

FRANKSTON HIGH SCHOOL

INFORMATION COMMUNICATION TECHNOLOGY & INTERNET USE POLICY

Approved June 2018 Updated September 2021

POLICIES AND PROCEDURES

POLICY STATEMENT

Rapid technological development and change in the 21st Century, combined with Frankston High School's 1:1 hybrid notebook tablet program, offer exciting and powerful benefits for enhanced teaching and learning opportunities and the continued improvement of student outcomes. Technology and the internet allow teachers and students to view and interact with the world through a modern lens and the ability to consume, create, collaborate and curate a vast array of information, knowledge and skills. The online world increasingly requires students and staff to be critical thinkers in a growing era of 'fake news' and 'alternative facts'. Social networking, instant messaging, smartphones, blogs, vlogs, wikis, virtual reality and an ever expanding array of new internet enabled 'smart' tools, services, apps and virtual spaces all play a significant role in both students' and staff' lives.

Students and teachers can:

- Conduct rich research
- Explore the world online
- Virtually visit and interact with museums, galleries and libraries around the world
- Access rich information resources to support research and investigations
- Communicate and collaborate with people all over the world
- Publish a vast array of media and content to the web
- Acquire new skills

Frankston High School has an important role in preparing students for 'life online', even though students and teachers may not access some online communities at school (e.g. Facebook, Instagram and Snapchat).

Before our students start to use school provided devices to explore the Internet, it's crucial to make sure everyone understands what is acceptable behaviour online.

Behaving safely online means:

- Protecting your own privacy and personal information
- Selecting appropriate spaces to work and contribute
- Knowing how to contribute positively in online spaces
- Protecting the privacy of others (this can be sharing personal information or images)
- Being proactive in letting someone know if something is 'not quite right' - at home this would be a parent or guardian, at school a teacher

These principles of safety and responsibility are not specific to the online world, but certainly apply to the use of internet resources and technology at school. Just as in the real world, the virtual world can involve some risk. Frankston High School has developed proactive strategies that help to minimise these risks to our students.

GUIDELINES

- Use of the school's devices and/or network to access the Internet and Internet services, including electronic mail, instant messaging and the World Wide Web, will be governed by an Acceptable Use Policy (AUP) for the Internet and any devices connected to it, including Personal electronic Devices (PEDs).
- The AUP is intended to encourage responsible maintenance and use of devices and to reflect respect for the ability of its adherents to exercise good judgement.
- Release of devices to students and independent student use of the internet at school will only be permitted where students and their parents/guardians provide written acknowledgement that students agree to act in accordance with the conditions of use and standards of conduct established in the AUP (see appendix A).
- While we do not ask staff to sign a written agreement, the Guidelines do apply to them. Staff should also be familiar with the DET Acceptable Use Policy which can be found at [DET Acceptable Use Policies](#)
- Students and staff can expect sanctions if they act irresponsibly and disregard their obligations to themselves, other users and the school as the provider of their Internet access.
- Students and staff must not use their laptop device or the school network in breach of a law or to commit an offence.

PROGRAM

- The use of the school's network is subject to the AUP (see appendix A). Briefly this means that the school's network can be used only by staff, students and associated individuals (e.g. visiting teachers) and only for, or in connection with the educational or administrative functions of the school.
- The AUP is intended to operate within and be consistent with existing school policies and procedures in areas such as:
 - **Anti-bullying (including cyber-bullying) and Anti-harassment**
 - **Student Wellbeing**
- Responsibility and accountability for network security is the shared responsibility of all network users. It is the responsibility of staff and students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects his/her account has been used by another person, the account holder must notify a teacher or the administration as appropriate, immediately.
- All messages created, sent or retrieved on the school's network are the property of the school, and should be considered public information. The school reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications including text and images can be disclosed to law enforcement and other third parties without prior consent from the sender.
- Independent student, staff and guest use of the internet on the school's network assumes acceptance of the AUP. By utilising our internet and network services, students, staff and guests agree to act in accordance with the standards of conduct established in this policy document and as set-out in the AUP. Students and parents sign the AUP policy upon enrolment at the school. This agreement remains active until the student graduates or exits the school officially. In any case where an agreement form has not been signed or returned, acceptance is assumed and will be enforced (See Appendix A)
- For breaches of the AUP students and staff can face a number of consequences depending on the severity of the breach and the context of the situation. More than one consequence may apply for a given offence. Serious or repeated offences will result in stronger penalties:

For Students

- Removal of network access privileges
- Removal of email privileges
- Removal of internet access privileges
- Removal of printing privileges

- Paying to replace damaged equipment
- Other consequences at the discretion of the school, as outlined in the school's discipline policy

For Staff

- Non-compliance will be regarded as a serious matter and appropriate action, including termination of employment may be taken
- Bullying and harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, gender or sexual preference will be transmitted. Violations of any guidelines listed above may result in disciplinary action.
- While the Internet may be largely a self-regulated environment, the general principles of law and community standards still apply to communication and publishing via the Internet. In addition to school penalties, there are legal sanctions for improper use of the Internet.

LINKS AND APPENDICES (including processes related to this policy)

The Key Link connected with this policy is:

[DET Using Technology to Support Teaching](#)

Appendix A:

AUP for the mobile devices and the Internet

Other school policies which are connected with this policy are:

- The school's Anti-bullying (including cyber-bullying) and Anti-harassment Policy
- The school's Student Engagement & Wellbeing Policy

EVALUATION

This policy will be reviewed annually or more often if necessary due to changes in regulations or circumstances.

FRANKSTON HIGH SCHOOL
Technology and Personal Electronic Device (PED)
Acceptable Use Agreement

Overview & Purpose

The use of Information and Communication Technologies (ICT) plays an integral role in the teaching and learning program of Frankston High School. Maintaining the safety and wellbeing of all students is vitally important, as is access to ICT resources, in order to enable our students to experience success and develop 21st Century skills. Students must be aware of how they can create and maintain a positive digital footprint for their future.

Parents AND students must read, discuss and adhere to the 'Acceptable Use Agreement', which will remain in effect for the duration of the child's enrolment at Frankston High School, and will apply even while on camps and excursions.

It is essential parents actively support the conditions and intentions behind this 'Acceptable Use Agreement'.

The Agreement

This agreement applies to all students and any ICT resource(s) that may be used when a student of Frankston High School is at school or associated with the school on extra curricular activities. This agreement also includes personal devices students bring on to school grounds. These are considered Personal Electronic Devices (PED). This agreement applies to students accessing Frankston High School Wi-Fi or their own personal/private connection to the internet. PEDs include (but are not limited to): mobile phones, smartphones, smart watches, notebooks, laptops, iPads/iPods, notebooks, slates and tablets, gaming consoles, cameras, 'dongles', 3G/4G/5G connected devices and any other device(s) that may provide a connection(s) to the internet or can be considered a digital tool.

Legitimate Use of ICT/PED Resources and Network Includes the Following

- Research and learning activities prescribed by teachers as part of the school curriculum.
- The use of e-mail and other teacher prescribed communication tools including social networks and media, software and web based services for exchanging appropriate information and engaging in collaborative projects, planning and communication for school work purposes.
- The creation of content for assigned classwork, homework and project work.
- The storage of content created for school purposes on the Frankston High School Portal, MySite, OneDrive and/or other approved storage solutions.
- The use of educational games and software related to prescribed learning activities by teachers to support teaching and learning.
- The completion of homework, research for school related assignments, projects and other set learning activities.

Unacceptable use of Computer/ PED and Network Resources Include:

- Being in the possession of, sending or displaying offensive and anti-social material (text, images, sound, video files, etc.).
- Using obscene language via e-mail or any other communication medium.
- The playing of non-approved computer games.
- Accessing or attempting to access blocked websites.

- Using ICT devices or software (including PED or Department of Education and Training owned) to harass, insult, intimidate, bully, defame or attack other people or groups in any way.
- Use computer and/or internet resources, **including social networking sites**, to cause harm to relationships between fellow students, staff members or anyone else in our wider community, be it at school or home.
- Failure to store and transport a laptop computer in an appropriate protective bag or carry case.
- Damaging computers, computer systems or computer networks (for example; by the creation, introduction or spreading of computer viruses, physically abusing hardware or peripherals, altering source codes or software configurations etc.)
- Installing and using a Private Virtual Network (VPN) in order to bypass the schools security and safety network or bypass the filtering of the schools firewall and policies.
- Seeking to or possessing software that is capable of accessing protected sections of any network, to damage the network, or to obtain other peoples' personal data and/or passwords.
- Violating copyright laws including the legal rights of software producers and network providers. Copyright and license agreements must be honoured (for example; illegally downloading or sharing copyrighted games, movies, music or TV programs could result in legal proceedings, resulting in a fine or conviction).
- Using or attempting to use other people's passwords or allowing others to use your login/password details.
- Trespassing or altering other students' or staff folders, work or files in any way without express permission.
- Employing the network for commercial purposes or activities by for-profit institutions or organisations, product advertisements or political lobbying is prohibited.
- Using the network to disrupt its use by other individuals or by connecting networks.
- Disrespect of others' privacy and intellectual property.
- Using any means to avoid scrutiny by teachers whilst the class is in progress (for example: hidden screens).
- Using the network in class without the express permission of the teacher in charge.
- Not keeping tablet notebooks or other ICT resources in working order.

Breaches of the Technology and Personal Electronic Device (PED) Acceptable Use Agreement

Breaching any of the above conditions will result in strict disciplinary action from Year Level Coordinators and/or technical intervention (for example: notebook/tablet re-imaged, loss of email and intranet privileges, network and/or internet access denied or restricted etc.). Further breaches will result in a formal meeting with parents/guardians, Year Level Coordinator and Assistant Principal to discuss your child's future use of and access to Frankston High School's technology resources and network. Serious breaches and incidents may also be referred to Police. Students who bring PEDs into school grounds, with or without independent internet access are bound by this agreement. Misuse of a PED will result in strict disciplinary action including confiscation of the device. Confiscated devices must be collected by a parent/guardian at a later date, following a meeting with a Year Level Coordinator and/or Assistant Principal.

Important: Network storage areas, internet history and use of the network will be treated like lockers, in that network administrators may review files and communications to maintain integrity and ensure that users are adhering to our expectations.

Note: This agreement, the conditions and intentions may be altered at any time. Changes will be announced through the school newsletter.

Further Cyber Safety Assistance

If parents, guardians or students require any further assistance or advice relating to cyber-safety related issues, please contact relevant sub school Coordinators, a member of the Student Wellbeing Team or an Assistant Principal.

For other matters or further advice and resources, you might like to consult the office of the Children's Safety Commissioner here: <https://www.esafety.gov.au/>

Please read the attached information closely, discuss with your child, sign, detach and return.

Parent

I have read the attached policy and agree to my son/daughter having access to the school network and ICT resources. I have discussed all the above points with my child and I believe they understand their responsibilities. I will support the school in its endeavours to provide a safe and reliable e-learning environment.

Signed: _____ **Date:** _____
(Parent/Carer)

Student

I have read the attached policy and understand my responsibilities. I agree to use any personal electronic device or school owned computer resource(s) in an acceptable manner as outlined above.

Student's Name: _____ **Year Level:** _____

Signed: _____ **Date:** _____
(Student)