College ICT Acceptable Use Guidelines

MARY MACKILLOP CATHOLIC COLLEGE
75 Highfields Road, Highfields Q 4352
P 4698 7777
E highfields@twb.catholic.edu.au

These guidelines cover the use of technologies that are beyond the One to One Technology Program and include, but are not limited to, desktop computers, laptops, tablets, projectors, digital cameras, photocopiers, mobile phones, music storage devices and audio visual equipment.

A Student at Mary MacKillop Catholic College will be responsible for:

1. Ensuring mobile phones and other personal technologies are not seen used at College during the course of the school day, unless specifically instructed by a teacher.
2. Ensuring personal mobile phones/technologies are locked away safely and not left unsecured at any time. The College bears no responsibility for any personal technologies that are brought to school.
3. Understanding that the use of technologies in school is primarily to support learning.
4. Ensuring that games – online, installed or on an external drive – and other recreational programs not directly linked to learning are not accessed during school hours. This includes videos, instant messaging and social media platforms.
5. Not removing, or attempting to remove, any software installed by the College on the device.
6. Only accessing the Internet by using the College network when at school. The bypassing of the Mary MacKillop Catholic College proxy server to access blocked sites is prohibited. This included using VPNs, TOR and the altering of DNS settings.
7. Complying with all legal requirements governing the use of devices and the accessing of information—such requirements include, but are not be limited to, privacy and intellectual property rights laws, and Identity Theft and copyright.
8. Not accessing, or attempting to access, monitor or tamper with, information on any of the College servers or any other person or organization's computer without explicit agreement of that person or organization.
9. Downloading and running only authorized programs and learning games; and maintaining settings for virus protection, spam and filtering which the College and/or Department have set.
10. Ensuring that passwords are private and confidential, not shared with anyone, and changed regularly.

11. Understanding that all actions taken using the student's user account are the responsibility of the account owner and that the network account (username and Password) identifies the students and that all communications (both external and internal) may be monitored.
12. Understanding that the device may be monitored during lessons and breaks to determine how students are using the device and noting that student internet history can be monitored by IT —consequences will follow for students found to be breaching the Code of Conduct Agreement.
13. Ensuring that all schoolwork and other data is regularly backed-up. Weekly backing-up of College related work is encouraged. Students are encouraged to store personal data on an external device. The College is not responsible for the loss of any work or files from students' technology devices due to damage, hardware or software failure.
14. Not tampering or changing any anti-virus, security, monitoring or remote access settings on technology devices that have been set by the College.
15. Understanding that the college reserves the right to remotely install or make changes to existing software in network updates and students must not override these changes.

Procedures for Breaches to the Agreements and Policies

The college will be vigilant in managing student use of the resources to improve learning outcomes. Misuse of desktop computers, laptops, notebooks, tablets, digital cameras and other technologies and mobile ICT devices will be dealt with according to the nature of the infringement.

Ongoing Monitoring

The College reserved the right to remotely and locally monitor student and College based devices on an ongoing basis. Students found to be breaching the conditions of the Acceptable Use Agreements and Policies will be issued consequences in line with this policy. Students may be called up at any time by IT, Middle Leader, Assistant Principal or Principal to have their device checked for compliance with the *College ICT Device Code of Conduct and Agreement* and *College Acceptable ICT Use Guidelines*.

Major Breaches

The following are considered major breaches:

1. Endangering the health and safety of or the property of others;
2. Vandalizing the property of others;
3. Harassing or bullying others;
4. Persistent minor breaches;
5. Accessing blocked sites using VPNs, altering DNS settings to bypass the College proxy server, or accessing the internet by tethering to smart devices or internet dongles with the intent of bypassing the College monitoring systems and filters;
6. Downloading, displaying, saving or transmitting any material that others may find offensive. This includes, but is not limited to, violent, racist, sexist material and pornography.

7. Bypassing filters and network security with the intention of changing settings and or interfering with existing sites;
8. Using someone else's password to access email, intranet profiles or other online forums under their identity;
9. Encouraging any of the above infringements or knowing about and failing to report or to a teacher, Middle Leader or member of the College Leadership Team.

Procedures & Consequences for Major Breaches

In the event that a student is in breach of these guidelines the relevant sub-school managers should be informed. After consideration of the breach, the person may have one or more of the following bans imposed:

- Temporary ban on using computers or mobile ICT devices;
- Temporary confiscation of the device/s (including but not limited to computers or other mobile ICT devices);
- Removal of email privileges and/or internet and network access;
- If equipment is damaged, the student will be asked to pay all associated costs in replacing or repairing the damaged equipment;
- Removal from classes where computer use or mobile ICT device is involved;
- Suspension or expulsion;
- Authorities such as police may be contacted where the law has been breached.

Minor Breaches

The following are considered minor breaches of the policy guidelines:

1. Playing games;
2. Straying to sites irrelevant to learning;
3. Communicating digitally when not relevant to the requirements of the learning task;
4. Disseminating irrelevant material;
5. Failing to follow fair and reasonable instructions – such as closing the notebook;
6. Changing settings for virus protection, spam and filtering that have been set as a departmental or College standard.

Procedures and Consequences for Minor Breaches

Minor breaches will be dealt with by the classroom teacher according to the established procedure which includes; a reminder of expected behaviour in the form of a warning, and the student temporarily logging off and completing the task without using digital technology.

Where a student repeatedly breaches, or commits multiple minor breaches, the student will be sent to an Assistant Principal. The student and teacher will complete an incident report. Students will incur one or more of the above consequences at the discretion of the teacher or Assistant Principal.