DIGITAL LEARNING
(INTERNET, SOCIAL MEDIA AND DIGITAL DEVICES)

Help for non-English speakers

If you need help to understand the information in this policy please contact Gembrook Primary School.

PH: 03 5968 1313 email: gembrook.ps@education.vic.gov.au

PURPOSE

To ensure that all students and members of our school community understand:

(a) Our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school.
(b) Expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets).
(c) The school's commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies.
(d) Our school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet.
(e) The various Department of Education policies on digital learning, including social media, that our school follows and implements when using digital technology.
(f) Our school prioritises the safety of students whilst they are using digital technologies.

SCOPE

This policy applies to all students and staff at Gembrook Primary School.

Staff use of technology is also governed by the following Department of Education policies:

- Acceptable Use Policy for ICT Resources
- Cybersafety and Responsible Use of Digital Technologies
- Digital Learning in Schools
- Social Media Use to Support Student Learning
- Staff also follow our school's Acceptable Use Policy

Staff, volunteers, and school councillors also need to adhere to codes of conduct relevant to their respective roles. These codes include:

- Gembrook Primary School Child Safety Code of Conduct
- The Victorian Teaching Profession Code of Conduct (teaching staff)
- Code of Conduct for Victorian Sector Employees (staff)
- Code of Conduct for Directors of Victorian Public Entities (school councillors)

DEFINITIONS

For the purpose of this policy, “digital technologies” are defined as digital devices, tools, applications and systems that students and teachers use for learning and teaching; this includes Department of Education provided software and locally sourced devices, tools and systems.

POLICY

Vision for digital learning at our school

The use of digital technologies is a mandated component of the Victorian Curriculum F-10.

Safe and appropriate use of digital technologies, including the internet, apps, computers, and tablets, can provide students with rich opportunities to support learning and development in a range of ways.

Through increased access to digital technologies, students can benefit from learning that is interactive, collaborative, personalised, engaging, and transformative. Digital technologies enable our students to interact with and create high quality content, resources, and tools. It also enables personalised learning tailored to students’ particular needs and interests and transforms assessment, reporting and feedback, driving new forms of collaboration and communication.

Gembrook Primary School believes that the use of digital technologies at school allows the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world. Our school’s vision is to empower students to use digital technologies safely and appropriately to reach their personal best and fully equip them to contribute positively to society as happy, healthy young adults.

Personal Devices at Gembrook Primary

Gembrook Primary School accepts that some parents provide their children with mobile phones and other personal electronic devices. However, whilst on school property and during school excursions and camps, use of mobile phones or other personal electronic devices is not permitted by students unless specifically authorised by the Principal.

Gembrook Primary School students must hand in all mobile phone devices and smartwatches to the school office on arrival at school each day. Students must ensure that the device is turned off. All student devices shall be kept in individual, labelled pouches, and stored at the school office in a lockable cabinet for the duration of the school day. It is the students’ responsibility to collect their device after being dismissed from their classroom at the end of each day.

Gembrook Primary School students may occasionally be invited to bring their own personal electronic device to school as part of our Positive Behaviours for Learning initiative. Mobile phones and smartwatches are not permitted as personal electronic devices for this purpose.

When bringing their own personal electronic device to school, students should ensure that it:

- Is fully charged.
- Is brought to school in a protective case.
- Is handed to their classroom teacher at the beginning of the day.
- Remains switched off before and after the activity.
- Remains switched off before and after school.

- Remains switched off while travelling on the school bus.

Please note that our school does not have insurance to cover accidental damage to or loss of a students' personal electronic devices, and parents/carers are encouraged to consider obtaining their own insurance for their child's personal electronic device.

Students, parents and carers who would like more information or assistance regarding our Positive Behaviours for Learning initiative 'Bring Your Own Device' reward sessions are encouraged to contact the school Principal.

Safe and appropriate use of digital technologies

Digital technologies, if not used appropriately, may present risks to users' safety or wellbeing. At Gembrook Primary School, we are committed to educating all students to use digital technologies safely, equipping students with the skills and knowledge to navigate the digital world.

At Gembrook Primary School we:

- Use online sites and digital tools that support students' learning and focus our use of digital technologies on being learning-centred.
- Use digital technologies in the classroom for specific purpose with targeted educational or developmental aims.
- Supervise and support students using digital technologies for their schoolwork.
- Effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students, consistent with our Student Engagement and Wellbeing and Bullying Prevention policies.
- Have programs in place to educate our students to be safe, responsible, and discerning users of digital technologies, including [insert details of specific programs.
- Educate our students about digital issues such as privacy, intellectual property and copyright, and the importance of maintaining their own privacy and security online.
- Actively educate and remind students of our *Student Engagement* and Wellbeing policy that outlines our school's values and expected student behaviour, including online behaviours.
- Have an Acceptable Use Agreement outlining the expectations of students when using digital technologies for their schoolwork (which must be signed by students and parents prior to usage).
- Use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities and removing offensive content at the earliest opportunity.
- Educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies.
- Provide a filtered internet service at school to block access to inappropriate content.
- Refer suspected illegal online acts to the relevant law enforcement authority for investigation.
- Support parents and carers to understand the safe and responsible use of digital technologies and the strategies that can be implemented at home.

Distribution of school owned devices to students and personal student use of digital technologies at school will only be permitted where students and their parents/carers have completed a signed *Acceptable Use Agreement*.

It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify the classroom teacher.

All messages created, sent, or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

Information on supervision arrangements for students engaging in digital learning activities is available in our Yard Duty and Supervision Policy.

Social media use

Our school follows the Department of Education's policy on Social Media Use to Support Learning to ensure social media is used safely and appropriately in student learning and to ensure appropriate parent notification occurs or, where required, consent is sought. Where the student activity is visible to the public, it requires consent.

In accordance with the Department of Education's policy on social media, staff will not 'friend' or 'follow' a student on a personal social media account or accept a 'friend' request from a student using a personal social media account unless it is objectively appropriate, for example where the student is also a family member of the staff.

If a staff member of our school becomes aware that a student at the school is 'following' them on a personal social media account, Department of Education policy requires the staff member to ask the student to 'unfollow' them, and to notify the school and/or parent or carer if the student does not do so.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with Gembrook Primary School's *Statement of Values, Student Wellbeing and Engagement* policy, and *Bullying Prevention* policy.

When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), Gembrook Primary School will institute a staged response, consistent with our Student Wellbeing and Engagement, and Bullying Prevention policies.

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation. This includes:

- Removal of network access privileges.
- Removal of email privileges.
- Removal of internet access privileges.
- Removal of printing privileges.
- Other consequences as outlined in the school's *Student Wellbeing and Engagement* and *Bullying Prevention* policies.

COMMUNICATION

This policy will be communicated to our school community in the following ways:

- Included in staff induction processes.
- Discussed at staff briefings or meetings, as required.
- Included in our staff handbook.
- Included as a reference in our school newsletter.
- Made available in hard copy from school administration upon request.

POLICY REVIEW AND APPROVAL

Policy last reviewed	May 2023
Consultation	School Council May 2023 School community Staff
Approved by	Principal
Next scheduled review date	2026

ANNEXURE A: ACCEPTABLE USE AGREEMENT

Gembrook Primary School Acceptable Use Agreement

Definitions of terms used in these guidelines.

a. 'Authorised user' means a person who has signed the Acceptable Use Agreement (or has had it signed on their behalf by a parent) and is authorised by the school to use school ICT.

b. 'Acceptable Use Agreement' refers to the name of the cybersafety guidelines that are followed at Gembrook Primary School to promote the safe, responsible and ethical use of ICT.

c. 'ICT' stands for 'Information and Communication Technologies' and includes network facilities, communication technologies, eLearning tools and ICT equipment/devices.

d. 'Network facilities' includes, but is not limited to, the Ultranet and internet access to files, web sites and digital resources via the school network.

e. 'Communication technologies' includes, but is not limited to, communication made using ICT equipment/devices such as internet, email, instant messaging, online discussions/surveys and mobile phone activities and related applications.

f. 'eLearning' refers to the use of ICT for educational purposes.

g. 'ICT equipment/devices' include, but are not limited to, computers (such as desktops, laptops, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, smartwatches and any other similar technologies as they come into use.

h. 'Agreement' refers to the Acceptable Use Agreement which will be reviewed annually.

i. 'School' means Gembrook Primary School.

j. 'School related activity' includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.

k. 'School ICT' refers to any ICT owned or operated by the school including, but not limited to, network infrastructure, computers, cameras, tablet devices.

l. 'Objectionable material' includes, but is not limited to, pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be detrimental to the wellbeing of students or unsuitable to a school environment.

m. 'Unacceptable student conduct' includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft or copyright infringement.

n. 'Educational purposes' means activities that are directly linked to curriculum related learning.

o. ‘Personal electronic devices’ includes, but is not limited to, handheld gaming consoles (including but not limited to Nintendo DS, PSP Wii U), MP3 players (including but not limited to iPod, iPod Touch), e-readers (including but not limited to Kindle, Kobo) other internet and 3G accessible devices, and any other similar such devices as they come into use.

Purpose

Our aim is to provide an educative environment by establishing a cybersafe culture which is in keeping with the values of the school, legislative and professional obligations, and the community’s expectation. Within this context, the objectives of these guidelines are to ensure the smart, safe, responsible use of ICT within the school community.

These guidelines outline the conditions applying to the use of all school ICT and behaviours associated with safe, responsible and ethical use of technology. Authorised users are required to comply with the usage agreement.

Authorised User Obligations

1. Authorised Usage Agreement

1.1. As the school provides network access, the contents of the school ICT system, including email messages, remain the property of the Department of Education. The school has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

1.2. All students, whether or not they make use of network facilities and communication technologies on school owned or personal ICT equipment/devices, will be issued with this Agreement. This document should be read carefully with the acknowledgement page signed and returned to the student’s class teacher.

1.3. The school’s ICT, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the acknowledgement page of this Agreement has been signed and returned to the student’s class teacher. Signed Agreements will be filed in a secure place.

1.4. The school encourages anyone with a query about these guidelines or the Agreement to contact your child’s class teacher in the first instance.

2. Obligations and requirements regarding appropriate use of ICT in the school learning environment

2.1. While at school, using school owned ICT equipment/devices is for educational purposes only.

2.2. When using school ICT on the school site or at any school related activity prohibited use includes, but is not limited to, any conduct that is defined as objectionable and inappropriate:

- Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, or sexism.
- Is derogatory or threatening to another e.g. libellous, slanderous, inflammatory, threatening, harassing.

- Has intention to deceive, impersonate or misrepresent.
- Forwards confidential messages to persons to whom transmission was never authorised by the school, including persons within the school community and persons/organisations outside the school community.
- Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus.
- Breaches copyright.
- Attempts to breach security and infrastructure that is in place to protect user safety and privacy.
- Results in unauthorised external administration access to the school's electronic communication.
- Propagates chain emails or uses groups or lists inappropriately to disseminate information.
- Inhibits the user's ability to perform their duties productively and without unnecessary interruption.
- Interferes with the ability of others to conduct the business of the school.
- Involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/devices.
- Involves the unauthorised installation and/or downloading of non-school endorsed software.
- Breaches the ethos and values of the school.
- Is illegal.

2.3. In the event of accidental access of such material, Authorised Users must:

- Not show others.
- Shut down, close or minimise the window.
- Report the incident immediately to the supervising teacher.

2.4. A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of school, or privately owned communication technologies, on the school site or at any school related activity, may also be found to have engaged in prohibited use.

2.5. While at the school or a school related activity, Authorised Users must not have involvement with any material which might place them at risk. This includes images or material stored on privately owned ICT equipment/devices brought onto the school site, or to any school related activity such as USB sticks.

2.6. Authorised users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any Authorised Users with a query or a concern about that issue must speak with the relevant class teacher or subject teacher.

3. Monitoring by the School

The school:

3.1. Reserves the right at any time to check work or data on the school's computer network, email, internet, computers and other school ICT equipment/devices, without obtaining prior consent from the Relevant Authorised User.

3.2. Reserves the right at any time to check work or data on privately owned ICT equipment on the school site or at any school related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the school for purposes of any such check and to otherwise co-operate with the school in the process. Before commencing the check, the school will inform the Authorised User of the purpose of the check.

3.3. Has an electronic access monitoring system, through Netspace (in accordance with Department of Education requirements), which has the capability to restrict access to certain sites and data.

3.4. Monitors traffic and material sent and received using the school's ICT infrastructures. From time to time this may be analysed and monitored to help maintain a cybersafe learning environment.

3.5. From time to time conduct an internal audit of its computer network, internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit of content and usage.

4. Copyright, Licensing, and Publication

4.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images.

4.2. All material submitted for internal publication must be appropriate to the school environment and copyright laws.

5. Individual password logons to user accounts

5.1. Authorised Users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system.

5.2. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with this Agreement. This includes ensuring that no electronic communications could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the school environment.

5.3. For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others online. Personal information may include, but is not limited to, home addresses and telephone numbers.

6. Other Authorised User obligations

6.1. Avoid deliberate wastage of ICT related resources, through actions such as unnecessary printing and unnecessary internet access.

6.2. Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.

6.3. Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

7. Privacy

7.1. School ICT and electronic communication should never be used to disclose personal information of another except in accordance with the school's privacy agreement or with proper authorisation. The Privacy Act requires the school to take reasonable steps to protect the personal information that is held by the school from misuse and unauthorised access. Authorised users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

7.2. While after school use of communication technologies by students is the responsibility of parents, school policy requires that no student attending the school may identify, discuss, photograph or otherwise publish personal information or personal opinions about school staff, fellow students or the school. Any such behaviour that impacts negatively on the public standing of the school will result in behaviour management measures being applied, consistent with our Student Engagement and Wellbeing Policy and Bullying Prevention Policy.

The school takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, Snap Chat, YouTube, Instagram, Tik Tok, Tumblr (and any further new technology).

8. Procedures for Mobile Phone and Other Electronic Device Use at School

Gembrook Primary School accepts that some parents provide their children with mobile phones and other personal electronic devices. However, whilst on school property and during school excursions and camps, use of mobile phones or personal electronic devices is not permitted by students unless specifically authorised by the Principal.

Responsibility

8.1. It is the preference of the school that mobile phones and personal electronic devices are not to be brought to school.

8.2. It is the responsibility of students who do bring mobile phones or personal electronic devices onto school premises to adhere to the Mobile Phone Policy.

8.3. Students are to switch off their phone or personal electronic device when they enter the school grounds and hand it to an office staff member for storage.

8.4. The school accepts no responsibility for replacing lost, stolen or damaged mobile phones or personal electronic devices. Their safety and security is wholly in the hands of the student.

8.5. The school accepts no responsibility for students who lose or have their mobile phones or personal electronic devices stolen while travelling to and from school.

8.6. It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

8.7. Students must protect the privacy and dignity of individuals and security of information, to maintain the public standing of the school and compliance with State and Federal laws.

8.8. The school strongly advises that for safety reasons headphones should not be used when students are traveling to and from school, e.g. walking, riding a bike, moving on and off buses.

8.9. In accordance with school policies, any mobile phone or personal electronic device being used during the school day will be confiscated and placed in secure storage located at the school office.

Parents are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way. Phone calls home to parents are to be made with a staff member.

Breach of Agreement

Breaches of this Agreement will be dealt with in accordance with the school Student Wellbeing and Engagement Policy and/or Bullying Prevention Policy.