THE NORWOOD MORIALTA HIGH SCHOOL

2014

Laptop Program

Code of Conduct
# Table of Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT Plan: Vision and Rationale</td>
<td>4</td>
</tr>
<tr>
<td>Device Image</td>
<td>4</td>
</tr>
<tr>
<td>2014 BYOT Laptop Options</td>
<td>4</td>
</tr>
<tr>
<td>Guidelines for Participation</td>
<td>5</td>
</tr>
<tr>
<td>Lost or Stolen Procedure</td>
<td>6</td>
</tr>
<tr>
<td>Faulty Devices</td>
<td>6</td>
</tr>
<tr>
<td>Software, Copyright and Intellectual Property</td>
<td>6</td>
</tr>
<tr>
<td>Internet Usage</td>
<td>7</td>
</tr>
<tr>
<td>User Security</td>
<td>7</td>
</tr>
<tr>
<td>Virus Protection</td>
<td>8</td>
</tr>
<tr>
<td>Non-school Applications and Files</td>
<td>8</td>
</tr>
<tr>
<td>Games, Music</td>
<td>8</td>
</tr>
<tr>
<td>Web 2.0 Applications</td>
<td>9</td>
</tr>
<tr>
<td>Inappropriate Use</td>
<td>9</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>10</td>
</tr>
<tr>
<td>Networks and Network Security</td>
<td>11</td>
</tr>
<tr>
<td>Security / Storage</td>
<td>11</td>
</tr>
<tr>
<td>Backup and Data Storage</td>
<td>11</td>
</tr>
<tr>
<td>Printing and Scanning</td>
<td>11</td>
</tr>
<tr>
<td>Power Issues</td>
<td>11</td>
</tr>
<tr>
<td>Caring for your Laptop</td>
<td>12</td>
</tr>
<tr>
<td>Special Conditions for Loan Laptops</td>
<td>13</td>
</tr>
<tr>
<td>DER Funded Laptops</td>
<td>13</td>
</tr>
<tr>
<td>Anywhere Anytime Laptop Scheme (AALS)</td>
<td>14</td>
</tr>
<tr>
<td>ACER through Learning with Technologies (LWT)</td>
<td>14</td>
</tr>
</tbody>
</table>
ICT Plan: Vision and Rationale

The Norwood Morialta High School has a strong focus on cultural and linguistic diversity, internationalism, academic achievement and quality learning to meet the needs of individual students. Our vision is to provide an educational environment in which students develop high level skills and abilities, including in ICT literacies that will enable them to be successful in the 21st Century.

To remain a provider of quality, internationally recognised education, the school has developed a comprehensive 3-Year ICT Plan based on the e-Strategy framework.

Our ICT Plan includes an expectation that all students have a 24/7 to school resources through a laptop program.

We expect that all staff and students will be involved in the 1:1 Laptop Program and using our eLearning environment for centralised management of learning resources and student files, which can be accessed seamlessly from school or home, and engaging in meaningful teaching and learning using a range of digital literacies, including Web 2.0 technologies.

Device Image – (DER, AALS, LWT Laptops)

- Each device will be set up with the standard school image and registered in the school laptop database with a unique identifier against the student’s ID.
- This image includes tracking software installed on its firmware to assist in tracking the device in the event of theft.
- Each device will be encoded with a BIOS password which prevents the user from changing the Operating System as part of the school’s security processes.

2014 BYOT - Laptop Options

Option 1 will include:
- Purchase a supported laptop through the school’s negotiated vendor.
  - This option includes an annual subscription to the Microsoft Office and access to Adobe suite.
- The benefits of this option are:
  - 3 year accidental warranty
  - On-site repair (hot swaps available).
  - At least an 8 hour battery life.
- Benefits of these devices:
  - All devices on offer are designed to allow students to produce as well as consume.
  - These are all Windows 8 based devices allowing compatibility with most home and business technologies.
  - Most of these devices also allow the use of the swipe technology used in iPads without the limitations of iPads; eg use of Flash Animations, Silverlight and other software used in the school curriculum.
  - They also have the flexibility of USB ports for data transfer.
- The devices available through this option are detailed on our website.
Option 2:

- **Purchase your own personally selected laptop that meets NMHS educational requirements.** Your own personally selected laptop will only have access to the NMHS network if it meets these requirements.
  - This means it must be able to emulate Windows in order to use software used in the school curriculum including Flash Animations (Adobe Suite), Silverlight etc.
  - You will also need to purchase licences for:
    - Microsoft Office Suite
    - Adobe Suite
  - You may wish to consider purchasing accidental damage cover and extended warranty for your device.
  - Your device must have an 8 hour battery life.
  - You will be unable to recharge at school as your device has not undergone an electrical testing process required by DECD.

- **The benefits of this option are:**
  - You will be able to choose a device which suits your student’s needs and interests.

- **Please beware that:**
  - Because this is not under a service agreement our ICT staff will be unable to assist with issues that are not related to our school network access.
  - Because there is no accidental warranty you will be responsible for organising and paying for the costs of repair or replacement.
  - You will be unable to connect to the school’s network until your device has been approved by the ICT Network Manager.

Option 3:

- **Borrow a NMHS loan laptop.**
  - Please beware that these laptops are more basic devices that are heavier and without a solid state drive which is more susceptible to ‘bump’ damage and consequent data loss.

**Guidelines for Participation**

Prior to devices being issued to students:

- Parents and students will need to sign the appropriate Laptop Agreement form agreeing to the terms and conditions of the program.
- Parents and students will need to ensure that they are familiar with the Laptop Program Code of Conduct prior to signing the agreement form.

After devices are issued to students:

- Laptops are to be carried in a laptop specific carry case and treated with appropriate care.
Lost or Stolen Procedure

If a laptop is lost or stolen:
1. It must be reported immediately to the Police and a Police Report Number obtained
2. The school must be notified in person to the ICT Service Desk (if out of hours, a message can be left on the answering machine).

In the event that you own the laptop you will need to follow your own personal insurance policy guidelines.

If a laptop is found it must be returned immediately to the ICT Service Desk where the relevant student will be identified.

In the circumstance that a laptop is lost or stolen, a ‘loaner’ laptop can be organised from the ICT Service Desk.

Faulty Devices

In the circumstance that a laptop is faulty and either owned by the school or has been purchased through a school approved vendor:

- The device needs to be taken to the ICT Service Desk for investigation
- A hot-swap laptop may be issued while the faulty device is being repaired.

Software, Copyright and Intellectual Property

Each device will be loaded with a Norwood Morialta High School approved software image configured for use on the school network.

The image will contain operating system software, anti-virus software and standard Microsoft and Adobe software. For 2014 Laptops as part of the BYOT scheme the Adobe Software will be delivered through virtualisation.

Software installed by the school is the property of the Minister of Education and as such is licensed for use on school devices only. It must not be distributed or deleted without written permission from the school.

Downloading Additional Software

Not all software available is compatible with the school laptops and network. Software that has been requested by staff and is compatible has been placed on the NMHS Moodle. It is also available via an icon on the device desktop.

Students will be able to view available software by clicking on the approved programs icon on their laptop. Students will be responsible for ensuring that they have downloaded any additional software required for their subjects and year level. In the event of software fault, students can also re-install the required software from this area or see the ICT staff for assistance.
In some circumstances, the downloading of software that has not been checked for compatibility may be blocked. If you wish to download this software, contact the ICT Service Desk for assistance.

**Internet Usage**

**Usage**

Access to the Internet through the school’s network whilst at school will be monitored.

Students may also use the Internet for their personal use at home after setting up the device to access it through their home Internet Service Provider. (Consult your ISP for processes to do this.) However, students are reminded that inappropriate downloads can be detected when the devices are connected to the school’s network.

Students will receive information on safe Internet usage and responsible digital citizenship.

**Cost**

Wireless access to the school network will incur no cost when used at the school.

Wireless access to the school network when accessed from home will incur a cost through your home ISP.

Internet access to sites outside of the school network whilst at school will incur a cost, as per the current policy. Students receive an internet allowance each term. Additional credits can be purchased.

Please refer to the schools Network and Internet Policy in the school diary for further information.

**User Security**

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

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. Any unauthorised access will be dealt with accordingly.

Attempting to break into a government computer system is a federal offence and serious breaches will be referred to the Police.
Virus Protection

Anti-virus software and monitoring software will be loaded onto the device through the initial imaging process. Updates of this software will occur regularly.

If a student machine attempts to connect to the school network and is found to have a virus, or the anti-virus software is not up to date, the connection will fail. The laptop will automatically receive the latest anti-virus protection files and be ‘cleaned’.

Students should ensure that anti-virus software is kept up-to-date on their devices and regularly check for viruses. This can be done at no cost at the school.

As students have the right to personally use their laptops, and connect to the Internet from home, they need to take all steps to protect the laptop from virus attacks.

Viruses can enter laptops through:

- Removable media such as CDs, DVDs, 3G devices and USB memory sticks
- Emails
- The Internet (including web browsing, FTP programs and chat rooms)

TIPS

- Do not open any files 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 viruses are discovered each month. Run your virus scan regularly

Non-school Applications and Files

Games / Music

The Norwood Morialta High School does not object to the installation of non-school applications and files on the school laptops in principle, provided that the installed applications and files:

- Are appropriately licensed (i.e. they do not breach copyright and intellectual property laws – this includes video and music downloads)
- Are ethically and morally acceptable (including consideration of school appropriateness, age appropriate ratings and privacy issues)
- Do not affect the efficient functioning of the laptops for educational purposes (i.e. they do not interfere with the speed and storage capacity of the laptop or the problems that might arise from increased battery use)
- Do not affect the school’s wireless network
- Do not interfere with the learning program (i.e. they may only be used in class under specific teacher direction)
In particular, while some games have significant educational benefits and will be included in the software available from the school network, other games have little educational merit and may affect network function. As a result:

- The use of network games is banned whilst at school.
- No ad-hoc networks are to be formed whilst at school.

Where there is a contravention of this code of conduct, consequences may include re-imaging the device which will result in the loss of data if back-ups have not been carried out effectively.

**Web 2.0 Applications**

There are significant educational benefits for some Web 2.0 applications. However, many Web 2.0 applications can be unproductive and distracting to student learning.

Educational Web 2.0 technologies will be used as part of a student’s study in various classes.

Decisions concerning the addition of further Web 2.0 applications are based on the policy 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.

**Inappropriate Use**

The ICT Support Team maintains 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 online chat 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 another student’s name.
- Passwords should remain confidential. No user should log-on another student using their password.
- It is the responsibility of students to maintain sufficient credit in their Internet and printing accounts to allow subject related tasks to be carried out.
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.
Do not engage in cyber bullying or e-crime, including intimidating and threatening behaviour.
Do not impersonate by using another person’s online profile when using social networking.
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 images or make audio recordings of individuals without their expressed permission and place these images on the Internet or in the public forum. This can constitute cyber bullying.
Users are reminded that any media files on the laptop are accessible to the school administrative systems.
Users are also reminded that any filed uploaded to the Internet should be regarded as “public” (even if the files are subsequently deleted!)

**NB: Please refer to the DECD Social Media Policy and Guidelines. These can be found at www.decd.sa.gov.au/socialmedia**

**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 groups, instant messaging, WebPages or SMS (text messaging)- with the intention of harming another person.

**Examples** can include communications that seek to intimidate, control, manipulate, 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.

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 “Harassment Policy” and “Internet & Computer network Policy”. Serious breaches are a police matter and will be dealt with through State and Federal laws and SA police.
Networks and Network Security

Wired networks: Students are forbidden to plug any device into the school’s wired network. Any student caught with a device plugged into the schools wired network will receive an immediate suspension. The school’s network security system will scan for and report on any non school devices plugged into the schools wired network.

Any type of software or hardware device designed to capture or view network data/packets is forbidden. The school’s network security system will scan for and report on any device capturing packets. Any student detected capturing network traffic will be suspended.

Hacking is a criminal offence and any serious hacking attempts will be forwarded to the police.

Security / Storage

During the school day when the devices are not being used (e.g. at lunchtime, during PE etc), the devices should be kept either with the student or securely stored in their locker.

The device must be properly powered off prior to storage to preserve battery life and to prevent heat build-up.

Backup and Data Storage

Critical student work will be regularly backed-up on the school, providing the student has sent a copy of the critical work to their Home drive. Students who do not choose this option and save instead to an external device (hard drive or USB) or to the local machine are responsible for ensuring adequate backup of their work. This means ensuring that the work is saved to at least two external storage devices (external hard drive or USB). If you cannot see your drive please see the ICT staff for assistance.

Printing and Scanning

There are a number of devices available at school for printing and scanning. Printing can occur wirelessly from laptops. Your printing quota will be available to view and monitor.

Power Issues

Each of the school approved laptops have a long battery life which is expected the school day, providing they are fully charged and that sensible energy conservation settings are used.

Students must come to school with their laptops fully charged each day.
Caring for your Laptop

Packing away your laptop

Your laptop comes in a protective sleeve or bag
- Always store your laptop in the sleeve or bag.
- The AC adapter (power cord) does not fit in the sleeve and must be left at home for overnight re-charging.
- You still need to be careful with the laptop while it is in the sleeve or bag. Do not drop the bag from your shoulder.
- Be careful when putting the laptop in the car or bus that no other items are on top of it and nothing will roll on to the laptop sleeve or bag.
- Laptops should be switched off before closing the sleeve or bag, not just put into sleep mode.

Operating conditions

- Please do not place objects on top of your laptop
- Before switching it on, gently place your laptop on a stable surface and then switch it on.
- Do not place the laptop on a soft surface (eg bed, lap, blanket) during use as this may cause overheating
- Avoid exposing your laptop to
  - Direct sunlight or sources of heat such as desk lamps
  - Dust, dirt, rain, liquids or moisture
  - Heavy shock or vibration

LCD Screens

The most common damage to the current fleet of laptops has been damage to the screen. LCD screens are delicate – they don’t like being poked, prodded, pushed or slammed.
- Never pick up or open your laptop by its screen.
- Don’t slam the screen closed and always be gentle when putting your laptop down.

To clean your LCD screen:

- Switch off your laptop
- Use a non-abrasive cloth (or a LCD screen wipe) and gently wipe the screen in a circular motion
- Do not directly apply water or cleaner to the screen
- Avoid applying pressure to the screen

AC Adaptor

- Connect your adapter only to your laptop
- Do not step on your power cord or place heavy objects on top of it. Keep your cord away from heavy traffic areas
- When unplugging the power cord, pull on the plug itself, rather than the cord
- Do not wrap your cord too tightly around the adapter box
Keyboard

- Gently brush your keyboard with a clean soft bristled paint brush or similar to remove dirt
- If any key tops are missing or keys are in a damaged state, take your laptop to the ICT Service Desk to be repaired.

Casing Cleaning

- Using a non-abrasive cloth (or LCD screen wipes) gently rub your laptop casing to remove any dirty marks
- Do not spray the laptop directly

Special Conditions for Previous Laptop Programs

Device specific information

Students are expected to participate in the 1:1 laptop environment through one of following 3 schemes:

- The DER Funded Laptops, including Loaner Laptops
- The 2012 Anytime Anywhere Laptop Scheme (AALS) and the
- 2013 Laptop Program (direct purchase of ACER through LWT)
- 2014 BYOT Program (refer to options on Page 4)

DER Funded Laptops End of Lifecycle Process

Students who are part of the DER or Loaner Laptop Scheme will be expected to return the laptop at the end of each year for stocktake and maintenance. Students who fail to return the laptop at the end of the term will be charged a holiday use fee of $50.

Students must leave the student identification labels on these machines and not alter the appearance of the laptop.

DER Funded Laptops cannot be taken overseas without the written permission of the Principal.

Students with DER Funded Devices are responsible for any damage to the device and the cost of repair. Please check your personal home contents insurance.
The 2012 Anytime Anywhere Laptop Scheme (AALS)

The Acer Laptop includes a 3 year Accidental Damage Cover. Whether this insurance applies in any particular situation will be determined by Acer, in line with the conditions of their policy as detailed below.

The ICT Service Desk must be notified immediately if a laptop is damaged. In most circumstances students will be provided a hot-swap laptop (with their existing hard drive) while their own laptop is being repaired.

Insurance does not cover vandalism or wilful damage to the laptop. If it is determined that the Accidental Damage Cover does not apply, parents will be contacted and billed for the cost of repair.

It is the responsibility of students to ensure that their laptops are stored in a secure place and to report any lost or stolen laptop (see Lost & Stolen Procedure). Loss and theft are not covered by the Acer Accidental Damage cover. Families are advised to check their household contents insurance to determine what cover they may already have, and what conditions may apply.

Please be aware that, if payments are not met as per the Agreement, then the laptop will be retrieved until payment has been made.

2013 Laptop Program (direct purchase of ACER through LWT)

The Acer Laptop includes a 3 year Accidental Damage Cover. Whether this insurance applies in any particular situation will be determined by Acer, in line with the conditions of their policy as detailed below.

The ICT Service Desk must be notified immediately if a laptop is damaged. In most circumstances students will be provided a hot-swap laptop (with their existing hard drive) while their own laptop is being repaired.

Insurance does not cover vandalism or wilful damage to the laptop. If it is determined that the Accidental Damage Cover does not apply, parents will be contacted and billed for the cost of repair.

It is the responsibility of students to ensure that their laptops are stored in a secure place and to report any lost or stolen laptop (see Lost & Stolen Procedure).

Loss and theft are not covered by the Acer Accidental Damage cover. Families are advised to check their household contents insurance to determine what cover they may already have, and what conditions may apply.

Please note that all financial matters related to laptops purchased through this scheme are between the families and the providers of this scheme.