MILDURA SENIOR COLLEGE E-SMART POLICY

INTRODUCTION

All students, staff and community members at Mildura Senior College should base behaviours on the College's values (Respect, Resilience, Responsibility, Independence, Success), that underpin all College policies and practices. These aim to provide a safe and inclusive environment where staff, students and parents are able to be a part of a positive school community. This includes the safe and productive use of technology, how we educate young people in its use and respond appropriately to education and community issues that arise as a result of appropriate or inappropriate use of the technology. The College is committed to the continued use and promotion of technology as a learning and social tool while providing its students with the capacity to be positive contributors to their community. This College policy is approved by College Council, is compliant with current Child Safe Standards and is reviewed regularly.

AIMS

The aim of this policy is to provide a framework for the implementation of appropriate practices within the school setting. It aims to ensure that every student, staff member and parent is informed of these practices and how these are applied in different settings and circumstances.

RELEVANT TECHNOLOGY

These policies are designed to apply to ALL digital devices that can be used to communicate or access digital content. This includes, however is not limited to devices that the College supplies for use of all students, Desktop Computers, Laptop, Notebook and Netbook Computers, Tablets and iPads, Smart Phones, iPhones and Mobile Phones.

DOCUMENTATION IN PLACE

- ICT Acceptable Use Agreement
- MSC eLearning Vision
- MSC Agreement Form
- Student Engagement and Wellbeing
- Staff Handbook
- BYOD Guidelines
- MSC Mobile Phone Policy

IMPLEMENTATION

- All members of the school community are aware of and have knowledge of the documents listed above.
- A copy of the College's values and appropriate related behaviours is displayed at various locations around the College, in all College communications, and the College website.
- All students and parents/guardians sign a copy of the Acceptable Use Agreement.

- The College uses a stage response process to dealing with all aspects of student behaviour including those related to the use of technology. This ensures consistency of response and that there is comprehensive documentation of situations by teachers, teacher advisors and school leaders.
- Information is provided to the school community through Compass Parent and Student Portal, College website and Facebook page, newsletters, and information sessions.

GUIDELINES

A student at Mildura Senior College is responsible for:

1. Ensuring mobile phones and other personal technologies are used appropriately in and out of class time. Mobile phones should be turned off and out of sight unless otherwise directly 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 video conferencing and instant messaging software such as Twitter, Skype, Facebook, Instagram and equivalents.
5. Not removing, or attempting to remove, any software installed by the college on the device.
6. Bypassing of the Mildura S.C. proxy server to access blocked sites is prohibited. This includes using VPN's and the altering of DNS settings.
7. Not accessing, or attempting to access, monitor or tamper with, information on any of the college servers or any other person or organisation's computer without explicit agreement of that person or organisation.
8. Downloading and running only authorised programs and learning games; and maintaining settings for virus protection, spam and filtering which the school and/or Department have set.
9. Ensuring that passwords are private and confidential, not shared with anyone, and changed regularly.
10. 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 student and that all communications (both external and internal) may be monitored.
11. Understanding that College provided laptops and other devices may be monitored at all times — consequences will follow for students found to be breaching the acceptable use agreement
12. 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 – this directly relates to item 10. Torrent downloading is strictly prohibited.
13. Ensuring that all schoolwork and other data is regularly backed-up. Weekly backing-up of school related work is encouraged. Only school related work can be backed-up on the student home drive on the Mildura Senior College network. 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 devices due to damage, hardware or software failure.
14. Not tampering or changing any anti-virus, security, monitoring or remote access settings on the device 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, netbooks, tablets, digital cameras and other technologies and mobile ICT devices will be dealt with according to the College's Student Engagement and Wellbeing Policy. This ensures that consequences are appropriate and ensure a restorative and educative aspect.

Breaching the conditions stated in the ICT Acceptable Use Policy may result in access restrictions and/or withdrawal of access to digital resources.

SERIOUS BREACHES OF COLLEGE POLICY

1. The following examples are considered serious breaches of College policy
2. Endangering the health and safety of or the property of others.
3. Vandalising the property of others.
4. Harassing or bullying others.
5. Persistent and multiple minor breaches.
6. Accessing blocked sites using VPN's, altering DNS settings to bypass the college proxy server, or other methods aimed at bypassing the college monitoring systems and filters;
7. Downloading, displaying, saving, or transmitting any material that others may reasonably find offensive. This includes violent, racist, sexist material and pornography.
8. Bypassing filters and network security with the intention of changing settings and or interfering with existing sites.
9. Using someone else's password to access email, intranet profiles or other online forums under their identity.
10. Knowing about and failing to report or encouraging any of the above infringements to a teacher/coordinator or member of the School Leadership Team.

Procedures and consequences for major breaches

The following consequences may be appropriate and applied following a significant and serious breach of College policy. On these occasions a student/parent conference will be convened with an appropriate member of the school leadership or E-Leaning Team (Pathways teachers of the student may also be engaged). A consequence appropriate for the behaviour will be applied based on the Student Engagement and Wellbeing Policy and ICT Acceptable Use Agreement, and may include the following.

- 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 and/or notebook is damaged, the student will be asked to pay all associated costs in replacing or repairing the damaged equipment;
- Suspension or expulsion;
- Authorities such as police may be contacted where the law has been breached.

MINOR BREACHES

The following examples are considered minor breaches of the policy guidelines:

1. Playing games.

2. Using sites irrelevant to learning without explicit teacher permission.

3. Communicating digitally when not relevant to the requirements of the learning task.

4. Distributing and disseminating irrelevant material.

5. Failing to follow fair and reasonable instructions—such as closing a netbook.

6. Changing settings for virus protection, spam and filtering that have been set as a departmental or school standard.

Procedures and consequences for minor breaches

Minor breaches will be dealt with by the classroom teacher according to the Student Engagement and Wellbeing Policy and the college's established procedures. This may include; a reminder of expected behaviour in the form of a warning or the student temporarily logging off and completing the task without using digital technology.

All loaned devices remain the property of Mildura Senior College. All accidental damages should be reported to the ICT Support Technicians immediately or as soon as possible. Damage to school owned machines will be assessed individually. In most cases students are responsible for the repair of devices when damaged in their care either at school, home or in transit to or from school.

EVALUATION:

This policy will be subject to a regular cycle of reviews undertaken by the Mildura Senior College E-Learning Team and the College Council. This will align with reviews undertaken on other College policies.

REFERENCES/RESOURCES

eSmart School Program - The Alannah and Madeline Foundation www.education.vic.gov.au/studentlearning/elearning

Cybersmart program- Australian Communications and Media Authority www.acma.gov.au and www.cybersmartkids.com.au

Policy created November 2016. To be reviewed November 2017

RESPONSIBLE USE OF DIGITAL TECHNOLOGIES

RATIONALE

As part of the College's e-Smart Policy the following guidelines have been prepared to help members of the Mildura Senior College community understand and meet the expectations for responsible behaviour when using technologies. These policies are designed to support students become appropriate users of technology and understand the community context of their use.

CORE EXPECTATION

Mildura Senior College is committed to providing a computer network and digital resources that promote educational excellence and support students to be effective users of technology in the context of creating stronger, safer communities. The resources and our curriculum programs provide students, teachers, and support staff with powerful digital tools that expand learning opportunities.

Associated with the opportunities that a digital teaching and learning program allows, is the responsibility for all members of our community to interact in a positive manner with the digital technologies provided. Ethics, integrity, and good judgement are expected when interacting with all digital devices at Mildura Senior College.

The college will be vigilant in managing student use of the digital resources to improve learning outcomes. Misuse of any digital resources provided by the college will be dealt with in an appropriate manner.

GUIDELINES

BEHAVIOURS

A student at Mildura Senior College will be responsible for:

1. Protecting one's own privacy rights and those of other students by not giving out personal details such as: full names, telephone numbers, addresses and images (this includes personal details, school details, images or photos).
2. Recognising other users' intellectual property and acknowledging these sources (in a bibliography including all text, images, and multimedia) where used.
3. Not participating in cyber bullying practices. In particular, students should not read or forward material that may be interpreted by others as bullying material and should report instances and material to a teacher. Students are expected to be up-standers in relation to any Cyber bullying, in line with Mildura Senior College ICT Acceptable Use Guidelines.
4. Seeking teacher or parent advice if unsure regarding Internet content or search methods, hostile or unpleasant emails, blogging or wiki content.
5. Avoiding all potentially offensive sites and refusing to be guided to these sites.
6. Ensuring that external data storage devices do not contain any programs or files that may cause harm or contain offensive material.
7. Respecting the rights of others in all collaborative, online communication forums, and email by using language that is polite and professional.
8. Respecting computer network security and the data of other users (including individuals, the college and the Department) and only log in using their own login code and password.

ONLINE BEHAVIOUR

This applies to all online interactions, from email and social media, to websites and instant messaging.

1. Behave online in a polite and fair manner at all times. Online behaviour and manners are very important. Your words may be easily misunderstood or misinterpreted, so be considerate and tactful. You are never anonymous online. You are accountable. Your actions can be traced.
2. Check the information in your profile to make sure your personal details are not available to strangers. Blogs and profiles should be available to your friends only.
3. Respect the rights of others in all collaborative, online communication forums and email by using language which is polite and professional.

DOWNLOADING AND UPLOADING

This applies to downloading and uploading:

1. If material you download could be offensive—it is your responsibility and you may have to face consequences. Laws exist to protect people from receiving material that may be rude and offensive. You may not think it is offensive, but someone else may be reasonably offended by it.

2. Remember, photos, videos, recordings and text that you upload to sites in any way (even on secure sites) can remain online forever. Once you upload content you lose control of it. It can be accessed for personal or commercial (advertising, marketing) purposes by anyone

~~2.~~3. If a site has been blocked and you consider this site to be of educational benefit—inform your teacher. Do not bypass department/college network security to access games, music or social networking sites whilst at school.

~~3.~~4. Do not download blocked content at home and access it from your hard drive whilst at school.

~~4.~~5. The Australian Law and Digital Rights Management (DRM) states that it is illegal to download or share copyrighted music, video, film and games without paying for them. Downloading these files illegally or sharing illegal downloads is breaking the law and you may be prosecuted.

USE OF EMAIL AND SECURITY

This applies to the use of email:

1. When emailing: imagine that you are speaking to the person and type a polite version of what you would say. Capitals are considered yelling.
2. Email is for communicating information and sending documents. Do not become involved in email arguments. If an email exchange is becoming less than friendly, then end it and speak to the person, in person, and/or consult a parent or teacher.
3. Take care with your email account. Don't give out your email address to unreliable sites or your inbox may fill with SPAM (junk email—advertising).

Users must only send emails from their own named accounts. If you create an anonymous email account (i.e. Ilikered@gmail.com account) and send inappropriate emails from this account you can be tracked. Anonymous emailing

4. such as this is prohibited.
5. Do not open emails that request that you update certain programs such as 'Flash' or 'iTunes'. Requests to update will generate from the programs themselves and will never be emailed. Do not open emails that promise gifts and opportunities. Simply opening these emails (not even the attachments) can release viruses or Trojans into y our computer.

6. Students must not use their digital device, or college owned technologies to create, save or send messages that contain offensive language, graphics, images, or attached graphics files or messages that are sexist, racist or otherwise prejudicial or inflammatory (intended for impact and strong reaction). Whenever a member of the college community is involved in sending such an email, or communicating such information using the Internet (whether from inside the college or beyond it) it is considered a breach of the Acceptable Use Agreement.
7. Email accounts are not designed for storing information. You need to save important information as documents on your personal hard drive. Clean out your deleted messages and sent mailboxes every fortnight or more regularly if required.