Mount Warrigal Public School

Safe, Responsible and Ethical use of ICT Procedure

BRIEF DESCRIPTION:

ICT is used as a general term for a diverse set of technologies which enable users to create, access, disseminate, store, manage, and communicate information in a digital format (e.g. applications, computers, internet, mobile phones, email, social media etc). ICT use at Mount Warrigal Public School provides opportunities for students, staff, and parents/carers to positively interact with each other, the community and the wider world.

LINK/S TO DEPARTMENT POLICIES AND GOVERNMENT SITES

https://education.nsw.gov.au/policy-library/policies/social-media-policy?refid=285859
https://education.nsw.gov.au/policy-library/associated-documents/social-media-procedures.pdf
https://education.nsw.gov.au/policy-library/policies/child-protection-policy-responding-to-and-reporting-students-at-risk-of-harm
https://education.nsw.gov.au/policy-library/policies/online-communication-services-acceptable-usage-for-school-students
https://www.acma.gov.au/
https://www.esafety.gov.au/

STATEMENT OF PURPOSE

We live in a connected global society. This procedure aims to provide guidelines so all stakeholders use technology in a safe, respectful manner. The following learning provides meaningful foci for our school community to develop knowledge and skills when using ICT to protect themselves and others:

Digital media literacy is the ability to access, understand and participate in or create content by using digital media. Users are introduced to appropriate online content e.g. realising the difference between strangers in the physical world to strangers online.

Positive online behaviour is the ability to develop positive, appropriate and constructive online relationships with peers, family and strangers in a variety of mediums. Concepts include: appropriate language to others, being kind when online, protecting personal information and responding to unwelcome communication.

Peer and personal safety involves developing protective behaviours while using a range of online media including social networking. Concepts for peer and personal safety include privacy, grooming processes, identifying unsafe feelings etc. E-Security is broadly defined as the protection of personal information online. It involves both electronic security and online security including spam, pop-ups and viruses.

Cyberbullying is harmful and is not tolerated at Mount Warrigal Public School. This includes: lying, spreading rumours, playing horrible jokes, leaving someone out on purpose, embarrassing someone in public etc. For more information see https://drive.google.com/open?id=1OkYFaqCDHcBxKsMPuyK1uQzNqa56mLvu

Mount Warrigal Public School

Safe, Responsible and Ethical use of ICT Procedure

The following guidelines provide information to all stakeholders on the standards for teachers when engaging in conversations or interactions using digital media (such as social networking sites, wikis, blogs, microblogs, video, audio sharing sites etc) for official, professional and personal use.

'School official use' refers to when an employee is participating on behalf of the department in relation to their role. For example, our school Facebook, Skoolbag or an online account (e.g. Twitter, Seesaw, Dojo, Google classroom etc) is used by an individual teacher in order to engage students and parents/carers of the school.

'Professional use' refers to when an account is publically open, content is published on an open, publically accessible channel or the purpose of the account has a connection to school related or department- related topics. For example, a teacher might create a blog specifically to share their knowledge about formative assessment with the general public. Although they are not officially representing the school, there is a connection between the content created and their employment as a teacher.

'Personal use' refers to an account that has secure privacy settings and is not visible to the general public. The purpose of the account has no connection to work-related or department-related topics or issues. Examples could include a staff member using a personal Facebook that has secure privacy settings or a private Instagram account. When personal devices such as mobile phones or cameras are used to take photos of students for social media purposes, photos should be deleted from the device within one week from the time of uploading.

All content on official accounts must be visible to the executive members of staff. Staff must not create accounts that cannot be monitored. Where social media accounts are created for communication between a staff member and students, the social media environment is viewed as an extension of the classroom and the same duty of care is owed.

IMPLEMENTATION

The following are expectations at Mount Warrigal Public School:

Teacher responsibilities:

Teachers who choose to use social media as part of their educational program should provide education to students on its appropriate use.

In some cases, social media interactions may be evidence for legal or investigation purposes. Staff should keep the following content for a minimum of two calendar years: content that serves an essential administrative, legal and historical purposes, including electronic documents, digital images, video and audio recordings, correspondence, files, forms and notes, all permission to publish forms, all permission for students to use social media, privacy notices and consent forms.

Communication with parents through online platforms (e.g. Seesaw/ Class Dojo):

Staff should make it clear that communications will not be monitored outside of the hours of 8am-5pm. However, if a teacher does see a message where there may be a duty of care, teachers are required to act (e.g. inform the police).

Mount Warrigal Public School

Safe, Responsible and Ethical use of ICT Procedure

Staff will:

- Always follow relevant department policies including the **Code of Conduct.**
- Only post things that they would be happy to be attributed to them as a teaching professional.
- Make sure their personal online activities do not interfere with the performance of their job.
- Be clear that their personal views are theirs, and not necessarily the views of the department.
- Not disclose confidential information obtained through work.
- Never name a student in comments without permission from the student's parent or guardian.
- Only publish photos of students if the correct Department of Education permission to publish forms have been completed by the student's parent or guardian (photos must be removed after one year of publishing unless further permission from the parent is sought).
- Not accept friend requests from current pupils, or ex-pupils under the age of 13 and will notify the parents if a child sends a friend request.
- Use extreme caution when corresponding with parents via social media, and preferably use a school email address instead as this platform is monitored by the department.
- Not act unlawfully (such as breaching copyright) when using social media.
- Report inappropriate use of personal platforms by colleagues if the safety, well being and confidentiality of a school community member has been breached.

Social Media Site Leaders and school executive:

School executive are responsible for monitoring staff's hours of engagement on school communication platforms to protect the wellbeing of staff.

Teachers and staff must seek approval from their principal to create official school social media channels. At least two staff members must have administrative rights to the account, including a school executive. Page or group creators accept the responsibility to monitor and moderate any accounts they create including reporting any inappropriate engagement that does not align with our safe, responsible and ethical guidelines. Administrators must undertake a review of the school social media channels at least once every school year to ensure that any content that is no longer relevant or accurate is removed.

Administration staff responsibilities:

Staff must seek parental consent to publish any identifying information such as full name or image, about any student within any social channel. Consent forms should include how the social media channel will be used for educational purposes and must explicitly describe:

- Which social networks will be used
- The purpose for the social media account
- How the interactions will be monitored
- Who will monitor and moderate interactions
- The duration of the account, for example, when the social media account will be removed
- The rules of engagement relating to the use of the social media account
- Who they can contact if they want to view the personal information, make changes, or withdraw consent.

School Facebook admins should act immediately to remove any social media posts when directed by the Principal or the Department of Education social media team.

Mount Warrigal Public School

Safe, Responsible and Ethical use of ICT Procedure

Parent and carer responsibilities:

As children start to navigate the online world and interact with others more independently, they are more likely to be exposed to risks of bullying or unwanted contact or accidentally coming across inappropriate content.
Some tips for kids aged 5 to 12:

- Keep the computer or device in an area of your home that can be supervised and check in regularly with your child to see what they are viewing.
- Consider setting up your own accounts with the sites your child/ren use most so you can see how they work and understand the risks.
- Explore the online world with them to help establish that this is not just a solitary activity. Play games with them. Do a creative project together.
- Think about social media readiness. Most social media sites require users to be at least 13 years of age before they can register, although some sites are created especially for children under 13.
- Encourage respect and empathy. Teach them to avoid sharing or posting things that may upset others.
- Start building resilience. Teach your child that there are ways they can deal with material that worries or frightens them. This includes immediately telling you or another trusted adult of any concerns or uncomfortable material.
- Monitor their amount of screen time by considering a range of factors such as your child's age and maturity, the kind of content they are consuming, their learning needs and your family routine.
- It is important to talk with your children about the possible consequences of sending or sharing intimate or sexually explicit messages, images, photos or videos.

Parent responsibilities for safe, respectful and ethical use of ICT

Respect other users by ensuring discussions within online platforms remain civil. Personal attacks, negativity and trolling are not beneficial to our school or our students. We reserve the right to remove comments that:

- Are deemed racist, sexist, abusive, profane, violent or obscene.
- Advocate illegal activity.
- Libel, incite, threaten or make personal character attacks on Mount Warrigal Public School students, employees, guests or other individuals.

Parental requirements include:

- Not posting photos, videos or comments that include other children at the school.
- Raising queries, concerns and complaints directly with the school rather than posting them on social media- whether on their own pages, in closed groups (e.g. groups set up for school parents to communicate with each other) or on the school's pages.

We reserve the right to remove any participant that does not adhere to the rules of engagement or community standards. Please keep in mind that your name and photo will be seen next to your comment, visible to all visitors on the page. We will not permit messages selling products or promoting commercial, political or other ventures.

Mount Warrigal Public School

Safe, Responsible and Ethical use of ICT Procedure

Student responsibilities:

Students who use the internet and online communication services provided by the department must abide by the conditions of acceptable usage. When using the internet, students are reminded of the acceptable usage policy each time they log on and must accept acknowledgement. Disciplinary action will be taken for students who breach this policy.

Students will:

- Never damage or disable computers, computer systems or networks of the department.
- Not disable settings for virus protection or spam that have been applied as a departmental standard.
- Ensure that communication through internet and online communication services is related to learning.
- Keep passwords and personal information confidential and never allow others to use their personal e-learning account.
- Log off at the end of each session to ensure that nobody else can use their e-learning account.
- Promptly tell their teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable. If this occurs close the page straight away, hit control-alt-delete if the site does not allow you to exit use a filter or other tool to block adult content, and use safe search settings in your browser report offensive content to the site administrator and talk to someone you trust if you have seen something that has shocked or upset you.
- Seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- Never knowingly initiate or forward emails or other messages containing:
    - a message that was sent to them in confidence.
    - a computer virus or attachment that is capable of damaging recipients' computers.
    - spam, e.g. unsolicited advertising material, chain letters and hoax emails.
    - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
    - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
    - sexually explicit or sexually suggestive material or correspondence.
    - false or defamatory information about a person or organisation.
- Be aware that all use of the internet and online communication services can be audited and traced to the e-learning accounts of specific users.
- Never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- Ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- Be aware they are held responsible for their actions while using the internet and online communication services and any misuse of the internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.
- Hand in personal phones to the office for safekeeping during the day if required to bring them to school.
- Not access social media on school devices, or on their own devices while they're at school.
- Not make inappropriate comments (including in private messages) about the school, teachers or other children.

EVALUATION

These procedures will be regularly evaluated and updated throughout the school year. A review of the procedures will be held by the conclusion of each year and any alterations noted.