Emmaus College
ICT Acceptable Usage Policy

Purpose

'The digital world is characteristic of the contemporary world…the web and social networks have created a new way to communicate and bond…Yet to understand this phenomenon as a whole, we need to realise that, like every human reality, it has its share of limitations and deficiencies.' Pope Francis, Christus vivit, 2019.

Access to digital technologies, including the internet, is provided to students and staff at Emmaus College (the College) because digital information and communication are important mediums for contemporary learning and teaching and administration. Within Melbourne Archdiocese Catholic Schools (MACS), a range of technology platforms, such as the Integrated Catholic Online Network (ICON) provide access to a suite of digital technologies. The information, communication and learning technologies used by students in classrooms will be appropriate to the age and development of students. These technologies are used to support professional learning and the development of networks within and between the College and other schools for professional learning. They enable effective communication also with our parents and allow them to participate in their children's education, working in partnership with teachers.

In using and managing internet and network services, students and staff at the College are expected to respect the rights and privacy of all persons. They are called upon to respect the dignity of every human person. The College, along with parents in our community, educate students in the use of information and communication technologies to assist them to become responsible users, creators and publishers in the digital environment.

Digital technologies and their use in classrooms are opening up new opportunities for learning, and previously unimagined approaches to teaching and learning. Today, young people have access to knowledge, people and new ideas like never before. They are able to connect, collaborate and build relationships with peers, educators and the wider global community. The use of digital technologies within Catholic schools supports learners to question, evaluate and consider the validity of information and then search for truths contained in those ideas. Learners are empowered to demonstrate adaptability and versatility in thinking and strategies as they select, use and manage a range of applications and technologies. We seek to develop students who are responsible and ethical communicators, creators and publishers in the digital community.

This policy outlines the appropriate use and management of digital technologies such as the internet and network services at the College in accordance with legal and moral requirements and expectations.

Scope

This policy applies to members of the College community in their use of digital technologies. It applies to all computers, devices, internet and network services, information and communication technologies, applications, and systems provided, operated and managed by the College. This policy does not apply to the curriculum content in the College. The curriculum and teaching practices and pedagogy are outlined in documents related to our learning and teaching programs.

Definitions

Computer is either a desktop or portable laptop device that performs processes, calculations and operations based on instructions provided by a software or hardware program.

Device refers to a unit of physical hardware or equipment that provides one or more computing functions within a computer system. It can provide input to the computer, accept output or both. Typical hardware includes a computer mouse, speakers, printer and microphone.

Email means the system that enables users to send data over the internet using computers and mobile devices.

ICON means the Integrated Catholic Online Network which is used to deliver shared services for educational and administrative purposes across Catholic schools.

Internet means the system of interconnected networks that connects computers for data transmission and storage.

Intranet refers to a local system of computers enabling students and staff to communication and share information within their school community.

Mobile devices refers to (but is not limited to) mobile phones, PDAs and portable storage devices.

Network services means the facilities and resources located on and delivered via a computer- based network, including communication systems, internet and intranet services, mobile devices, electronic mail, web services, printer services, database services, back-up services, file services and network management services.

Parents includes parents, guardians and carers.

Social networking means web-based services that allow individuals to create their own online profiles and communicate with each other by voice, chat, instant message, image sharing, video conference and blogs in a virtual community.

Staff means salaried, voluntary, and contracted persons.

Students means those students enrolled at the College

Website is an internet-based page or series of pages grouped together and managed by a person or group.

Principles

The use of digital technologies within the College by staff and students is underpinned by the following principles and understanding:

- that digital technologies provide valuable opportunities for staff and students to collaborate, connect, learn and create with peers, colleagues, experts and the wider community
- that online behaviour will at all times demonstrate respect for the dignity of each person in the community
- users will behave in a manner that is ethical when using the internet and network services (even for personal communication)
- the Catholic beliefs and ethos of the school, and professional expectations and standards required by teachers are demonstrated in the way the technologies are used
- inappropriate online behaviour, including cyberbullying, will not be tolerated.

Policy

Internet and Network Access

Access to internet and network services are provided by MACS to College staff and students for educational and administrative purposes. From time to time, other MACS policies and requirements in particular schools may result in restrictions.

Access rights assigned to students and staff at the College will be determined by the Principal and may vary as educational and administrative purposes change.

Students and staff at the College may not use the internet and network services provided for commercial purposes, either offering or acquiring goods or services for personal use. The services cannot be used for political lobbying or proliferation of unnecessary communications.

Expectations of users

All students and staff at the College are required to use the internet and network services in accordance with this policy. Any use of devices or services that may be questionable, offensive, and controversial or against the Catholic ethos is unacceptable. This includes personal communication with students on matters not related to curriculum or education. These standards apply whenever the College equipment or communication lines are used, including use from home or other non-school location and when a private account is used.

Non-compliance with this policy

Disciplinary action may be undertaken by the College against any student or staff member, who is found to be using the provided internet, network services, device or mobile device inappropriately. The Principal will determine the disciplinary measures to be undertaken in accordance with other policies and guidelines. These measures may be outlined in staff handbooks or the Acceptable User Agreement for students used by the College.

Duty of Care

The College provides instruction to students in online personal safety issues, including inappropriate sites, stranger danger, cyberbullying and scams. The College prepares staff to deal with these issues.

Monitoring

Students

Online activities may be monitored or reviewed to assess network efficiency, examine system security and to investigate alleged breaches of this policy.

Staff

An authorised person (e.g. a principal, a regional manager or other MACS staff member) can monitor the use of MACS ICT resources. Server logs may also be used in an investigation of an alleged breach of this policy or other College policies.

Security

To minimise risk to MACS information and communication networks from viruses and intrusions, current virus screening software is activated, and where appropriate, passwords are used by staff and students at the College to maintain Firewalls. The management of system protocols and configurations are the responsibility of the staff authorised by the College or MACS. Non-authorised staff and students are not permitted to have access to these levels of system management.

Email

Email communication is provided for educational and administrative purposes. The College staff and students must identify themselves appropriately by using a signature block at the bottom of the email message that includes their name, College phone number and postal address. The College advises students and staff that they may be held accountable for the email they create and distribute using the network.

Websites

The College Principal may create, or have created a website for the College. These websites must be established and maintained in accordance with MACS policies and guidelines and relevant legislation.

Social Networking

Provision of social networking for students must be related to an educational purpose. This is at the discretion of the College Principal.

Related school policies

- Anti-Bullying Policy
- Child safety policies
- Codes of conduct for students, parents and staff
- Data Breach Policy
- Managing Complaints and Grievances Policy
- Privacy Policy
- Social Media Policy for staff
- Student Behaviour Policy.
- Staff Student Professional Boundaries

Emmaus College Acceptable Use Agreement

Students

Access to digital technologies at the College is provided for staff and students as a tool for teaching and learning. Student behaviour when using the technologies provided by the College must reflect the high standards of behaviour expected at the College and be according to the principles outlined in these guidelines.

The guidelines aim to facilitate the appropriate, effective and equitable use of the computer network for all College students. Integral to this is the protection of users and digital resources provided by the College network and digital infrastructure. It is important that all students read and understand the expectations outlined in these guidelines and follow them at all times.

The College reserves the right to, at any time and without prior notice, examine email messages, files stored on student devices and in network locations, Internet favourites, history and cache files and other information stored on ICT devices and on the network.

Online Behaviour

You have been provided with an individual username and password, which you should always keep secure – don't disclose it to anyone, unless required for the maintenance of your ICT device by ITS staff.
- you should access the College network or any ICT device only within the College using your own username and password.

- always log off or lock your ICT device before you move away; and be sure to log off shared ICT devices always (eg: in the Library).
- you should not intentionally access, interfere with, copy or move other students' files or settings.
- you should not interfere intentionally with, move or delete shared files stored on the network.
- you must not install or store inappropriate or illegal software on your ICT device or on the network.
- you may utilise the College network only to host or participate in game playing if this has been approved by your teacher.
- the College network must not be used as a medium to bully, harass, threaten or intimidate other users. Your behaviour on-line should reflect your behaviour offline or in person. Treat others fairly and with common courtesy.
- if you experience harassment or bullying online, don't respond, record the details, save any information you can, and contact a teacher or ICT staff member as soon as possible.
- file sharing between students' ICT devices over the network can be a security risk and you should avoid allowing other students to access your ICT device.

Internet Usage

Internet access at the College is provided for educational use and therefore personal use should be limited. All Internet use is logged and may be reviewed at any time, at the discretion of the ICT Manager.

During class time, make sure you have your teacher's permission to use the Internet. The College's internet connection is filtered to prevent access to sites, which are deemed inappropriate for College use. You should not attempt to circumvent this security.

You should exercise care when using the Internet and should not seek to download inappropriate, offensive, discriminatory or intimidating material. If you find such material you should report it to a staff member or the IT helpdesk (helpdesk@emmaus.vic.edu.au)

Accessing, storing or distributing material that is inappropriate, offensive, discriminatory or intimidating in nature, or which puts any member of the community at risk, is contradictory to the ethos of the College and will lead to disciplinary action. This may involve reporting the matter to Police where State or Federal laws have been breached.

Legal Implications

Students need to aware that the use of any ICT Device, in accessing the Internet and email is subject to specific legislation.

Section 474.17 of the *Criminal Code Act 1995 (Cth)* states that a person is guilty of an offence if they knowingly or recklessly: "Use a telecommunications device supplied by a carrier in such a way as would be regarded by reasonable persons as being, in all circumstances, menacing, harassing or offensive."

Copyright

When obtaining information from the Internet, be conscious of copyright, and always take care to verify data, as not all information found on the internet can be considered accurate. Wherever possible, the information should be validated from more than one source. References & sources should always be cited. The correct way to cite a website is URL: http://www.royal.gov.uk/Home.aspx Brief Explanation: Official Website of the British Monarchy Date & time Accessed: 19/11/2018 3:15 PM

Security and Viruses

The College provides students and parents/guardians with a copy of the College's Acceptable Use Agreement and this policy.

The Acceptable Use Agreement is provided in full for consideration by all signatories. The Agreement is to be signed by the student, parent/guardian and school representative before the student is given access to, and use of, a school's internet, network services and devices.

You should exercise caution always when you download files from the internet, as these may contain viruses, adware or spyware. Anti-Virus software is provided as part of access to the College network and you should scan your ICT device regularly to ensure that it is free from infections. Attachments on emails can contain viruses. It is important that students do not open attachments unless the source can be verified.

Unsolicited emails (SPAM) which may be offensive also, can put you, your ICT Device, and the College network at risk. The College will not be responsible for any loss or liability incurred by you through your use of the Internet.

Social Networking Sites (including Chat / Instant Messaging)

You should be careful not to give out personal information about yourself or others while using social networking, or other online applications.

- you should always follow the general guidelines outlined in this policy when accessing social networking resources, and for guidance on what to do if you encounter harassment or bullying.
- you should be sure always that you know or trust the people with whom you communicate online. Your communications should be positive in nature, and you should use appropriate language at all times. **Despite privacy settings, social networking sites are not private areas of communication.** You need to understand this fact when posting comments online.
- you need to be aware that Australian laws protect the individual's privacy and reputation. You need to understand the consequences of legal repercussions should you engage in behaviour that is defamatory, misleading or fraudulent online. Legal action can be taken by individuals in these matters.

Mobile Digital Communication Devices (Webcams / Mobile Phones/ iPads)

You should follow the College's policy always for the 'Acceptable Use of Digital Communication Devices' when using mobile phones, cameras and web cameras at the College.

- during class time, make sure you have your teacher's permission to use digital communication devices, and that it is relevant to the task being undertaken in class.
- when you record sounds or images of others, ensure that the people who are being recorded are aware and have given their consent.
- you must not upload images of other students in uniform, or images of the College grounds or buildings onto the internet.
- you must not upload material, which is inappropriate or intended to be offensive, discriminatory, intimidating or bullying in nature.

Email Usage

When you communicate via email, your communications should be positive in nature, and appropriate language should be used at all times.

- you should not use email to send material, which is inappropriate or intended to be offensive, discriminatory, intimidating or bullying in nature.
- during class time, make sure you have your teacher's permission to use email.
- you must not send unsolicited email to multiple recipients.
- you must not send email messages to more than 30 recipients at one time.
- you must not email games or game installation files to other students. This contravenes Copyright Laws and you can face prosecution if Federal & State agencies are involved.

Backup

Students must take responsibility for the backup of their schoolwork.
- students are provided with storage space on the College network to make a backup of files known as H: (or home) drive. Students are provided with 2GB space.
- students are provided also with 1 TB of cloud storage with Microsoft One Drive. This is offered through the college's licensing agreement with Microsoft.
- students should regularly backup to the network, cloud storage, portable hard drive, or any another medium outside of the student's ICT device.
- iPads need to be backed up on a home computer with iTunes software. All iPad users are to have set up an iCloud account which enables backup to Apple cloud services.

NB: Loss of data resulting in late submission of assessment tasks and classwork will not be deemed an appropriate excuse for non-submission of course work. It is the student's responsibility to ensure that they have appropriate means and procedures of back up

The College will not be responsible for any data lost.

Security and Care

Your ICT device is an essential part of learning at the College:
- you should take care to maintain your ICT device in good working condition. If you have a problem with your ICT device, you should contact the helpdesk@Emmaus.vic.edu.au so that the issue can be resolved and your ICT device returned to you.
- when your ICT device is not in use, it should be stored in its cover/bag. Your ICT device should always be kept in a locked area, or in your possession. You should take care to ensure that other students cannot gain access to your locker and always keep your combination secure.
- your ICT device should not be moved or transported while turned on. When moving the ICT device between locations, you should shut down, or place the ICT device in Hibernate or Standby.
- if you misplace your ICT device, you should immediately report this to the Assistant Principals/Head of Campus and the helpdesk@Emmaus.vic.edu.au who will then take steps to locate your ICT device.
- if you find an ICT device and the owner cannot be immediately located, you should promptly hand it to ITS or the Assistant Principal/Head of Campus so that the owner can be found.

Home Networks

The College recognises that your ICT device may be connected to a network outside the College, however, it is important that you understand that certain policies may be loaded on your ICT device in order that your device can function as required at the College.

These settings & policies can affect, and in some cases erase home wifi settings. You and/or your parents are responsible for recording your home network settings and passwords – your Internet Service Provider, provides you with these details.

Any support provided by ITS (helpdesk@Emmaus.vic.edu.au) for non-College networks is provided on a best-effort basis only, and should not be an expectation of the service provided by the technicians.

Printing

Care and conservation should be paramount considerations with regard to the use of the College printing facilities. You should keep printing to a minimum and consider each other and the environment when using these facilities. You are expected to review your documents on screen before printing out a final copy unless a teacher has requested a draft copy.

Shared Equipment

All equipment in shared areas (eg: Library) or classrooms should be treated with care, and must not be interfered with in any way. No printers, cables, ICT devices, monitors or other equipment should be moved or removed. You should never attempt to repair faulty equipment
- this includes attempts to remove paper jams from printers. You should report any failure of equipment to a member of staff or the helpdesk@Emmaus.vic.edu.au

Software Licensing Considerations

Software installed on ICT devices purchased through the College are subject to Academic Licensing agreements, and as such, the use of the software is restricted to the College and student use only.

This agreement is signed by parents and students before they are allowed to use the College facilities and devices.

Staff

Staff are required to use the internet and network services in accordance with this and other policies. The College provides staff with the following:

- a copy of this policy
- a copy of the Acceptable User Agreement.
- Information on ownership, Care, use and support of devices and mobile phones where appropriate.

Related school policies

- Anti-Bullying Policy
- Child safety policies
- Codes of conduct for students, parents and staff
- Data Breach Policy
- Managing Complaints and Grievances Policy
- Privacy Policy
- Social Media Policy for staff
- Student Behaviour Policy