Getting Started Information

The information below has been presented to get you started on your one-to-one laptop program journey. Please take the time to review this information at the start of every term to refresh your memory on the care & maintenance of your device and your online safety.

Help Desk Information:

If students have problems with their device they are to bring it to H4 in the library during the first 15 minutes of each recess to access the One-to-One Help Desk. If passwords need resetting, this is the time to come too. Students will not be permitted to leave classes and move around the school during lesson times.

General Care & Maintenance of your Device:

Please follow these guidelines on getting the most out of your device & looking after it appropriately –

Packing away & Handling of your Device

- Always store your device bottom down and with the LCD facing away from the front of the backpack.
- Do not wrap the cord too tightly around the power adapter or the cord will become damaged.
- Try to avoid moving your device around when it is on. Before switching on, gently place your device on a stable surface and then switch on.
- You still need to be careful with your device while it is in the bag. Do not drop the bag from your shoulder. Always place the device bag gently down. Wrap device shell in a plastic bag before leaving to go to or from school in the event of rain.
- Be careful when putting the device in the car that no other items are on top of it and nothing will roll onto the device bag.

- Devices should always be operated from within the shell whilst at school – always use the zip to open (never the velcro opening) and ensure that the elastic bands are over the bottom of the laptop and the screen corners.

Operating conditions

Please don’t place objects on top of your device and never carry it around while it is turned on.

Avoid exposing your device to:

- Direct sunlight or sources of heat such as desk lamps.
- Dust, dirt, rain, liquids or moisture
- Heavy shock or vibration
**LCD screen**

LCD screens are delicate - they don’t like being poked, prodded, pushed or slammed. Never pick up your device by its screen. Don’t slam the screen closed and always be gentle when putting your device down.

To clean your LCD screen:

- Switch off your device.
- Use a cotton cloth to gently rub the screen.
- Do not directly apply water or cleaner to the screen.
- Avoid applying pressure to the screen.

**AC Adapter**

- Connect your adapter only to your device.
- 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.

**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 device to Technicians to be repaired immediately. A single key top can easily be replaced but continuing to use the keyboard with a missing key top can result in having to replace the entire keyboard.

**Casing Cleaning**

- Take a non-abrasive cloth, spray Windex or like cleaner on to cloth to moisten, do not spray the Device directly, gently rub device.

**Behaviour Management:**

To ensure the maximum benefit of the device within the classroom and for the success of the program please note the following—

1. **10% of students will be randomly sampled to have their laptops screened each week**-
   - Any software that the student has loaded should be legal and not pirated. Students will be asked (within a one week window) to provide proof of purchase (ie receipt, original software disks, purchase email etc) to ensure that pirated software is not being installed on school equipment. Please ensure that any games etc are appropriate for the age level.

2. **Removal of the Tamper Proof Seals**-
   - The removable panels at the back of the device will have tamper proof stickers placed across them. If peeled off they change colour and it is evident that they have been tampered with. If a student alters the back panels to access the internal workings of the device the warranty will be void. If a student brings a machine to be repaired and the tamper proof stickers have been peeled, parents will be liable for repairs. These seals will be checked at the weekly random screenings as well.
Breaking of Rules Above-

- If students install pirated software onto the device it threatens the stability of the device as often illegal software can introduce viruses and other unknowns to the computer. If this occurs, the student will have their administration rights to the device removed, meaning that they will not be able to load any software to the device and will have to use it as issued.
- If students are caught playing games during class time from software loaded on to the device then they too will lose administrator rights and be unable to load software again.

Cyber Safety:

The cybersafety help button

From Tuesday, 7 December 2010, schools will notice a Cybersafety Help Button icon on the desktop of all Department of Education and Training school-based computers.

The Cybersafety Help Button is a new Australian Government initiative, supported by the Department of Education and Training, designed to keep children and families safe online. It is an online resource hub that provides instant 24 hour access to cybersafety help and information.

While the internet offers many benefits, there are also potential risks for children and teenagers such as cyberbullying, scams and fraud, offensive content and unwanted contact. The Cybersafety Help Button is a tool to help reduce these risks.

School staff and parents are encouraged to explore the new button and discuss its use with students. Students should also be encouraged to report any concerns to school staff for investigation and appropriate action. Child protection concerns must be reported through the appropriate school processes outlined in the Department's Student Protection policy.

The Cybersafety Help Button can also be downloaded on home/office computers via the Department of Broadband, Communications and the Digital Economy website. It is compatible with all major PC and Mac operating systems and is easily installed onto home, school and library computers.

The Cybersafety Help icon sits on the computer desktop. When the icon is double-clicked, the Cybersafety Help Button appears. If the button is double clicked, the users are taken directly to a web page where they can talk, report or learn about cybersafety issues.

The talk function gives a link to Kids Helpline. Users who are worried by cyberbullying or offensive online behaviour or content can phone or chat online to a professional counsellor.

The report function offers direct links to pages on social networking sites such as Facebook, MySpace and Twitter that have site-specific cybersafety information. There are also links for reporting scams, fraud, inappropriate websites and improper behaviour and for contacting the Australian Federal Police.

The learn function provides a range of cybersafety educational resources through the ACMA's Cybersmart website and the Department's Stay Smart Online website.

SYSTEM RECOVERY

STEP 1 CREATING A SYSTEM RESORATION POINT

1. Turn your computer off then on and from the boot options that display select Symantec OBR (not windows)
2. Accept Symantec Agreement
3. Will get error message that Network Adaptor Failed - click OK
4. Select Backup My Computer
5. Select NEXT
6. Check the box beside System C:\ drive then NEXT
7. Select BROWSE then double click Data (D:) then select MAKE NEW FOLDER then create folder called RECOVERY
8. Select RESTORE then click OK then click NEXT
9. Accept defaults and click NEXT
10. Click FINISH (backup will take approximately 10 minutes)

RECOVERING SYSTEM FROM RESTORATION POINT

1. Turn your computer off then on and from the boot options that display select Symantec OBR (not windows)
2. Click OK when the message window appears telling you no recovery points were found
3. Select BROWSE then double click COMPUTER then (D:) then double click folder called RECOVERY
4. Select the recover point which will be titled System_C_Drive.v2i and click OPEN
5. Select NEXT
6. Accept defaults and select NEXT
7. Tick the box REBOOT WHEN FINISHED then click FINISH
8. Click YES when the next window appears (recovery will take approximately 10 minutes)
Parents should take the time to be aware of the online movements of their child at nights. It’s easy to think that when they go to bed at night, they’re heading off to get a good 8 – 10 hours of sleep to effectively rest their brain for the following school day.

Recent research suggests that teenage students are spending more time online during the hours after 10pm – 6am than ever before. For Australian students this is simply because the best time to play games is around 2 – 5am due to the global gaming community (linked to USA game times).

Setting up a Charging Station

The best thing a parent can do to help their teen is to setup a basic rule. No electronic devices in your room when you go to bed. Easier said than done for some of you with troublesome teens I’m sure. The best thing you can do is to setup a charging station where the mobile devices need to be put after 9pm at night. Most importantly make sure you turn the devices to silent, and before your child goes to bed, simply make sure it’s not in their room. If the device isn’t in their room, they won’t hear incoming messages and will get that ever so important uninterrupted sleep.

Don’t forget in some cases your sons or daughters friends might have sent the text message at 7pm, which is more than acceptable, but it arrives via the telco network at 11pm the same night. No person can control that, and it’s certainly not your child’s fault, or their mates. Keep it simple – “Phone on Silent, put it on the charging station!” Your charging station might go more high tech than the one illustrated – might involve a lockable cupboard if required.

Electronic devices that can access online content

There are many ways in which your child can be active at night in their “online life” without your knowledge. Be aware that nearly all online devices can connect to your local network or internet. What devices are amongst the most common to connect to the internet to access inappropriate content (including pornography and pirated software – which often contains malware and viruses):

- Laptop & Desktop Computers
- Mobile Phones (iPhone, HTC, Nokia, etc)
- Gaming Consoles (xbox, wii, playstation 3, etc)
- Hand Held Gaming Consoles (Gameboy, Nintendo DS, PSP, etc)
- Hand Held Multimedia Devices (iPod Touch, iPad2, Acer Iconia)

Securing the Device via your Router

Your router (the little box that connects you to the internet in your house) has what’s called IP addresses (read more here about IPs). In your home, for any device to connect to the internet you need to get an IP address from the router. HERE is your power. If you set all your devices to permanent IP Addresses, you can tell the router what time the device has access to the internet. For example. My child has an iPod Touch. It’s 10pm and the router denies access to the device and the device no longer has internet access. It’s really that simple.

How do you create these settings? It may be a little tricky – in that case, simply get your local tech guy to come over and do it. It shouldn’t take more than 1 hour to setup your network to do this, and cost less than $150 (based on standard 2011 tech costs in Brisbane). For those who are a little more advanced you may be able to do this yourself.