LE FEVRE
HIGH SCHOOL

ICT SERVICES POLICY

INTRODUCTION

All staff and students can connect their own personal device to the Le Fevre High School (LFHS) network. All students in years 7 to 12 are required to have their own personal device of either a Chromebook or Laptop that meets the school minimum specifications. The device must be brought to school each day and used in accordance with this policy.

It is an expectation that devices owned by students and brought to school comply with the appropriate legal operating system and software licensing requirements. Connection to the network will allow access the following:

- access to the school wireless network
- limited technical support
- access to the internet
- access to printing
- access to the school's learning management system – Daymap
- provision of access at no cost to Microsoft Office and OneDrive cloud storage whilst enrolled as a Department for Education student at Le Fevre High School

Note: access to the school's file servers is not allowed or permitted.

Bringing a device to school and using the school's network is a privilege and not a right and may be revoked by the school.

ALLOWED DEVICES

To assist in teaching and learning, staff are allowed to connect any type of device to the network.

Students are permitted to only connect a laptop or Chromebook to the school's network. Any attempt to connect their mobile phone or other smart device will be prohibited.

ACCEPTABLE USE

Students connecting to the network either on a school issued device or personal device must comply with the following:

- Students must only use their own assigned computer network account.
- Students must not share personal information about themselves or other students with third parties, including their username or passwords.
- School ICT assets must not be used to access or share inappropriate content online, including sexually explicit materials, obscene depictions, harmful materials, illegal activities, profane or abusive language, or content that other students may find offensive.
- Web and email content filtering must not be circumvented to access content that has been deemed inappropriate for students.

- Copyright materials (including games and movies) must not be illegally downloaded onto or acccessed using school or department issued ICT assets.
- When using online communities, users must communicate kindly and respectfully at all times. Students must not participate in harassing or bullying other students online.
- Students should not forward chain letters, spam or other unsolicited communications.
- Students must not participate in business activities that is not staff approved or done so as part of curriculum learning.
- All students must report suspicious activity or violations of this policy to a staff member.
- Students must not violate any state or federal laws, including purchase of illegal items or substances, criminal activities punishable by law, etc.
- Students must not take photos or videos of another individual without their consent.
- Students should not use school or department ICT assets to stream large volumes of data unless in the course of curriculum activities (e.g. streaming services such as Netflix, online gaming etc).
- Students must not install unapproved software on school or department issued devices.

If a school owned ICT device is damaged or lost by neglect, abuse or malicious act, the Principal will determine whether replacement is appropriate and/or whether or not the student retains access to another laptop or other school computing facilities for use. In such cases repair or replacement costs may be passed on to the parent/caregiver for payment. School policies related to the recovery of debts will apply.

Our school reserves the right to monitor use of ICT assets used by students. Students that misuse assets or use assets in an inappropriate manner may have their access revoked.

PRINTING

- At school, users will be able to print to a printer queue and collect their printing from a nearby printer/print release station via the PaperCut App.
- Students will receive a yearly allocation of funds for printing.

Note: students can check they have sufficient credit by logging into their PaperCut account and can request additional funds from the ICT support centre or with their teacher.

LIMITED TECHNICAL SUPPORT

Students who require support for connecting their account to the network are able to obtain assistance from ICT Services, however any technical or software faults should be returned to the place of purchase or a preferred repairer.

BACKUP AND DATA STORAGE

It is the student's responsibility to ensure their data is regularly backed up. The method for backing up data is dependent on the device but it highly recommended that students use the OneDrive cloud storage provided for this purpose. Users are responsible for backing up their data to the cloud or other methods such as a portable USB or hard disk.

- School network drives will not be available for storage of student work.
- Students can submit work to teachers by email or Daymap.
- The school cannot be held responsible for lost work due to a failure to backup.

GAMES

The use of games within the teaching and learning program is at the discretion of the teacher. Games must be PG rated and during school time as this will impact on battery performance negatively. It is the student's responsibility for proper battery management. In particular, while some games have significant educational benefits, other games have little educational merit and may affect network function. As a result:

- the use of network games is banned.
- no ad-hoc networks are to be formed.

INTERNET ACCESS

USAGE

Internet usage is monitored and is subject to Department for Education filtering. Inappropriate downloads can be detected when devices are connected to the school's network. While every reasonable effort is made by the school and Department for Education to prevent student exposure to inappropriate content when using the Department's online services, it is not possible to eliminate the risk of such exposure. In particular, the Department cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. The Department recommends the use of appropriate Internet filtering software.

COST

Using the internet and downloading data incurs a cost when used at school. Credit for internet usage is covered in the Materials and Services fee.

VIRUS PROTECTION

- Anti-virus software must be installed onto the device.
- If a student's device attempts to connect to the school network and is found to have a virus, the laptop will be disabled.
- Students should ensure that anti-virus software is kept up-to-date on their devices and regularly check for viruses.
- As students have the right to use their own laptops and connect to the internet from home, they must take all necessary steps to protect the laptop from virus attacks.

VIRUSES CAN ENTER LAPTOPS THROUGH:

- removable media such as CDs, DVDs and USB memory sticks
- emails
- the internet (including web browsing, FTP programs and chat rooms).

TIPS:

- do not open any files or links attached to suspicious or unknown emails
- exercise caution when downloading files from the internet. Save the files to the laptop's hard disk and run the virus scanner on the files before opening them
- delete chain and junk emails. Do not forward or reply to any of these
- never reply to spam
- hundreds of new viruses are discovered each month. Run your virus scan regularly.

WEB 2.0 APPLICATIONS

There are significant educational benefits for some Web 2.0 applications. A Web 2.0 site allows its users to interact with other users. These include web-based communities, hosted services, web applications, social-networking sites, video sharing sites, wikis and blogs. However, many Web 2.0 applications can be unproductive and distracting to student learning. If accessed at home the school will not be liable for any consequences.

Educational Web 2.0 technologies will be used as part of a student's study in various classes. The use of Web 2.0 applications are based on the condition that:

- the technologies, and the use of the technologies, do not breach any ethical and moral issues
- the applications do not distract student learning
- the Web 2.0 technologies are not to be accessed in class, unless specifically directed by the teacher for educational purposes
- Web 2.0 technologies may be accessed at recess and lunch times.

CLOUD COMPUTING

The detail below sets out the terms on which you may access 'Cloud Computing Services' provided by the school, including but not limited to; Google Apps for Education, blogs, Office 365, ClickView, Snowflake, eBooks, Adobe Creative Cloud, Freshdesk, Trimble Sketchup, General Audit Tool, Wheelers ePlatform, Acer PAT, Naplan, SACE, GeoGebra. Le Fevre High School reserves the right to sign-up students to other cloud-based services for educational purposes. Cloud computing involves the use of internet-based services (rather than a PC or school server) for functions such as email, blogs and data storage.

By signing the Student Permissions Form, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this Policy, including the consequences of any breach of the terms.

Le Fevre High School will use personal information, such as student's first name and last name to sign up to Cloud Computing Services. The services accessed by the students will have educational value and will be used as instructed by Le Fevre High School staff.

1. PRIVACY CONSENT

Information that you transfer or store using the school's Cloud Computing Services may be stored by their respective service providers in the United States of America, or such other country as the cloud service providers may decide. By using the school's Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

2. ACCEPTABLE USE

You agree that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

- give your account password to anyone else;
- access (or try to access) anyone else's account, or try to defeat any security controls;
- send or help to send unsolicited bulk email (spam);
- publish, send or knowingly access material that is pornographic, hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;
- knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.

3. MONITORING

You agree that IT Support Staff responsible for IT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

If you notice a problem with the Cloud Computing Services, or if you think that someone is trying to access your account (or someone else's account), you agree that you will tell the school's IT Support Staff immediately.

HACKING

Hacking is a criminal offence under the Cyber Crime Act (2001). Any hacking attempts will be forwarded to SAPOL.

CYBER BULLYING

E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways. Cyber bullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technology such as email, chat room discussion group, instant messaging, WebPage or SMS (text messaging) with the intention of harming another person. Examples can include communications that seek to intimidate, control, manipulate and put down or humiliate the recipient.

Activities can include flaming (repeated negative messages), sexual and racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking. The targeted person often feels powerless and may need help.

ELECTRONIC CRIME (E-CRIME)

Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.
Cyber bullying can therefore be an e-crime, a fact often not clearly understood by those involved.

E-crime occurs when a computer or other electronic communication devices (eg. mobile phones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence. Serious breaches are a police matter and will be dealt with through State and Federal laws and SAPOL.

SECURITY AND STORAGE

During the school day when the devices are not being used (for example at lunchtime and during PE etc), the devices should be kept securely locked in the student's locker or carried with the student. The device must be properly powered off prior to storage to preserve battery life and to prevent heat build-up.

POWER ISSUES/BATTERY/CHARGING

Students should come to school with their laptops fully charged as NO charging is allowed in classrooms, as per Work Health and Safety regulations.

LAPTOP/CHROMEBOOK LOAN PROGRAMS

- The school reserves the right to confiscate any device issued through school device programs if the conditions of the agreements entered into with Le Fevre High School are broken.
- Users who have agreed to loan a School Owned Chromebook or Laptop are wholly responsible for always maintaining the device in good repair and condition. Any breakages or wilful damage can be subject to cost recovery and must be reported to ICT Services. Chromebook manufacturing defects are covered by the school warranty.
- A Chromebook / Laptop Program device purchased or loaned through the school, may have other applications installed by the user of the device, providing that the software meets the following criteria:
  - does not attempt to circumvent security measures or gather information from other devices (snooping, sniffing or other network inspection tools)
  - does not gain unauthorised access to other systems or school ICT infrastructure and is legally obtained. No pirated software or media of any kind is permitted.

AGREEMENT

All Parents/Caregivers and students are required to accept the conditions of this Policy by signing the student permissions form.

Students are required to register their BYO device with ICT Services to enable connection to the school network.

Updated December 2023