and the ICT Service Department's responsibility and authority in taking action to safeguard members of the Schools. The ICT Service Department of Merchant Taylors' Schools provides facilities which support the aims and objectives of the Schools.

Personal Responsibility
Pupils must accept personal responsibility for using the Schools' ICT facilities and their own devices with respect and in accordance with this policy. It is the responsibility of the pupils to report any misuse to a member of staff.

Software & Hardware Safeguards
Although software safeguards are used, it remains the responsibility of the pupils to treat all resources, facilities and services with respect and to adhere to this Acceptable Use Policy.

Acceptable Use
The policy makes no distinction between the acceptable use of the School network (via wired or wireless access) or personal devices using cellular data services during the school day or on school business. It is acceptable to use the facilities for research, learning and some limited personal use. All care must be taken to check removable media such as USB drives for viruses. All pupils must exercise network etiquette including politeness and respect and especially adhere to the rules about privacy. Pupils must only access the network via their own username and password and must adhere to the strict security guidelines within this policy. Pupils must adhere to the School's expectations around distance learning and live lessons as detailed in this policy.

Unacceptable Use
It is unacceptable for pupils to attempt to gain unauthorised access to information and services, to access chat rooms, to engage in cyber bullying, to publish defamatory material, to access/transmit material which may be deemed threatening, abusive, obscene, racist, sexist or otherwise offensive, to cause the good name and reputation of the Schools to be undermined, to make malicious use of instant messaging services over the school network or to use VPN / proxy sites. Parents should not use any device to take photographs of any children other than their own, addition parents should not participate in online lessons except where this is requested by the School due to the age of the pupil or due an SEN requirement

Prevention and investigation of misuse and disciplinary action
Merchant Taylors' Schools will monitor all data, information and activity on its computer systems for the purposes of prevention and investigation of misuse. Permission may also be requested to access a pupil's personal device should suspicion arise that it has been used in a way which contravenes the spirit of this policy. Disciplinary action may be taken against anyone found to be misusing the Schools' or their own ICT facilities.

Health and Safety
Users should be familiar with and abide by the guidelines set out in the ICT Health & Safety Policy. Pupils should ensure that their own devices are fully charged before bringing them into School. Personal chargers must not be used on the School site.