Waikerie High School

WAIKERIE

SEQUERE SCIENTIAM

COMPUTER BORROWING HANDBOOK

Computer Handbook

Contents

1. Vision and Rationale 2

2. Computer Use Agreement 2

3. Student and Parent Responsibility 3

5. Early Return Policy 3

6. Appearance / Personalisation 4

7. Device Specifications 4

8. Bring Your Own Device 4

9. Guidelines for Participation 4

10. Insurance 5

11. Loss and Damage Policy 5

12. Faulty Devices 5

13. Technical Support 5

14. Software, Copyright and Intellectual Property 5

15. Internet Usage 6

16. Users and Security 7

17. Virus Protection 7

19. Networks and Network Security 7

20. Inappropriate Use 8

21. Cyber Safety 8

22. Electronic crime (e-crime) 9

23. Security and Storage 9

24. Power Issues/Battery/Charging 10

25. Backup and Data Storage 10

26. Portable USB Optical Drives 10

27. Printing 10

28. Caring for your Device 11

29. Returning a Loan Device 12

Strategies to help keep student’s Cyber-safe 13

1. Vision and Rationale

Waikerie High School has a strong focus on Information and Communication Technology (ICT) literacy's 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.

The goal is to ensure that all children have access to learn anytime and anywhere and that they have the tools that make this possible.

Waikerie High School has invested in a sustainable and meaningful change to teaching and learning in our school and to prepare students for further education and training, jobs of the future and to live and work in a digital world.

Waikerie High School will endeavour to give computing access to all students and access to the school's network through a variety of ways. This will take shape of the school providing access through sustainable means to its staff and students. Students in Year's 11 and 12 have the ability to bring their own devices (BYOD), subject to agreements set up by the school.

2. Computer Use Agreement

At School and Take Home or BYOD:

Waikerie has a flexible approach to Take Home Device, supplied by the school under certain agreements with outside agencies and within the school or by means of BYOD. To this end, Waikerie High School, has embarked on an extensive program to upgrade and increase the number of computers in school in a sustainable manner. The agreement will remain in force as long as your child is enrolled at this school.

As part of the program, Use Agreements are required to be signed by students and parents/caregivers in relation to the use of the computers at school and if on loan to be taken home. This agreement supersedes all previous signed agreements relating to computer use in schools.

When a device is taken home it is considered to be on loan from the school to the student for either a short or long term period.

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

Procurement/Disposal:

All equipment purchased by the school is the property of the South Australian Minister for Education.

At the end of the computer's life, defined as four years, Waikerie High School will dispose of the devices as per instructions set out from the Minister of Education.

All software installed on Take Home devices are owned by the Department of Education and Child Development (DECD).

Acceptable Use:

As is the case with all Information and Communication Technologies (ICTs) in DECD' schools and preschools, policies on the safe and acceptable use of ICT apply to all ICT devices.

All students and their parents/caregivers are required to sign a Use Agreement which 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 the allocated computing resource 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 of school hours or off site.

Waikerie School reserves the right to monitor the content of laptops on loan.

3. Student and Parent Responsibility

Students are expected to care for loan devices in relation to carrying, cleaning, storage and security both on and off-site. If it is BYOD, the student will take full responsibility of the device including its safe storage and bring their device at their own risk.

In some cases, parents may be responsible for the full replacement cost of the loan device, eg if the damage is wilful, not covered by the warranty, or if it is lost from an unsecured location.

If a loan 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 a device on loan for home 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.

Any replacement computer will usually be the same age and model as the one it replaces and may be pre-used by other students.

Repair and maintenance:

The school will endeavour to repair and maintain all loan devices. A third party will make a final decision if the repair was accidental or fault of the student. If it is deemed the fault of th student, an invoice for the coat of repair will be sent home to be paid in full before another device is issued.

The school is responsible for the repair (normal wear and tear) and maintenance of the computers through regular maintenance or servicing schedules. Students will be notified of such scheduling.

BYOD devices, this is at the cost of the student or parent. Waikerie High School will not under any circumstances be involved in any repairs or maintenance of the device.

Loan Devices:

Waikerie has established a small pool of replacement loan devices for students to use if an on loan device is unavailable for more than five days because it is being repaired under warranty or after being damaged. However, availability of a replacement loan device is not guaranteed nd subject to damaged caused to previous device.

5. Early Return Policy

If your child leaves before completing Year 12, any loan device must be returned to the school. As part of the return process, a maintenance check will occur to ensure that the device is in good order. Any repair or replacement costs may be passed on to the parent/caregiver for payment. School policies related to the recovery of debts will apply.

If a student leaves the school prior to the end of the school year, the computer must be returned to the school.

The device must be returned in the original condition it was when issued and personal identifications must be removed. If the device is not returned in this condition, an additional fee to repair or replace the device will apply.

6. Appearance / Personalisation

Loaned devices are the property of the school, they are not to be altered or personalised in any way that is not completely irreversible, this includes the OEM license sticker on each computer. Labels or stickers are OK but must be removable. The barcode and name on the bottom of the device should not be altered or tampered with.

If the device is not in its original condition upon its return, a cost will be incurred to bring the device back to its original state.

7. Device Specifications

It is expected that all loan devices will be of the same specification to assist in management and curriculum development. Students are not permitted to change the device specifications, make modifications or add upgrades. Note. The device warranty is void if attempts are made to change the hardware.

8. Bring Your Own Device

The use of private devices on the school's network creates issues on the management and the security of the network system. Therefore, the school's wireless network system is able to accommodate private devices for internet and printing use only. An appointment needs to be made with the schools' ICT Technician for this to take place. More details are outlined in the BYOD Use Agreement.

It should be noted that the school cannot support the maintenance of the private device and that all software needs are to be supplied by the user. Software that is not Cyber Safe or set out by the DECD ICT services cannot be used at the school. The school is not licensed to put software on private devices and this is the responsibility of the owner at their cost. We suggest you make arrangements for software with your supplier at time of purchase. A list of suggested software is available on request. Issues relating to private computers will not be the responsibility of the school, as the school will not risk the integrity of the device or its warranty.

9. Guidelines for Participation

Prior to devices being issued to students:

- Parents will need to have paid for school fees or have arranged with the finance officer to pay off the school fees over a period of time.
- Parents will need to sign a Computer Agreement Form agreeing to the terms and conditions of the program if they wish to participate in the computer scheme.
- The signed Computer Agreement form indicates that this booklet has been read by the student and the parent/s and are aware of the rules and responsibilities associated with the agreement form
- Each loan device will be imaged with the permitted school image for each and registered in the schools' database system with a unique identifier against the students' ID.
- Students will be given a further induction to ensure that they are familiar with their roles / responsibilities on pick of the computing device.
- The device must be available for use at school each day.
- Students will need to follow the schools' core values or the device may be removed.

10. Insurance

Waikerie High School will take no responsibility if the device is stolen, lost or accidentally broken. It is the sole responsibility of the student and parent to arrange insurance for the device. Where a loss or damage occurs that is not covered by parents' car or home contents insurance policies, it will be the parents' responsibility to cover the cost to replace or repair of the device.

11. Loss and Damage Policy

Parents must ensure that students report lost, stolen or damaged devices to the school's Technology Coordinator or IT Technician within 24 hours of the incident occurring.

If a device has been lost or stolen, it must be reported to the police.

If a device is damaged in any way it should be reported to the IT Technician immediately.

12. Faulty Devices

If a device is faulty, technical support is available through the IT Technician. Students will need to organise a suitable appointment time suitable with the IT Technician and not during lesson time.

13. Technical Support

Students who have loan devices and are experiencing technical and software faults should proceed according to the following steps:

- If the computer has an obvious hardware fault (screen or keyboard not working) then it should be taken to IT technician where the vendor will be contacted for support.
- If the computer has any other issues a re-image must be performed. This will be carried out by the IT Technician and an appointment time will need to be made (not during lesson time).

  Be warned: a re-image process will completely reset a laptop to its original settings.

- IMPORTANT FILES MUST BE BACKED UP BEFORE RE-IMAGING.
- If a problem still persists the vendor will be contacted.
- During the year important updates that cannot be delivered wirelessly will require the devices to be returned for work to be completed. It is expected that the student may be without their computer for up to six days per year for servicing.
- Students will be informed when updates or re-imaging are required.

14. Software, Copyright and Intellectual Property

Each loan device will be loaded with a Waikerie 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 other DECD approved software.

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 the computer use agreement policy that they understand the software copyright laws.

Students may add their own private software as required. This software must be legally purchased with a user licence. The software must not be malicious or offensive or breach copyright laws.

Non-school Applications

Waikerie High School does not object to the installation of non-school applications and files on the loan devices 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 computer for educational purposes (i.e. they do not interfere with the speed and storage capacity of the device 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).
- Meet the schools' and DECD Cyber Safety regulations.

In particular, while some games have significant educational benefits, other games have little educational merit and may affect network function. As a result:

- The use of network games is banned
- No ad-hoc networks are to be formed
- Where there is a contravention of this policy, consequences will include re-imaging the device which will result in the loss of data if back-ups have not been carried out effectively. Other sanctions may be imposed as appropriate and determined in consultation with the Technology Coordinator, IT Technician and the Leadership Team.

15. Internet Usage

Usage

Students can access the Internet through the school's network while on site. Access to the Internet through the school's network at school will be monitored and subject to strict filtering. Therefore, ad-hoc Internet is permitted at school.

Students do not need to purchase or bring personal internet devices to school, as each student has their own internet account at school and has an appropriate filtering system. Personal internet devices do not have any filtering and can cause security and other issues at the school. For that reason they are banned at school.

Students with loaned devices 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 download scan be detected when the devices are connected to the school's network.

Cost

Using the Internet and downloading data incur a cost when used at the school. This is incorporated in a combined Internet and printing allocation at the start of each year. If a student runs out of credit for Internet or printing, credits should be purchased at the book room. Students should ensure they have sufficient credit for curriculum use.

16. Users and Security

Each student will be required to have an individual password for logging in to the school's network. This password cannot 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 and in severe cases will be referred to the police.

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. Outside access will be monitored and referred to the police.

17. Virus Protection

Anti-virus software (McAfee) and monitoring software will be loaded onto the loan device through the initial imaging process. Updates of this software will be scheduled at various times. BYOD device will need to source their own. This has been outlined in the use agreement form.

If a student loan device attempts to connect to the school network and is found to have a virus the laptop will automatically be 'cleaned'.

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, floppy disks 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

19. Networks and Network Security

Ad-hock networks: Ad-hock networks (the creation of a standalone wireless network between two or more laptops) are strictly forbidden while at school. The school's network security system will scan for, remove and report on any ad-hock networks detected.

Wireless Access Points (WAP): Any students caught tampering with any wireless access point will be immediately suspended and will be invoiced for any damage caused to the device.

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.

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. Any student detected capturing network traffic will be suspended. The school's network security system will scan for and report on any device capturing packets.

20. Inappropriate Use

The Network managers maintain computers and networks so that they operate effectively, and 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.
- Use unapproved software or applications or creation of ad-hoc networks.
- 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 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.
- 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.

21. Cyber Safety

Waikerie High School is committed to being a cyber-safe learning environment. Please see the attachment *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.

Many sites have forums, chat lines, cloud storage. Although some of these sites and applications have benefits, it does pose many threats and issues to our students. It is also difficult to filter or provide safe checking protocols at school. Therefore, DECD have strict policies on allowing cloud base technologies through the filtering system without a risk assessment completed by the school. The school will determine and make a final decision depending on the risk.

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 technologies–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.

22. 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 "Harassment Policy" and "Acceptable Use of Technology Policy".

If 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.

23. Security and 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. If the student is unable to keep the device on their person, then the device needs to be 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.

24. Power Issues/Battery/Charging

Students should come to school with their computers fully charged, regardless if it is a loan device or a privately owned computer. Students cannot charge devices at school due to WHS regulations.

Battery Life

New technology gives much longer life to modern batteries in computers. The school has purchased extra long life batteries for each device. These should give 6 – 8 hours, sufficient for the school day.

Conditioning the battery

The battery needs to be conditioned to ensure a long life. The laptop battery should be completely powered down before recharging. It should then be fully charged over night. This needs to be repeated 3 times before you run the laptop from the power outlet. **RUN DOWN FULLY/RECHARGE/RUN DOWN FULLY/RECHARGE/RUNDOWN FULLY/RECHARGE**

Then it can be used connected to the power outlet if needed. This is not usually required as the laptops run effectively when fully charged.

Charging

Students should bring the laptop to school each day fully charged. Due to WHS, students are unable to charge their device at school.

Students will not be permitted to recharge laptops at school.

25. Backup and Data Storage

It is important to keep backups of critical student work. There are number of options students should consider.

Student with loan devices can have their curriculum network drive set up for synchronisation. This enables students to save their work to the curriculum network drive and when synchronised, student's can access their folder at home. When students join the network at school again, their drive will be synchronised. The advantage of this system is that the curriculum network is backed up every night on the schools server system. An instructional worksheet can be collected from the IT Technician for this set up.

Work should also be regularly backed up to a USB device or a portable USB hard drive, supplied by the student.

The school cannot be held responsible for lost work due to a failure to do backups or faulty devices.

26. Portable USB Optical Drives

The computers do not come with optical drives such as CD/DVD readers and burners.

Students are encouraged to purchase a portable USB optical drive if they require these features.

27. Printing

At school the resource centre will be the default printer. Students will also be able to select a nearby printer to use.

At home you may need to save your work to a USB storage device and print from a computer connected to a printer. You may also want to install your home printer to the laptop. You can also print to a printer with a wireless network card that is connected to your modem if you have this feature. Your supplier can give advice on how to set this up, the school is unable to support you with this.

28. Caring for your Device

You may wish to purchase a carry case for the device to help protect it in transit to reduce damage. The school does not supply these cases.

Packing away your device

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 it on, gently place your device on a stable surface and then switch it on.

You still need to be careful with the device while it is in the bag. Do not drop the bag from your shoulder. Always place the laptop bag gently down.

Be careful when putting the device in the car or bus that no other items are on top of it and nothing will roll on to the device bag

Computers should be switched off before being placed into the bag

Operating conditions

Please do not place objects on top of your device and never carry it around while it is turned on

Avoid exposing your computer to

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

LCD Screens

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
- Lightly dampen a non-abrasive cloth with water 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 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

Do not wrap your cord too tightly around the adapter box

Be aware of the power savings that come from running your device effectively from battery after being fully charged. This can amount to a significant amount per year.

29. Returning a Loan Device

The student will return the device to the resource centre and various checks will be undertaken, to make sure everything is working order and nothing is broken on the device.

If the device is damaged, not returned in its original condition, needs cleaning and removal of personal identification, parents may incur this cost to return the device back to its original condition.

Once the device is returned, the device will be re-imaged with the schools image. Therefore all data stored on the computer will be lost. All data will need to be copied or stored before its return.

Strategies to help keep student's 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 us 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 Use Agreement form and the completed form has been returned to school.
2. If I have my own user name, I will log on only with that user name. 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 schools' 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 an adult is present. I will not use ad-hoc networks due to safety issues outlined in the booklet.
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 or 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 written 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 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.

14. 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.

15. 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.

16. 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.

17. 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.

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.