

Cashmere Avenue School Cyber Safety Procedures

Reviewed: June 2011

Important terms used in this document:

- (a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies.
- (b) **'Cybersafety'** refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones
- (c) **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below
- (d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, 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, digital, webcams), all types of mobile phones, video and audio players/receivers

Cashmere Avenue School will review and maintain rigorous and effective cybersafety practices, which aim to:

- Maximise the benefits of the Internet and ICT devices/equipment to student learning;
- Minimise and manage any risks to students and staff; and
- Assist students to receive education about the safe and responsible use of present and developing information and communication technologies

Procedures

1. The school's cybersafety practices are to be based on information contained in the latest version of the *NetSafe[®] Kit for Schools*, which is endorsed by the New Zealand Ministry of Education as best practice for New Zealand schools.
2. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.
3. Cashmere Avenue School use agreements will cover all board employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school.
4. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at Cashmere Avenue School is to be limited to educational, professional development, and personal staff usage appropriate in the school environment, as defined in individual staff code of conduct agreements.
5. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.
6. The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.
7. The safety of children is of paramount concern. To avoid children encountering undesirable sites the school will run Ministry of Education approved filtering software and anti-virus programmes.
8. Limitation of Liability - Cashmere Avenue School will not be responsible for financial obligations arising through the unauthorised use of the system. Any invoices received for unauthorised transactions will be forwarded to the relevant staff member, or caregiver/s if it is children involved.
9. Any apparent breach of cybersafety will be taken seriously. In serious incidents, advice will be sought from an appropriate source, such NetSafe, the New Zealand School Trustees Association and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Student Cyber Safety Rules

1. I cannot use the school ICT equipment until my parent/s or caregiver/s have given signed permission.
2. I can only use the computers and other ICT equipment for my schoolwork and only with a staff member's permission.
3. I can only go online or use the Internet at school when a staff member gives permission and an adult is present.
4. I will not tell anyone my password or anyone else's password.
5. I will not use the Internet, email, mobile phones or any other ICT equipment to be mean, rude, or unkind about other people.
6. If I find anything that upsets me, is mean or rude, or things I know are not acceptable at our school, I will:
 - Not show others
 - Turn off the screen and
 - Get a staff member straight away
7. I will ask a staff member's permission before I put any personal information about me or other people online. Personal information includes:
 - Names
 - Addresses
 - Email address and other personal web links
 - Phone numbers
 - Photos of me or other students.
8. I will be careful and will look after all our school ICT equipment by:
 - Not being silly and playing around with it
 - Following our school cyber safety rules
 - Telling a staff member about anything wrong or damaged.
9. I must ask my teacher before uploading any files from any electronic storage device or disk that I bring from home.
10. I can only bring a mobile phone to school if I have my parent's permission. It is only to be used after school. During the school day it must be off and stay in my school bag or with the teacher.
11. I must not bring any other ICT equipment/devices to school. This includes things like iPods, games, cameras, and software.
12. I understand that if I break these rules the school may need to tell my parent/s.

Staff responsibilities include: (personal use responsibilities – see Staff code of conduct)

- To view all information and communication “posted” on the Internet (on web pages, comments or posts on blogs & wikis, in emails or on network sites) by students in their care as part of learning programmes.
- To moderate (view & approve before posting) all posts from members of the public on class or student wikis, blogs or other such sites, which they have established or developed with students.
- To only promote or recommend sites that are highly likely to be safe online environments for students.

Staff may approve the following student information being “posted” (publicly viewable) on the Internet (on web pages, comments or posts on blogs & wikis, in emails or on network sites):

- First name
- Room number
- Class email address
- School postal address and phone number
- Photos where students are not readily recognisable. Eg. Very small in size

Any information beyond this will require an informed consent from parents.

Parent(s)' responsibilities include:

- To read this cyber safety procedure. Then discuss the cyber safety rules with your child/ren, explain why they are important and encourage them to follow them.
- To return the signed student ICT Use Agreement to the school (this form is provided at enrolment and the beginning of each school year)