



Appendix 1

**STUDENT CODE OF CONDUCT FOR NETBOOKS
NETWORK LOAN CHARTER**

We are excited about the introduction of Netbooks as a valuable digital tool for learning. Our students will be expected to use the Netbooks appropriately following the conduct outlined in the Netbook Loan Charter.

Student name and surname: _____

Parent/Guardian name and surname: _____

Purpose

The school ICT initiative "Using Netbooks for e-learning" aims to improve student learning experiences both in and out of the classroom. The students may use the Netbook for a particular topic of work, school projects or need.

Ownership

The loaned Netbooks remain school property and ownership is not transferable to students. If the loaned Netbook gets damaged or lost, the student will be required to replace the Netbook.

Please note: a Netbook Loan Charter must be provided to the students and signed before the Netbook will be loaned.

Students and parents/guardians must carefully read this charter prior to signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed.

Netbook Loan Charter

I have read the Netbook Loan Charter.

I understand my responsibilities regarding the use of the digital Netbook and the Internet.

In signing below, I acknowledge that I understand and agree to the Netbook Loan Charter.

I understand that failure to comply with the Netbook Loan Charter could result in loss of future loan permission.

Signature of student: _____ Date: / /

Signature of parent/guardian: _____ Date: / /

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL

For Office use only

Netbook User Account No: _____

Netbook Registration No: _____

LOAN CHARTER

1. Purpose

The digital Netbook is to be LOANED as a tool to assist student learning both at school and at home.

2. Equipment

2.1 Ownership

2.1.1 The student must bring the Netbook fully charged to school every day if required. Chargers should be left at home.

2.1.2 The school retains ownership of the Netbook.

2.1.3 All material on the Netbook is subject to review by school staff. If there is a police request, ICS will provide access to the Netbook and personal network holdings associated with your use of the Netbook.

2.2 Damage or loss of equipment

2.2.1 All Netbooks and batteries are covered by a manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the Netbook. It does not cover negligence, abuse or malicious damage.

2.2.2 Any problems, vandalism, damage, loss or theft of the Netbook must be reported immediately to the school.

2.2.3 In the case of suspected theft, a police report must be made by the family and an event number provided to the school.

2.2.4 In the case of loss or accidental damage, a parent/guardian should write and sign a statement about how it happened.

2.2.5 Netbooks that are damaged or lost by neglect, abuse or malicious act, may need to be paid for. The Director of ICT will determine whether replacement is appropriate and/or whether or not the student is responsible for repair or replacement costs and whether or not the student retains access to Netbook loans.

2.2.6 Students will be required to replace lost or damaged chargers.

3. Standards for digital Netbook care

The student is responsible for:

- i) Taking care of Netbooks in accordance with school guidelines.
- ii) Backing up all data securely. This should be on a memory stick, online storage or on other external storage device. Students must be aware that the contents of the Netbooks may be deleted and the storage media reformatted in the course of repairs.
- iii) Never damaging or disabling digital Netbooks, Netbook systems and networks or establishing, participating in or circulating content that attempts to undermine or bypass Netbook security mechanisms for either software or hardware.

4. Acceptable computer and Internet use

Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

4.1 Access and Security

4.1.1 Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- ensure that communication through Internet and online communication services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their computer or network account.
- log off at the end of each session to ensure that nobody else can use their computer or network account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- Immediately report to supervising adult (teacher/parent/guardian) if another online user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
 - a message that was sent to them in confidence
 - a computer virus or attachment that is capable of damaging recipients' computers
 - chain letters and hoax emails
 - spam, e.g. unsolicited advertising material.
- never send or publish:
 - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
 - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
 - sexually explicit or sexually suggestive material or correspondence.
 - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and Internet and online communication services are generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks of ICS.
- ensure that services are not used for unauthorised commercial activities, online gambling or any unlawful purpose.
- be aware that all use of Internet and online communication services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

4.2.1 Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs,

- credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.3 Intellectual Property and Copyright

4.3.1 Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the Internet or Intranet has the approval of their teacher and has appropriate copyright clearance.

4.4 Misuse and Breaches of Acceptable Usage

4.4.1 Students will be aware that:

- they are held responsible for their actions while using Internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access Internet and online communication services.
- the misuse of Internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, evaluation and reporting requirements

5.1 Students will report:

5.1.1 any Internet site accessed that is considered inappropriate.

5.1.2 any suspected technical security breach involving users from other schools or other organisations.

Updated: December 2010

Review Date: December 2011