APPENDIX A GUIDELINES

A.1 RESPONSIBLE USE OF ONLINE SERVICES

The agreements and forms provided in the appendices provide examples of the type of document that can be used to obtain agreement and sign-off from students and parents or responsible persons. These forms do not constitute or contain legal disclaimers but they do help to meet the requirement to make students and parents aware of their obligations and the risks associated with online services use. Similarly the *logon reminder text* in the appendix is provided as an example of the type of information window that schools may find useful to have automatically displayed to all users when logging in to the school network.

Schools may wish to periodically repeat requests for sign-off (e.g. at the start of the school year) on the agreements by students and parents as a means of reminding them of their responsibilities when using the Department's information and communication technologies.

Monitoring and tracking online activity across the Department's network is a complex and expensive activity, resulting in the creation of extremely large system event log files which are difficult to store and use. It is important therefore to realise that it will not always be possible for ICT staff to trace online activity or to provide comprehensive historical details of individual online activity.

A.1.1 ACCEPTABLE USAGE AGREEMENT

A typical school *Acceptable Usage Agreement* should stipulate that students:

- agree to adhere to the rule's set out in the *Acceptable Usage Agreement* each time they log on to online services (see appendices C, D and E);
- ensure that all communication using online services is related to learning or school activities;
- keep passwords confidential, and change them when prompted or when known by another user;
- never knowingly allow others to use their personal online services account unless directed to by a teacher for the purposes of collaborative learning;
- not use their online file storage to share or store personal or inappropriate content;
- log off at the end of each session to ensure that nobody else can use their online services account;
- not send or publish unacceptable or unlawful material or remarks including offensive, abusive, defamatory or discriminatory comments;
- not access or attempt to access inappropriate material;
- not engage in any bullying, intimidation or other inappropriate behaviour online;
- ask a staff member's advice if another user is seeking excessive personal information, asks to be telephoned, offers gifts by email or wants to meet them;
- immediately tell a nominated staff member if they receive a computer virus or a message that is inappropriate or makes them feel uncomfortable;
- never knowingly initiate or forward emails containing:
  - a message that was sent to them privately;
  - a computer virus or attachments that are capable of damaging recipients' computers;
  - chain letters and hoax emails; and

    - spam such as unsolicited advertising material, or mail unrelated to learning;
- be made aware by teachers that emails sent or received via the Department's online services may be audited and traced to the online services accounts of specific users;
- not damage or disable computers, computer systems or networks of the school or the Department; and
- ensure that online services are not used for unauthorised commercial activities, political lobbying, gambling or any unlawful purpose.

A.2 GUIDELINES FOR TEACHERS

It is recommended that teachers:

- are aware of their responsibilities for supervising student use of online services as laid out in this policy and the *Duty of Care for Students* policy;
- maintain an informed view of the relative risks and educational benefits of online activity by their students. A variety of resources are available from ACMA's Cybersmart site (http://www.cybersmart.gov.au/) to assist with this including professional learning materials, online cybersafety games, interactive learning programs, lesson plans and units of work, online helpline for students, information guides and presentation materials;
- ensure that students are aware of the possible negative consequences of publishing identifying information online including their own or other students' images;
- refrain from publishing student images or any student-identifying information on the Internet. If such publication is necessary, limit the amount of time the information is online as much as possible;
- check that any material planned for publication on the Internet or intranets has the approval of the principal and has appropriate copyright and privacy clearance;
- are aware of the steps to take and advice to give if students notify them of inappropriate or unwelcome online activity by fellow students or members of the public. Such steps may include:
    - collecting as much information as possible about the incident including copies of communications;
    - emphasising to the student that the event is not necessarily their fault;
    - identifying any risky behaviours on the part of the reporting student and counselling them on the need to adopt more protective behaviours; and
    - if the incident warrants further attention, escalate it to school and/or Department authorities, notifying police only if you suspect the law may have been broken, such as a possible attempt by an adult to groom or encourage the student to meet face-to-face;
- inform parents that student Internet access from home or other non-school sites does not occur via the Department's network and therefore Internet browsing may not be filtered;
- use group photos only with subjects in regular school uniform or day clothing when publishing on the Department's intranet or Internet. Photographs of lone individuals, of students in swimming costumes, or similar should be avoided;
- promote the use of strong passwords for students who can cope with the complexity. Stronger passwords:
    - contain a mixture of alphabetic and non-alphabetic characters;
    - are changed frequently;
    - do not contain dictionary words;

- do not contain easily identified personal information such as name, date of birth, etc;
- do not contain any part of the account identifier such as the username; and
- are not written down.

Full details on password security can be found in the *ICT Security Procedures: 1.2 Password and User ID* policy;

- adapt the sample 'Acceptable Usage Agreements' attached to this policy to suit the class context and the needs of students. In particular, giving consideration to the value of having students with disabilities or younger students signing an agreement: teachers may choose to use the agreement as a guide to discuss responsibilities with students or provide an option for parents to sign on their behalf.

A.3 GUIDELINES FOR PRACTICAL USE OF ONLINE SERVICES

It is recommended that principals and teachers:

- set realistic expectations with students prior to use of online services, for example when they can expect email replies;
- use mail enabled groups and list services to facilitate communication within and between schools;
- encourage users to manage their mailbox, deleting unnecessary email and backing up important emails or attachments; and
- encourage users to be mindful of the negative impacts on the school network of sharing or transmitting large files.