Managing and Caring for your Laptop

Henley High School has a 1:1 laptop program based on a recommended device that meets the needs of all curriculum learning areas and is suitable for the demands of secondary education and the school's technology environment.

POWER ISSUES/BATTERY/CHARGING

New technology gives much longer life to modern batteries in computers. The school recommended device has a battery which will last the entire school day although this is highly dependent on power settings and how the laptops are used. It comes with intelligent battery management technology designed to improve battery efficiency and extend battery lifespan through smart charging and real-time power management.

The battery needs to be conditioned to ensure a long life. The laptop battery should be run down before recharging. It should then be fully charged overnight. The laptop battery will perform better if it is not plugged in and unplugged from the charger for short periods as that counts as a charging cycle.

It is the student's responsibility to bring a fully charged laptop to school each day. Students will not be permitted to charge laptops in classrooms, however, there are charging lockers available for use in emergencies.

IDENTIFYING YOUR LAPTOP

It is recommended that students put a name label on their laptop and that they do not remove the barcode label on the bottom of the laptop as this is what we use at the school to identify the owner of the laptop.

BACKUP AND DATA STORAGE

It is important to keep backups of student work.

OneDrive Online Storage is the recommended option and folders should be set up in an organised fashion for ease of use.

Files can also be regularly backed up to a USB device or a portable USB hard drive. The school will not be responsible for lost work.

FAULTY DEVICES AND REPAIRS

Technical Support

If the computer has a fault then it should be taken to the IT Services Helpdesk where the fault will be assessed and dealt with accordingly.

If a laptop needs repair, a “Hot Swap” loan laptop will be provided while the machine is being repaired. The loan laptops are for daily use only and need to be returned at the end of each day. You will be charged $100 for warranty repairs. This is required to be paid prior to the laptop being collected when fixed. The warranty will be voided if laptops are taken outside the school to repair.

For significant performance issues a factory reset may be necessary. However, the reset process will completely reset a laptop to original settings and delete all personal files. Important files must be backed up before a factory reset.

LOSS AND DAMAGE POLICY

Parents are advised to add the laptop to their household insurance policy as the school does not provide comprehensive insurance on laptops. There is however an accidental damage policy which is active for the laptops 3 year warranty period and covers accidental breakages.

Students should ensure that every effort is undertaken to look after and protect their laptops. In the event that a laptop is damaged, it needs to be brought to the IT Services Helpdesk for assessment.

An incident report form will be emailed home to be completed and signed by the parent or caregivers with details of how the damage occurred so the unit can be submitted for an accidental damage claim. Currently the excess cost is $100. This cost is subject to change without notification.

If a laptop is lost, it must be reported immediately to IT Services Helpdesk. The school does not take any responsibility for lost laptops. It’s suggested that any lost or stolen laptop is reported to the police.

SOFTWARE INSTALLATION

Although the laptop is owned by the family, installing programs or changing settings is strongly discouraged as making changes will impact on the performance of the machine. Students do so at their own risk.

Peer to peer software, torrenting programs or the use of VPNs or any other proxy bypass programs are prohibited and will be dealt with inline with school and department behaviour management processes. These practices can create a high risk of virus infections, malware and changed computer settings.

WHAT DO I DO IF MY LAPTOP IS FAULTY OR DAMAGED?



1. Laptop not working properly or is damaged?

   Have you tried restarting it first?

2. Student to take the laptop to IT Services

   Do not take it to outside repairers as this will void the warranty.

3. IT Services technicians inspect, assess and document the fault/damage

   If there is serious damage (eg a cracked screen), an Incident Report will need to be completed by the student.

4. If the issue is determined to be product failure following a manufacturer's evaluation, the laptop will be repaired under warranty.

5. If the damage is due to accident/ negligence:

   1. House Leader meets with the student to discuss the circumstances of the damage.
   2. Any behavioural issues will be dealt with and parents will be advised.
   3. Repairs will commence once incident form is signed and returned.
   4. Commitment to pay signed by parent for $100.
   5. Invoice for the repairs is sent to parents.

6. Student is issued with a daily loan laptop until such time as the laptop is repaired.

7. Laptop is fixed, invoice paid and returned to the student.

SECURITY AND PROTECTION

Virus Protection

Anti-virus software and monitoring software will be loaded onto the device through the initial imaging process. Updates of this software may be scheduled at various times.

If a student machine 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. As students have the right to personally use their laptops, and connect to any other network, they need to take all steps to protect the laptop from virus attacks.

Viruses can enter laptops through:

- Removable media such as USB memory sticks and External Hard Drives
- Emails
- The internet (including websites, FTP programs and social media platforms)
- Installation of software

Do not open any files or links attached to suspicious or unknown emails. Exercise caution when downloading files from the Internet. Delete chain and junk emails. Do not forward or reply to any Spam. Hundreds of viruses are discovered each month. Do not turn off automatic updates to ensure virus protection software is kept up to date.

Networks and Network Security

The school's internet connection is filtered so that students operate in a safe environment. There will not be specific filters installed on the laptop so access at home will be under parent's supervision.

Hacking

Hacking is a criminal offence under the Cyber Crime Act (2001). Any hacking attempts will be forwarded to the police. Any attempt to break into a government computer system is a Federal Offence carrying strict penalties which are also applicable to minors.

Any type of software or hardware device designed to capture or view network data\packets is forbidden. Any student detected capturing network traffic will be dealt with through the school and department behaviour management processes. The school's network security system will scan for and report on any device capturing packets.

Users and Security

Each student will be required to have an individual password for logging in to the school network. This password should not be divulged to any other party under any circumstance.

Our network logs information on the user logging in and the computer which is attempting to log in to. This information can, and will, be used to track user access and usage.

SOFTWARE, COPYRIGHT AND INTELLECTUAL PROPERTY

Each device will be loaded with a Henley High School approved software image configured for use on the school network. The image will contain operating system software, anti-virus software, standard Microsoft software and software relevant to each teaching area.

Software installed by the school is copyright and must not be distributed or deleted without written permission from the school. The parent will need to sign off on a software use agreement when issued with the laptop. Students may add their own private software as required. This software must be legally purchased with a user licence and must not interfere with the running of the machine. The software must not be malicious or offensive or breach copyright laws.

Software that is installed by the user must:

- Be ethically and morally acceptable (including consideration of school appropriateness, age-appropriate ratings and privacy issues)
- Not affect the efficient functioning of the laptops for educational purposes (ie they do not interfere with the speed and storage capacity of the laptop or the problems that might arise from increased battery use)
- Not affect the school's wireless network
- Not interfere with the learning program (ie they may only be used in class under specific teacher direction)

Given the computer is for school use, all installed games need to be PG rating. Playing games or videos during school time will impact on battery performance negatively. It is the student's responsibility for proper battery management.

CYBER SAFETY CYBER BULLYING

Technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways. Cyberbullying is bullying which uses technology as a means of victimising others. It is the use of an internet service or mobile technologies – such as email, chat room discussion groups, instant messaging, web pages 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.

Consequences

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