St Thomas More Catholic High School

St Thomas More Catholic High School Network Acceptable Use Policy

Last Update: September 2022

COMPUTING FACILITIES

Users are encouraged to make use of the school computing facilities for educational purposes. All users are expected to act responsibly and to show consideration to others. This policy applies to ALL users regardless of their position in the school.

USE OF OTHER TECHNOLOGY

Technology such as smart phones, MP3 players, Tablets, memory cards, USB Storage Devices and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with ICT Acceptable Use Policy. Such devices must not be connected to the school network without specific permission.

LOGGING ON AND SECURITY

- Users are responsible for the protection of their own network logon accounts and should not divulge passwords to anyone.
- Passwords have to be a minimum of 8 characters and should not be words or phrases that are easily guessed
- Users should not log on as someone else, nor use a computer which has been logged on by someone else.
- Users should change their passwords regularly.
- Staff members should take all precautions to ensure confidential data is protected.
- Staff members should never take, or attempt to take confidential or personal data pertaining to other Staff or students outside of the school unless previously authorised. If authorised this data must be appropriately protected.
- Staff members must never use personal storage (physical devices or cloud based) to store any personal information relating to any member of the school.

- Staff members should never allow students to use their network login, for any reason.

Users should also log off or lock the keyboard (using CTRL+ALT+DEL or Windows Key+L) when leaving a workstation, even for a short time.

REMOTE ACCESS

Staff members have the facility to use the school network from their home PC using a school hosted solution. This Policy applies to remote access users where applicable with the following additions:

- Users must ensure that they logoff when they have finished.
- Only Staff members are permitted to use this facility.
- Users should NOT allow any other person to use this system from their home PC/laptop.
- Users should be aware that remote access is logged and can be monitored.
- Some information held on the school network may be confidential and therefore must be treated with due care and consideration. It should never be made or left visible to users who are not members of staff.

USE OF THE NETWORK AND OTHER RELATED FACILITIES

It is not acceptable to;

- Attempt to download or install any programs to a school owned computer.
- Attempt to introduce a virus, malware or malicious code onto any device.
- Attempt to bypass network and systems security.
- Attempt to access another user's account.
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking or password cracking software / system.
- Connect or install any networking device (router, switch, wireless access point etc) to the network or via a computer.
- Connect or install any form of internet access device such as modem, broadband or internet enabled mobile phones directly to the network or via a computer.
- Use any device to access the internet via anything other than the school provided method (such as mobile data routers, hotspots etc.)
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- Engage in activities which waste technical support time and resources.
- Take food or drink of any kind into the ICT Rooms

- Wilfully damage or tamper with any network equipment, computer, monitor or laptop.

All networked computers in the school can be monitored remotely. This monitoring is usually undertaken when there is suspicion that the Acceptable Use Policy (AUP) is being contravened in any way.

USE OF THE INTERNET

Access to the Internet is filtered to prevent access to inappropriate sites, and to protect the computer systems. Users should be aware that the school logs all Internet use for all users.

- The use of public chat rooms and forums is not allowed unless otherwise specified.
- The internet is not to be used for downloading resources for uses other than those relating to school work.
- Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- All users' internet usage is logged and is regularly checked. Inappropriate use will result in the user having their internet access rights revoked.
- Use of or attempted use of proxy avoidance sites is strictly forbidden, any such attempts will result in removal of network access.

USE OF EMAIL

- Students are not allowed to use email during lessons, unless the teacher for that lesson has allowed its use.
- If a user receives an e-mail from an unknown person, or which is offensive or upsetting, the relevant teacher or a member of the ICT staff should be contacted. Do not delete the email in question until the matter has been investigated.
- The sending / forwarding of chain e-mail is not acceptable.
- Do not open attachments from senders you do not recognize, or that look suspicious.
- Users may only use the e-mail accounts set up by the School. The use of e-mail facilities such as Hotmail is not allowed.
- Users email can be monitored if there is any reason to believe it is being used inappropriately.
- Using offensive or abusive language in emails will result in your email account being removed.
- Email should not be used to forward rumours or malicious content
- Users should not forward private messages without permission from the original sender.

USE OF G SUITE AND CLOUD STORAGE

The school provides email and other cloud services using Google G Suite for Education.

This also provides cloud storage (Google Drive) for every user.

- Cloud storage should be used for school related resources only.
- Confidential/damaging information should never be stored in a user's Google Drive. Staff should never store information regarding students in their cloud storage.
- As cloud storage can be accessed externally, users should always make sure they have logged out of all areas (Google Mail, Drive, Sites etc) when they have finished.
- Cloud storage should not be used for personal resources.
- Cloud storage should not be used for storing copyright protected material such as Music & Video content.
- Accessing your Google account is possible on personal devices such as mobile phones and iPads etc – but you MUST ensure your device is password or PIN code protected to prevent the possibility of confidential information being read outside of the school.
- All users are expected to use their school provided GSuite account and not their personal accounts.
- Staff must use a second authentication method to their account (such as a mobile phone) for extra security.

USE OF SCHOOL PROVIDED MOBILE DEVICES

The school provides a number of mobile devices to both Staff and students. The use of these must also comply with this policy with the following additions

- Staff devices may be taken home on the understanding that due care and consideration will be taken with the device.
- Staff devices will only be used by the assigned person and not by any other person outside the school, even if a family member.
- Student devices should only be used in lessons with the teachers consent.
- Student devices should be replaced in their provided storage (trolley/cabinet etc.) after use.
- Any damage, loss/theft or other issues should be reported to ICT immediately. If a damaged/missing device is not reported then that department will be liable for the replacement item cost.
- Any mobile devices must only be charged with the provided power supplies/cables etc. Faulty or missing cables should be reported to ICT so they can be replaced.

USE OF INSTANT MESSAGING AND ONLINE MEETING SOFTWARE

The use of Instant Messaging (IM) of any kind is not allowed unless otherwise specified. Online meeting software such as Google Meet, Microsoft Teams, Goto Meeting or Zoom should only be use for school purposes. Video conferencing facilities can be setup where required – please contact ICT for more information.

PHONES AND CAMERAS

Students' mobile phones must not be visible at any time during the school day.

Exam board regulations ban mobile phones from any examination room. Legally, children are not allowed to take and store photographs of staff or other children without their written permission (in accordance with the Data Protection Act 1998)

PERSONAL LAPTOPS / COMPUTERS & STAFF LAPTOPS

- Personal laptops/computers/tablets etc. (i.e. those other than those provided by the school) should not be brought into the school or connected to the network.
- In the case of Staff laptops, no other software other than the approved school software will be installed without consultation with the ICT Staff.
- Students should not bring their own laptops/devices etc. into school without prior permission.
- Students are not permitted to connect, or attempt to connect any device (laptop or otherwise) to the school network.

PRIVACY AND PERSONAL PROTECTION

- Users must at all times respect the privacy of other users.
- Users should not supply personal information about themselves or others, on websites, within email or other messaging systems.
- Users must not attempt to arrange meetings with anyone met via a website, email or other messaging systems
- Users should be aware that the school has a right to access personal folders on the Network/Email/Cloud Storage. Privacy will be respected unless there is reason to think that the ICT Acceptable Use Policy or school guidelines are not being followed or there is a Safeguarding concern.
- The use of secure HTTPS sites in school is permitted but these sites will also be monitored using inspection methods. No personal information is read or collected in any form.

VISITORS

Visitors to the school are expected to abide by all aspects of this policy. Visitors are not permitted to use their own devices on the school network – unless access is requested by a member of staff to the Guest wireless system.

DISCLAIMER

St Thomas More Catholic High School makes no warranties of any kind whether expressed or implied, for the network service it is providing.

St Thomas More Catholic High School will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, miss-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions.

Use of any information obtained via the network or other information systems is at your own risk.

St Thomas More Catholic High School specifically denies any responsibility for the accuracy of information obtained via its Internet services.

DISCIPLINARY PROCEDURES

Those who misuse the computer facilities and contravene the ICT Acceptable Use Policy will be subject to disciplinary procedures.

IMPORTANT - Users of the network may be held liable for costs incurred for repair and/or replacement of equipment where the damage was caused by misuse.

Agreement to the Acceptable Use Policy.

Please sign below to show your acceptance of the terms and conditions outlined in the St Thomas More Network Acceptable Use Policy.

Pupils Full Name:

_____ Signature _____

Parent or Guardians Full Name:

_____ Signature _____

Address:

_____

_____

_____

_____

Date:

_____