



NETWORK & ONLINE COMMUNICATION

POLICY DETAIL

Revision #	2
Effective Date	November 2024
Review Date	September 2025

CONTEXT

At Thomas More College, integrating Information and Communication Technology (ICT) is essential to modern educational theory and practice. We are committed to providing diverse opportunities for our students to benefit from exposure to, familiarity with, and expertise in computer-related technology. It is imperative that students access and use communication technologies in a manner that aligns with our college values, policies, and the law. This policy outlines the security measures, administrative protocols, and internal rules that should be observed when communicating electronically or using the ICT facilities provided by the school.

PURPOSE

The purpose of this policy is to establish clear guidelines for the appropriate use of the school's network resources and online communication tools. It aims to ensure a safe, respectful, and productive digital environment that supports educational objectives and minimizes potential damage to colleagues, students, and the school.

SCOPE

This policy applies to all students, faculty, staff, and visitors who access the school's network, internet services, and online communication platforms, whether on-campus or remotely.

PROCEDURE

1. ACCESS AND SECURITY

1.1 Authorised Access

Individual users are responsible for their behaviour and communication over the network. Users must only use their assigned login credentials and keep them confidential. They should never allow others to use their account and must log off at the end of each session to ensure that nobody else can access their account.

1.2 Password Protection

Users are required to create strong passwords that are not obvious or easily guessed. They must keep these passwords confidential and change them when prompted or if they become known by another user by notifying ICT services. Sharing of your password with anyone is strictly prohibited.

1.3 Account Security

Staff are required to use MFA (Multi-Factor Authentication) as implemented and in accordance with college access management requirements.

1.4 System Integrity

Users must not disable settings for virus protection, spam filtering, and other security measures that have been applied as departmental standards. Installing software without ICT permission is prohibited. Users must never damage or disable computers, computer systems, or networks of Thomas More College.

2. ACCEPTABLE USE

2.1 Education Purpose

Network resources are provided primarily for educational and research purposes. Users should ensure that their communication through internet and online services is related to learning and school-related activities. Personal use should be kept to a minimum to ensure resources are available for educational purposes.

2.2 Respectful Communication

All online communication must be conducted in a respectful and courteous manner, adhering to the school's code of conduct. Users should engage in positive and constructive online behaviour, respecting the rights and opinions of others.

3. PROHIBITED ACTIVITIES

3.1 Unauthorised Access and Use

Using others' accounts or passwords, or accessing their files, folders, or work without permission, is strictly prohibited. Unauthorized access to network resources or restricted areas is also forbidden.

3.2 Malicious Software and Activities

Introducing or attempting to introduce viruses, malware, or any harmful software into the network is prohibited. Intentionally wasting limited resources or engaging in activities that could harm the network's performance is not allowed.

3.3 Inappropriate Content

Sending or displaying offensive messages or pictures is prohibited. Using obscene or inappropriate language is not allowed. Accessing inappropriate internet sites is forbidden.

3.4 Harassment and Bullying

Harassing, insulting, or attacking others online is strictly prohibited. Engaging in cyberbullying or any form of online abuse will not be tolerated.

3.5 Communication Restrictions

Users must never send or publish unacceptable or unlawful material, including offensive, abusive, or discriminatory comments. They should not send messages that were sent to them in confidence and must not initiate or forward chain letters, hoax emails, or spam.

3.6 Resource Misuse

Using unauthorized programs and downloading unauthorized software, graphics, or music not associated with learning is prohibited. Storing personal files on school equipment without permission is not allowed.

3.7 Commercial and Illegal Activities

Using the network for unauthorized commercial activities, advertising, or political lobbying is prohibited. Engaging in any activity that is illegal under local, state, or federal law is forbidden. Participating in online gambling using school resources is prohibited.

4. PRIVACY AND CONFIDENTIALITY

4.1 Personal Information

Users must not reveal personal information, including but not limited to, names, addresses, photographs, credit card details, or telephone numbers of themselves or others. They must never publish or disclose the email address or personal information of a staff member or student without explicit permission.

4.2 Confidentiality

Users must ensure privacy and confidentiality by not disclosing or using any information in a way that is contrary to any individual's interests. They are responsible for protecting personal and confidential information.

5. INTELLECTUAL PROPERTY AND COPYRIGHT

Users must never plagiarize information and must always acknowledge the author or source of any information used. They must respect intellectual property laws, including copyright and licensing agreements. Users must ensure that permission is gained before electronically publishing others' works or drawings. Any material published on the internet or intranet must have the approval of the Principal or their delegate and appropriate copyright clearance.

6. DIGITAL CITIZENSHIP AND ONLINE BEHAVIOUR

Users should ensure that when publishing or sharing content online, it reflects positively on themselves and the school community. Plagiarism and cheating are violations of the school's academic policies and are unacceptable in any form, including digital submissions. Users should engage in constructive online behaviour, respecting the rights and opinions of others.

7. Cyberbullying and Harassment

7.1 Zero Tolerance

The school has zero tolerance for cyberbullying, harassment, or any form of online abuse.

7.2 Reporting Mechanisms

Victims or witnesses of cyberbullying should report incidents to a trusted faculty member or administrator immediately. Reports will be handled confidentially to protect all parties involved.

7.3 Consequences

Violations related to cyberbullying will result in disciplinary action, which may include loss of network privileges, detention, suspension, or expulsion.

8. Social Media Use

8.1 Personal Responsibility

Users are responsible for their behaviour on social media platforms, even when off-campus. They should not share their social media account passwords with others.

8.2 Representation of School

Users must not represent themselves as official spokespeople for the school unless authorized. They should not use the school's logos or images without permission.

8.3 Content Guidelines

Posting content that is harmful, inappropriate, or damaging to the school's reputation is prohibited. Users must respect privacy and not post images or information about others without their consent.

9. MONITORING AND PRIVACY EXPECTATIONS

Users should have no expectation of privacy when using school network resources. The school reserves the right to monitor, inspect, and disclose all data transmitted through or stored on its network. All use of internet and online communication services can be audited and traced to specific users.

10. SECURITY REPORTING AND INCIDENT RESPONSE

Users must promptly inform their supervising teacher or the ICT Manager if they suspect they have received a computer virus, spam, or any inappropriate message. They must report any suspected security breaches or vulnerabilities immediately, including any suspected technical security breach involving users from other schools or external sources.

11. MISUSE AND BREACHES OR ACCEPTABLE USAGE

Users are responsible for their actions while using internet and online communication services and will be held accountable for any breaches caused by allowing others to use their account. Misuse may result in disciplinary action, including withdrawal of access to services and other appropriate measures.

12. ENFORCEMENT AND DISCIPLINARY ACTIONS

12.1 Policy Violations

Failure to comply with this policy may result in disciplinary actions such as loss of network privileges, detention, suspension, or legal action. Illegal activities will be reported to the appropriate authorities.

12.2 Investigation Process

Reported violations will be investigated promptly and fairly by school authorities. All investigations will be properly documented.

12.3 Appeals

Users have the right to appeal disciplinary actions in accordance with the school's established procedures.

13. MONITORING, EVALUATION AND REPORTING REQUIREMENTS

The school will monitor the use of internet and online communication services to ensure compliance. Regular evaluations will assess the effectiveness of this policy, leading to necessary adjustments. Users must report any inappropriate sites accessed or breaches encountered.

14. POLICY REVIEW

This policy will be reviewed annually to ensure it remains current with technological advancements and legal requirements. Suggestions for revisions are welcome and should be submitted to the ICT Manager.