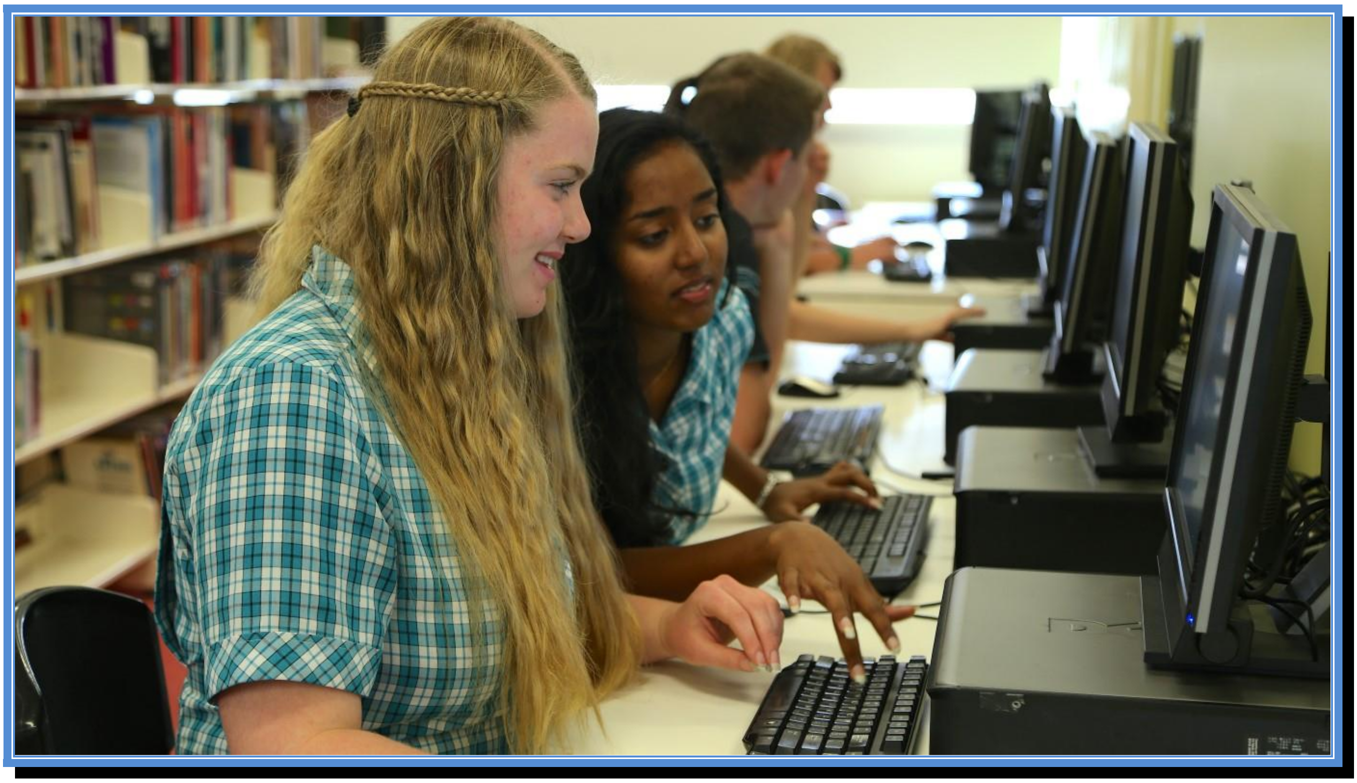
Information and Communication Technologies (ICT) Use Agreement at Le Fevre High School 2017



Issue No: 6
Dated June 2016

ICT USE AGREEMENT AT LE FEVRE HIGH SCHOOL

The aim of the Australian Government's Digital Education Revolution (DER) is to ensure all Year 9-12 students have improved access to computers to improve their learning. To this end, Le Fevre High School, together with the Department of Education and Child Development (DECD), has embarked on an extensive program to upgrade and increase the number of computers in the school.

All equipment purchased through the DER program is the property of the South Australian Minister for Education.

As part of the DER initiative, ICT Use Agreements are required to be signed by students and parents/caregivers in relation to the use of computers at school. **This agreement supersedes all previously signed agreements relating to computer use in schools. The agreement will remain in force as long as your child is enrolled at this school.**

If it becomes necessary to add/amend any information or condition, you will be advised in writing.

Acceptable Use

As is the case with all ICTs in DECD schools, policies on the safe and acceptable use of ICTs apply to DER computers. (See *Important Terms* later in this booklet for explanation of ICTs.)

All students and their parents/caregivers are required to sign an ICT Use Agreement that covers the care, use and management of computers in a cyber-safe learning environment. Included in the management are security, email, Internet access and virus protection as well as cyber-safety.

The use of school applications and files is for the benefit of students' learning. As such, the use of an allocated or on loan computing resources is on the understanding that your child will access applications and files in safe and ethical ways. Your child needs to be aware that the school's wellbeing and behaviour management processes extend outside school hours or off-site.

Le Fevre High School reserves the right to monitor the content of student laptops.

Cyber-safety

Le Fevre High School is committed to being a cyber-safe learning environment. Please see the enclosed POLICIES AND STRATEGIES TO HELP KEEP STUDENTS CYBER-SAFE for strategies to help us stay safe when using ICT at school and after formal school hours.

It should be noted that if a student who is enrolled in a school behaves online in a manner that threatens the wellbeing of another child, student, parent or member of the school community, even if this occurs off-site and/or out of school hours, the principal has the authority under the Regulation pursuant to the Education Act 1972 to suspend or exclude a student from attendance at school.

If the Principal or a delegate of the Principal suspects an electronic crime has been committed, this must be reported to the South Australian Police Department (SAPOL). Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device, eg laptop, the device will be confiscated and handed to the investigating police officer. SAPOL will determine any further action.

RESPONSIBILITIES WHEN COMPUTERS ARE USED AT LE FEVRE HIGH SCHOOL

Care of computers

Students are expected to care for computers.

Students have access to computers with the knowledge that the computers are in good care and working order. At the time of use students are required to report operational or damage issues to their teacher AND the IT managers/technicians.

In the case where a computer/laptop has been provided to a student for in-school use, it is provided in good care and working order and is confirmed at the time. If at any time there are operational or damage issues, your child will report it to the IT technicians. If the damage is wilful or if the computing device is lost from an unsecured location, parents may be responsible for the full replacement cost of the laptop. School policies related to the recovery of debts will apply.

If a laptop 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.

Non-school applications and files

At all times the performance of computers and laptops is for the primary purpose of student learning. Some software can slow down the performance of the device or corrupt it so that it is unusable. **Approval from the IT Manager must be sought before loading non-school software.** Some software, even if approved for installation, may not be supported by the school. In general restrictions are in place to ensure students cannot install software on the IT facilities of the school.

The consequence of contravening school policies on the use of non-school applications will be the restoration of computers and laptops to their original specifications, with the consequential loss of all student data. In addition ***other consequences may apply including but not limited to the right of access or use to school ICT equipment being revoked by the school in such circumstances for a period to be determined by the Principal, and or disciplinary measures such as immediate referral to the withdrawal room, internal or external suspension.***

It is the responsibility of the student to ensure files related to their learning are backed-up in an alternative location as a matter of good practice.

Printing

Students are advised to use the print preview that is available in programs and restrict printing to single copies only. The printing software provides an annual allowance. Further printing may then be purchased.

Students are expected to meet their obligations

in relation to use of the computers and laptops

POLICIES AND STRATEGIES TO HELP KEEP LFHS STUDENTS CYBER-SAFE

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception, and we invite you to discuss with your child the following strategies to help them stay safe when using ICT at school and after formal school hours.

1. I will not use school ICT equipment until my parents/caregivers and I have signed my ICT Use Agreement form and the completed form has been returned to school.

2. I will log on only with the user name provided to me by the school. I will not allow anyone else to use my name.

3. I will keep my password private.

4. While at school or a school related activity, I will inform the teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (eg bullying or harassing).

5. I will use the Internet, e-mail, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.

6. I will use my mobile phone/s only at the times agreed to by the school during the school day.

7. I will go online or use the Internet at school only when a teacher gives permission and/or an adult is present.

8. While at school, I will:
   - access, attempt to access, download, save and distribute only age appropriate and relevant material
   - report any attempt to get around or bypass security, monitoring and filtering that is in place at school.

9. If I accidentally access inappropriate material, I will:
   - not show others
   - turn off the screen or minimise the window
   - report the incident to a teacher immediately.

10. To ensure my compliance with copyright laws, I will download or copy files such as music, videos, games or programs only with the permission of a teacher and the owner of the original material. If I infringe the Copyright Act 1968, I may be personally liable under this law. This includes downloading such files as music, videos, games and programs.

11. My privately owned ICT equipment/devices, such as a laptop, mobile phone, USB/portable drive I bring to school or a school related activity, is also covered by the Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.

12. Only with permission from the teacher will I connect any ICT device to school ICT, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.

13. I will not install any application onto the ICT equipment of the school, including laptops without the express permission of the IT Manager.

14. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:
    - my full name
    - my address
    - my e-mail address
    - my phone numbers
    - photos of me and/or people close to me.

15. I will respect all school ICTs and will treat all ICT equipment/devices with care. This includes:

- not intentionally disrupting the smooth running of any school ICT systems
- not attempting to hack or gain unauthorised access to any system
- following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
- reporting any breakages/damage to a staff member.

16. The school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including e-mail.

17. The school may monitor and audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including e-mail.

18. If I do not follow cyber-safe practices, the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

19. I will not use school ICT equipment to access other wireless networks other than that provided by the school for use on its equipment.

IMPORTANT TERMS:

'Cyber-safety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

'Cyber bullying' is bullying that uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person.

'School and preschool ICT' refers to the school's or preschool's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

'ICT equipment/devices' includes computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies.

'Inappropriate material' means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

'E-crime' occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.