Security and Storage

During the school day when the devices are not being used (e.g. at lunchtime, during PE etc), they should be kept either with the student or securely stored. If the student is unable to keep the laptop with them, it may be stored in a laptop locker. Shared laptop lockers are available in the library and also provide recharging.
The laptop must be properly powered off prior to storage to preserve battery life and to prevent heat build-up.
Every care should be taken if devices are stored in student school bags to prevent malicious or accidental damage.

Power Issues/Battery/Charging

It is each student's responsibility to bring their devices fully charged for each school day. Classrooms have no facilities to recharge devices.
Devices cannot be charged at school due to the Work Health and Safety regulations, however, the School, has secure laptop storage lockers located in the 7-12 Campus Resource Centre. These lockers have built in power sources and devices can be charged during lunch and recess or other times when the device is not needed.

Backup and Data Storage

It is important to keep backups of student work. There are number of options students should consider.
Work can be stored to the student's network drive. (U:) or to a USB device, a portable USB hard drive or to a CD. It is the student's responsibility to ensure that they regularly create backups in case the laptop requires re-imaging.
The school cannot be held responsible for lost work due to a failure to do backups.

Printing

At school you will be able to select a printer to use through the BYOD Virtual Desktop. Your supplier can give advice on how to install your home printer to your device.

Vision and Rationale

Eastern Fleurieu School has a strong focus on Information and Communication Technology (ICT) literacies that will enable students to be successful global citizens in the 21st century. ICT is a significant feature in the school's strategic plan and the school has invested heavily to support this vision. Many schools around the country have implemented a "Bring Your Own Device" (BYOD) system to meet the increasing demand of ICT in the classroom. In 2015 the BYOD initiative was introduced to Eastern Fleurieu as we believe that it is a sustainable way to allow students to have one-to-one access to technology.

Bring Your Own Device - BYOD

The Virtual Desktop infrastructure we have implemented allows for a wide range of operating systems and devices to be used, including laptops and tablets. The system will allow the user to access school network drives, printers and internet while at school. Students are not required to buy a device if they already own a suitable laptop or tablet. All devices must meet the minimum requirements (listed overleaf). Guidelines for participation are:

- Parents will need to sign a BYOD Agreement Form agreeing to the terms and conditions of the program.
- A minimal cost, covering licensing and network expenses of $33.00 (inc GST) per year must be paid before the device will be connected to the School network.
- The device must be available, with enough charge in the battery, for use at school each day.
- It is advised that devices be carried in a protective cover when not in use.

If you wish to buy a device, you may purchase from a vendor of your choice. We have connections with two online suppliers who have 'parent portals' for purchasing devices (listed overleaf) for your convenience.

Parent Online Purchasing Portals: devices can be purchased by credit card, PayPal or interest free finance (subject to approval):

IP Partners – Acer and other devices:
http://efs.ippartners.com.au

LeetGeek–Apple devices:
https://shop.leetgeek.com.au/easternfleurieu/

DEVICE SPECIFICATIONS

As there are many models of computers and devices available but as a guide the School recommends the device you purchase should have the following specifications as a **minimum**:

Tablet:

	Windows:	Android	iPad: Mini & 4th Gen
Processor:	Intel Atom Z3740 (1.33 GHz)		
Memory:	2 GB DDR3	2 GB	16GB – 128GB
Storage:	64 GB Solid state	16GB – 128GB	
Screen:	8" or 10" & 10 finger touchs	8" or 10" resistive touch	7" or 10" touch
Wireless:	a/b/g/N - 2.4 & 5 GHz	a/b/g/N - 2.4 & 5 GHz	a/b/g/N - 2.4 & 5 GHz
Usb:	1 x Micro of full size Port	1 x Micro of full size Port	
HDMI:	Micro or full size	Micro or full size	
Sound:	Headphone/Microphone jack	Headphone/Microphone jack	
SD:	Micro SD slot	Micro SD slot	
Battery:	8 hour	8 hour	8 hour
Price Guide:	**$350 - $900**	**$300 - $900**	**$350 - $920**

Notebooks/Laptops:

	Windows:	MacBook:
Processor:	Core i3, i5, i7 (1.5GHz or better)	Core i5 (1.5GHz or better)
Memory:	2 GB DDR3 or better	4 GB DDR3
Storage:	320GB 5400rpm or better (could be solid state)	128GB – 512GB Solid state
Screen:	11.6", 14", 15.6" WXGA Wide Screen (could be touch)	11", 13", 15" WXGA Wide Screen
Network:	Gigabit (RJ45)	Gigabit (RJ45)
Wireless:	a/b/g/N - 2.4 & 5 GHz	a/b/g/N - 2.4 & 5 GHz
Usb:	USB 2.0 & USB 3.0	
HDMI:	Micro or full size	Micro or full size - Proprietary
Sound:	Headphone/Microphone jack	Headphone/Microphone jack
SD:	SD Card reader	
Battery:	6 hour or better	6 hour or better
Price Guide:	**$550 - $1500**	**$1050 - $2500**

INAPPROPRIATE COMPUTER USE

The Network Managers maintain computers and networks so that they operate effectively, ensuring that the resources needed are available, and that the screen interface operates in a consistent way.
The following guidelines are outlined to ensure all users are able to access the latest research available with the latest technology in an acceptable and safe learning environment.

- Users will avoid sites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way.
- Engaging in chat lines or downloading files is not permitted unless forming part of a legitimate class activity guided by the teacher of that class.
- The Federal Communications Act determines guidelines for appropriate use. Inappropriate use of the internet and email is a serious matter and can have significant consequences, *eg* sending a message over the internet using someone else's name.
- Passwords should remain confidential. No users should allow their passwords to be used by any others.
- It is the responsibility of students to maintain sufficient credit in their Internet and printing accounts to allow subject related tasks to be done in class.
- Do not remove files or folders that have been installed to the hard disk or network.
- Do not use inappropriate or offensive names for files or folders.
- Do not bring to school, or use, games or any other materials which may be offensive to others or cause distractions to learning.
- Do not engage in cyber bulling or e-crime.
- No laptop (or mobile phones) with camera capabilities are to be used in change rooms or toilets.
- Under privacy legislation it is an offence to take photographs of individuals without their expressed permission and place these images on the Internet or in the public forum.

Consequences

Any form of cyber bullying or e-crime will be dealt with through the school's "Harassment Policy" and "Acceptable Computer Use Policy". Serious breaches are a police matter and will be dealt with through State & Federal laws and SA police.

VIRUS PROTECTION

Every device connected to the Eastern Fleurieu School network must have virus protection installed. Anti-virus software (Microsoft Forefront Endpoint Protection) and monitoring software will be supplied on the laptop if required. If a student laptop attempts to connect to the school network and is found to have a virus the laptop will automatically be 'cleaned'. Students should ensure that anti-virus software is kept up-to-date on their devices and regularly check for viruses.

NETWORKS AND NETWORK SECURITY

- **The use of network games is banned!**
- **Ad-hoc networks:** Ad-hoc networks (the creation of a standalone wireless network between two or more devices) are strictly forbidden while at school.
- **Wired networks:** Students are forbidden to plug any device into the school's wired network.
- **Hacking:** Hacking is a criminal offence under the Cyber Crime Act (2001). Any hacking attempts will be forwarded to the police.
- **Packet Sniffing:** Any type of software or hardware device designed to capture or view network data\packets is forbidden.
- **Proxy Servers:** The use of an on-line proxy to bypass servers are attempt to over-ride the school internet filtering system.

The school's network security system will scan for and report on any devices attempting any of these actions. Students responsible will face disciplinary action potentially including suspension.

Private 3G or 4G services: Students using their own 3G or 4G connection will not be filtered through the school network. The content and use of these devices remains the sole responsibility of the parents or guardians. Eastern Fleurieu School does not encourage or condone the use of 3G or 4G connected devices. It is preferable for the safety and wellbeing of the student that the device is filtered through the school network.

TERMS AND CONDITIONS

SUPERVISION AND MONITORING

Internet filtering is a requirement of all public schools. All network access must be filtered regardless of the device you use to access it while in a public school. Our school and network administrators and their authorized employees monitor the use of information technology resources to help ensure that users are secure and in conformity with this policy. Administrators reserve the right to examine, use and disclose any data found on a student's device or the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement. Eastern Fleurieu School reserves the right to determine which uses constitute acceptable use and to limit access to such uses.

LOSS AND DAMAGE POLICY

Like any other personal items, students bring their BYOD devices to school at their own risk. Eastern Fleurieu School will not be held responsible for any damage, loss and damage due to fire, theft at any time.

In the event of loss, theft or damage, students are to contact their Year Level Leader. Some devices have a device locator; it is recommended that you enable this feature if possible. It is always a good idea to record the device's serial number to have in case of loss or theft.

We recommend your device is insured (often offered by vendors at purchase, via third parties or through home and contents insurance).

If a laptop is damaged, lost or found, it must be reported immediately to the ICT Helpdesk

- The school is not responsible for the loss of a device from any location on or off school grounds.
- It is the user's responsibility to report lost or stolen devices to the nearest police station.

Technical Support

The school only offers support on the the Virtual Desktop Client and the VD environment only. Software loaded onto the computer is the responsibility of the owner.

Software, Copyright and Intellectual Property

Each device will be loaded with Eastern Fleurieu School Virtual Desktop Client and configured for use on the school network. Any software installed by the school is licensed and must not be distributed or deleted without written permission from the school. We recommend having at least two updated web browsers on your device and recommend: Internet Explorer, Safari, Google Chrome, Firefox.

The installation of non-school applications and files is permitted provided that the content:

- Is appropriately licensed
- Does not breach copyright/ intellectual property laws (including video and music)
- Is ethically, morally and legally acceptable
- Does not affect the efficient functioning of the device for educational purposes
- Does not affect the school's wireless network.
- Does not interfere with the learning program.

Where there is a contravention of this policy sanctions may be imposed as appropriate and determined in consultation with the ICT Coordinator, Network Manager and the Year Level Leaders and if necessary the Principal according to the school behaviour management guidelines.

Internet Usage

Students can access the Internet through the school's ICT network while on site.
All Internet activity through the school's network is monitored and subject to filtering. Internet access must be for educational purposes only whilst at school.
Students may set up the laptop to access the Internet for their personal use at home through their Internet Service Provider. (Consult your ISP for how to do this.)
However, students are reminded that inappropriate downloads can be detected when any devices are connected to the school's network.
Students receive instruction on Cyber-Safety and topics such as

- Personal information security.
- Plagiarism, Copyright and referencing.
- Cyber bullying and libel.
- Unlawful computer / internet use.

These topics are outlined in the student diary and detailed in the EFS Computer Users agreement.

User Password and Security

Each student is required to have an individual password for logging in to the school network. This password must not be divulged to any other party under any circumstance. Sanctions will be taken against any sharing of passwords.
Any attempt to break into a government computer system is a federal offence carrying strict penalties which are also applicable to minors.
Our network audit logs contain information on the user logging in, the computer which is attempting to log in and various other parameters. This information can, and will, be used to track user access and usage. Unlawful access will be recorded and referred to the police.