Education and Training

SCHOOL POLICY: ACCEPTABLE USE OF INTERNET, EMAIL, COMPUTER FACILITIES AND EXTERNAL NETWORKS.

This policy replaces *Acceptable Use of Computer Facilities and External Networks* published in Bulletin No 646 18 April 1996 and also replaces Circular Minute 66/96.

PUBLISHED: September 2001
REVIEW DATE: September 2003

1. PURPOSE

1.1 This policy supports and describes the process for the acceptable use of departmental computer facilities and external networks, including the internet and email, for the purposes of administration and the fostering of educational activities in ACT schools, central office and other departmental non-school workplaces.

2 DEFINITIONS

2.1 *Computer Facilities and External Networks* Includes computers, local area networks, connections to external electronic networks, and subscriptions to external network services.

2.2 *Licensed Software* Collectively refers to copyrighted and proprietary programs, data and documentation.

2.3 *Internet* Refers to the global network of multi-platform smaller computer networks which allows the user to access information and communicate electronically

2.4 *Email* Refers to a electronic communication tool which can internal or externally available to users to distribute and receive information.

2.5 *Parent* Father or a mother.

2.6 Guardian …One who is entrusted by law with the care of the person or property, or both, of another, as a minor or some other person legally incapable of managing their own affairs.

3. POLICY STATEMENT

3.1 Access for all authorised users are for educational administration and/or learning and teaching purposes.

3.2 All work places are responsible for establishing and maintaining on-site procedures for a secure computing environment with regard to authorised access, student supervision and acceptable use by staff and students consistent with the role and functions of the department, as well as the Copyright Act 1968 and the Privacy Act 1988.

3.3 Each school must implement a Code of Practice for acceptable use (see attached examples).

3.4 Central office and other non-school workplaces must implement the attached Central Office Code of Practice.

4 RESPONSIBILITIES

4.1 It is the responsibility of the **department** to:

- ensure that authorised use of computer facilities and external networks, including the internet and email, relates to departmental business and is consistent with principles, regulations and laws relating to the privacy and safety of students and departmental staff.

4.2 It is the responsibility of **all users** to:

- obtain authorisation prior to using departmental computer facilities and external networks, including the internet, through the use of passwords and user identification.

4.3 It is the responsibility of **principals** to:

- implement a School Code of Practice (use attached examples as a guide to developing a school-based code) for students, and if not accessing external networks and the internet through EduNET, staff;
- ensure that Codes of Practice are made available to and understood by all users;
- ensure that student access will be appropriately supervised as determined by the school, taking into account the age and capacity/skills of users;
- highlight to users the possible dangers of communicating personal information including full names and photographs on the internet;.

- provide information to and acquire from the person with parental responsibility, annual written permission for students under 18 years of age to use the internet and email as part of their learning and to publish or transmit student work which may or may not include identifying student information. This includes permission for any electronic publishing of student work which may be done by a third party on their behalf for every instance on a school website or sent via external email message;
- provide information to and acquire written permission from students 18 years and over (refer to previous point);
- manage and monitor web access to minimise the risk of exposure to offensive or inappropriate material; and
- promote practices for students and teachers to minimise such risks. The choice of Internet service provider (ISP) will influence the ability of schools to minimise the risks. When selecting an Internet Provider, schools should ask whether the ISP provides: a comprehensive web site and e-mail filter service and a comprehensive user reporting facility. These facilities should be explained in a Parent Information Sheet (refer to example at Attachment D) with the Code of Practice.

4.4 It is the responsibility of **managers/relevant staff** to:
- implement the Central Office Code of Practice (attached); and
- ensure that Codes of Practice are available to and understood by all users.

5 MANDATORY PROCEDURES

5.1 **Acceptable use is:**
- related to learning and teaching;
- related to educational administration;
- to facilitate and disseminate knowledge;
- to encourage collaborative projects and resource sharing;
- to aid technology transfer;
- to foster innovation;
- to build broader infrastructure in support of education and research;
- to foster professional development;
- to undertake administrative functions and any other tasks which support the business of the department; and
- minimal personal use that does not contravene this Policy and is in the spirit of users becoming comfortable and confident in using information and communication technologies.

5.2 **Supervision of computer facilities and external networks**
Workplaces and schools must take measures to ensure that computer networks are used in an acceptable manner. Procedures to ensure this must include:
- school codes of practice for students and, if not accessing external networks and the internet through EduNET, staff;
- a central office code of practice;
- security procedures to ensure authorised access to computing network;
- appropriate supervision of users that considers the age and the capacity of users;
- the use and ongoing management of appropriate software, either on site or by the service provider, to allow access to appropriate online sites only;
- education programs that focus on ethical and acceptable uses of the internet and email, as well as correct online etiquette; and
- ensuring logging procedures of system use are in place and widely publicised including specifying the positions of officers authorised to view logs and the process for informing and acting on breaches of this Policy.

5.3 **Prohibited Activities**
- For students under 18 years of age, use of internet and email, and/or publishing or transmitting student work which may or may not include identifying student information including full name or photographs, without at least written permission from the person with parental responsibility. Students 18 and over must give their own written permission. (Refer to Attachments E and F for proformas).
- Using chat rooms that are not coordinated through a teacher or staff member.
- Creating email addresses that identify student personal details.
- Uses that unduly interfere with the work of other users of the network or with their host systems or that seriously disrupt the network, or that result in the loss of a user's work.

- Transmitting or deliberately accessing material, the use of which may be harmful emotionally or physically (eg, instructions to make a bomb).
- Uses that contravene existing laws regarding transmitting or deliberately accessing information (eg, hacking), which contains profane language or panders to bigotry, sexism, or other forms of discrimination.
- Transmitting or deliberately accessing information which contains sexually explicit material.
- Uses that violate Commonwealth, State or Territory laws.
- Uses that violate the privacy of individuals.
- Communicating any information concerning any password, identifying code, personal identification code or other confidential information without the permission of its owner or the controlling authority of the computer facility to which it belongs.
- Creating, modifying, transmitting or using any computer program or instructions intended to gain unauthorised access to, or make unauthorised use of, a computer facility, software or licensed software.
- Use of the departmental computing network for commercial or excessive private purposes.
- Creating, modifying, transmitting or using any computer program or instructions intended to obscure the true identity of the sender of electronic mail.
- Accessing or intentionally destroying software or licensed software in a computer facility without the permission of the owner of such software or licensed software or the controlling authority of the facility.
- Making unauthorised copies of licensed software.
- Communicating any credit card number or other financial account number without the permission of its owner.
- Effecting or receiving unauthorised electronic transfer of funds.
- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.
- Loading unauthorised software onto computer facilities.
- Using the computer facilities and external networks in a manner inconsistent with the department's contractual obligations to suppliers of computer facilities and external networks or with any published departmental policy.