ACT Government
Education

COMMUNITIES ONLINE: ACCEPTABLE USE OF ICT – PARENTS AND STUDENTS GUIDELINES

This guidelines must be read in conjunction *and interpreted in line with the* Communities Online: Acceptable Use of ICT – Parents and Students Policy, *the* Use of Personal Electronic Devices (PEDs) in Schools Policy *and the* Education Privacy Policy

Table of Contents

1. Overview 1
2. Appropriate use provisions 1
3. Logging and monitoring 2
4. Reporting misuse, breaches and inappropriate material 3
5. Access and security 4
6. School responsibilities 4
7. Personal Electronic Devices 5
8. Appendices 6

1. Overview

1.1. This document is designed for internal use, to equip schools with information and direction in using ICT appropriately in school and communicating user expectations to their parents and students, including the use of PEDs. It is a supplementary document to the Communities Online: Acceptable Use of ICT – Parents and Students policy and the Use of Personal Electronic Devices (PEDs) in Schools policy. Sample and templates of acceptable use forms are included in the appendices for schools to tailor to suit their school approach to the use of ICT resources.

2. Appropriate use provisions

2.1. Users must not create, send or access information that could damage the ACT Government's reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory. This includes pornography and other offensive material. Material may be pornographic under *the Criminal Code 1995* (Cth) even if it features fictional or cartoon characters. The transmission, storage or downloading of obscene or offensive material may also put users at risk of breaching discrimination laws. Such use may result in disciplinary and/or legal action.

2.2. In addition to prohibited material, there are categories of internet content that are considered inappropriate for access through ACT Government ICT resources. To address this, Shared Services ICT has deployed a content filter to monitor Internet access. This filter intercepts web requests and determines whether the site being accessed is acceptable under the terms of this policy. If the filter determines that a site falls outside the policy, the site will either be blocked or a warning screen will be displayed advising that the site appears to be in breach of the policy.

2.3. The content filter will warn or block access to categories of websites including:

a) adult content
b) gambling
c) unsupervised chat rooms

d) dating
e) crime/terrorism
f) violence/undesirable activities
g) malicious
h) government blocking list (illegal websites)
i) swimsuit/lingerie models

2.4. Should users need to access legitimate sites for their work but find them filtered, they will need to seek permission from their school's ICT Coordinator or relevant executive teacher, under delegation from the school Principal, to arrange for approved access to the sites.

2.5. Users must not create, send, access, download or store inappropriate or prohibited material.

2.6. Users must not use Government resources to encourage others to engage in industrial action.

2.7. Users must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

2.8. User must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent consent for minors) being recorded and the permission of an appropriate staff member.

3. Logging and monitoring

3.1. The following information about logging and monitoring of the network is taken from the *ACT Government's Whole of Government Acceptable ICT Use Policy.* While it refers specifically to staff, the same principles and processes apply for students and their families when they are accessing the ACT Government's ICT resources.

3.2. Logging refers to the automated collection of transaction records. Monitoring includes active, ongoing surveillance by Shared Services ICT Security under the Senior Manager, Shared Services ICT Security. This document describes the way in which employees' activities may be monitored and how employees should be notified that this monitoring is being carried out.

3.3. ACT Government monitors staff use of Government computers and ICT systems by:

- maintaining logs, backups and archives of computing activities including workstations, laptop computers, servers, printers, and network connected devices, including smart phones and tablets (where applicable)
- monitoring email server performance and retention of logs, backups and archives of emails sent and received through ACT Government servers, and
- retaining logs, backups and archives of all Internet access and network usage.

3.4. Shared Services ICT Security has access rights to logs of all of staff members' activity including:

- backups and archives of all files, including emails, which are current and those that have been deleted by the user
- email messages and attachments, and
- the URLs or website addresses of sites visited, the date and time they were visited and the duration of site visits and logs.

3.5. Shared Services ICT Security in consultation with the Directorate Executive may authorise access to user logs in the event that there is a perceived threat to:

- ACT Government ICT system security

- the privacy of ACT Government staff
- the privacy of others, or
- the legal liability of the ACT Government.

3.6. These records can be called up and cited as a chain of evidence in legal proceedings and actions following virus attacks. Access will be fully logged and documented.

3.7. Shared Services ICT will not disclose the contents of monitoring to a person, body or Directorate (other than the individual concerned) unless one or more of the following applies:

- the staff member is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person, body or Directorate
- they have consented to the disclosure
- Shared Services ICT believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person
- the relevant Directorate Executive has requested monitoring or investigation
- the disclosure is required or authorised by or under law
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

3.8. Shared Services ICT may log on a random or continuous basis:

- for system management and planning
- to ensure compliance with ACT Government policies
- to investigate conduct that may be illegal or adversely affect ACT Government employees, or
- to investigate inappropriate or excessive personal use of ACT Government ICT resources.

3.9. Under the provisions of the *Workplace Privacy Act 2011*, employers must – upon being requested by the worker – provide access to the worker's surveillance records. Workplace surveillance records will be kept in accordance with the requirements of the *Territory Records Act 2002.*

4. Reporting misuse, breaches and inappropriate material

4.1. Schools MUST report any suspected illegal activity, security incidents and other incidents of a serious nature in accordance with the ACT Education Directorate's *Critical/Non-Critical Incident Management and Reporting* policy and procedures.

4.2. Schools must report to the Shared Services ICT Service Desk without delay any suspected technical security breach by users. Shared Services ICT are then responsible for following up on these complaints.

4.3. Where a school has reasonable grounds to suspect that a personal electronic device (PED) contains data which breaches the Use of PEDs Student Agreement, the Principal may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, school disciplinary action may be taken including referral to the police.

4.4. Low-level breaches of acceptable usage provisions may be managed at the school level in accordance with the school's whole of school behaviour support plan.

4.5. Where disputes arise in the handling of such breaches and cannot be resolved at the school level, they are to be escalated in line with the ACT Education Directorate's *Suspension, Exclusion and Transfer of Students in ACT Public Schools Policy.*

4.6. By signing an acceptable use agreement, the student and parents acknowledge the terms of the agreement and

- Agree to comply with the conditions of the Communities Online or Use of PEDs policy; and
- Understands that noncompliance may result in disciplinary action

5. Access and security

5.1. Prior to accessing the Directorate's ICT resources or connecting a PED to the department's Wi-Fi network, students and/or parents and guardians are required to read these guidelines and the accompanying policy: Communities Online policy and if applicable the Use of PEDs policy. All parents/guardians (with the exception of those whose children have already turned 18) are required to sign an Acceptable Use Statement for use of ICT resources and, if engaging in a school Use of PEDs program, a Use of PEDs Student Agreement. Schools may also ask students to sign an Acceptable Use Statement, depending on their age and level of understanding. Examples of forms that may be used by schools are in the Appendices.

5.2. Schools must inform parents of their right to have their child *'opt out'* of using all or part of the online services available through their school.

5.3. Schools are responsible for ensuring that their school communities have regular access to information relating to cyber-safety. Schools are also responsible for provisioning usage monitoring and internet filtering in the delivery of ICT resources.

5.4. Students bring their PEDs onto the school site at their own risk. Insurance is the responsibility of parents and students. In case of malicious damage or theft of another student's device, existing school processes for damage to school or another student's property apply. Accidents/incidents or near misses must be reported within 48 hours.

6. School responsibilities

6.1. It is the duty of each school to ensure that their school community is aware of their responsibilities under the Communities Online policy and the Use of PEDs policy.

6.2. Schools must:

- Inform their school community of the existence of these policies.
- Make these policies (and associated guidelines) available to parents/guardians and members of the school community.
- Ensure that students and their parents are aware of, and agree to their obligations under the school's guidelines and procedures, and other relevant Directorate policies.
- Ensure that school communities are adequately informed about the use of the ICT resources within their school community.
- Ensure that school communities are informed of their rights and responsibilities relating to ethical and safe usage of ICT resources.
- Report any school related accidents/incidents or near misses within 48 hours by using the appropriate form located at https://index.ed.act.edu.au/governance/risk-management.html

- Provide students equitable access to online services-enabled computers within the limits of available resources.
- Retain a copy of the acceptable use agreements signed and place it on the student's file as a record.

7. Personal Electronic Devices

7.1. ACT Public Schools allow students to bring their own personal electronic devices (PEDs) to school for the purpose of teaching and learning.

7.2. Schools will consult with their communities about the use of PEDs approach, timing of the transition, which year groups will be participating and the approach to addressing any equity issues.

7.3. The principal will retain the right to determine what is, and is not, appropriate use of PEDs at the school within the bounds of the Directorate's policies and relevant legislation such as the *Information Privacy Act 2014.*

7.4. While the Directorate will make every reasonable effort to provide a safe, secure and appropriate online learning experience for school communities, the Directorate cannot filter, monitor and control private telephone mobile access on PEDs that are using 3G/4G type networks. However, existing student welfare and behaviour management practices already in the school would apply to their use. Similarly, the individualised nature of PEDs means that the Directorate is unable to provide technical support.

7.5. Usage of PEDs on school grounds, whether accessing the Directorate network or not, is provisional on the expectation that it complies with the terms and conditions of the Communities Online policy and the Use of PEDs in Schools policy.

7.6. Users must comply with Directorate, and school guidelines and procedures, concerning the use of devices at school while connected to the Directorate's Wi-Fi Network.

7.7. Mobile phone voice and text, SMS messaging or device instant messaging use by students during school hours is a school-based decision.

7.8. Users should not attach any school-owned equipment to their PEDs without the permission of the school principal or an appropriate staff member.

7.9. Users must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the Directorate or the school.

7.10. Schools are under no obligation to provide technical support for hardware or software associates with PEDs. Schools may choose to provide this service to students if there are sufficient resources available in the school.

7.11. Long-term care and support of PEDs:

- Students and their parents are solely responsible for the care and maintenance of their devices.
- Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions as outlined on the Use of PEDs Student Acceptable Use Agreement.

- Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.
- Students are responsible for managing the battery life of their device. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for (or restricted from) providing facilities for students to charge their devices.
- Students are responsible for securing and protecting their device in schools, and while travelling to and from school. This includes protective/carry cases and exercising common sense when storing the device. Schools are not required to provide designated or secure storage locations.
- Students should clearly label their device for identification purposes. Labels should not be easily removable.
- Students should understand the limitations of the manufacturer's warranty on their device, both in duration and in coverage.

8. Appendices

- Appendix i. Sample Acceptable Use of ICT Statement – Parents or Guardians**:** An example of an Acceptable Use statement that schools could provide for students and parents to sign. This may be adapted to suit the needs of the school and the age level/ability of the student.
- Appendix ii Sample Acceptable Use of ICT Statements – Students**:** While it is important that parents acknowledge the policy in relation to their child, some schools might also have their students sign an Acceptable Use statement. Included in Appendix ii provides some examples that may be used or modified to suit individual school contexts.
- Appendix iii. Sample Acceptable Use of PEDs in Schools Agreement**:** Samples of the Use of PEDs Student Agreement including device requirements and student responsibilities have been provided; however, schools should modify them to suit their Use of PEDs model and school level.
- Appendix iv. Sample Use of Third Party Web Based Educational Services Guidelines and Mandatory Procedures**:** Sample Permission forms for schools to use in seeking consent from Parents or Legal Guardian in the use of third party web based providers by their students. These forms may be used or modified to suit individual school needs