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

These 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

1.1.   The Internet and other Information and Communication Technology (ICT) resources constitute a critical component of the teaching, learning and administrative functions of Weetangera Primary School.

1.2.   It is the duty of Weetangera Primary School to ensure that all staff are aware of their responsibilities under this policy.

1.3.   To ensure continued access to reliable and robust ICT services, Weetangera Primary School will take responsibility for managing ICT assets in line with the procedures attached to this policy.

1.4.   All users should have a secure password that aligns with requirements. Secure access to critical business systems should only be granted to key staff. The creation of generic passwords and sharing of passwords is not permitted.

1.5.   The use of data and information at Weetangera Primary School is becoming more important, in relation to legal requirements, assessment, school improvement and productivity. To ensure that data is managed appropriately, Weetangera Primary School will make themselves familiar with relevant Records Management, Privacy and Security policies. 1.1. The Education and Training Directorate (the Directorate) is committed to the use of Information and Communication Technology (ICT) in ACT public schools.

1.6.   Students will use ICT in a variety of ways including class work, homework, projects and assignments; as well as collaboration and communication with others.

1.7.   Effective use of ICT allows Weetangera Primary School to strengthen communication with parents and carers, and streamline administrative processes.

1.8.   Prior to accessing the resources provided by Weetangera Primary School, students and parents are required to read this policy (as well as any attached documents) and, where applicable sign an Acceptable Usage Statement.

1.9.   Weetangera Primary School reserves the right to revoke, suspend or terminate the access permissions of any user at any time, with or without notice.

1.10. Users should be aware that usage data will be logged, maintained, backed-up, archived and monitored for computing activities accessing ACT Government networks and resources. This includes workstations, laptops, servers, printers, network connected devices, and personal electronic devices including (but not limited to) smart phones and tablets.

1.11. Whilst the Directorate provides filtering that will minimise inadvertent access to inappropriate content on the internet, it is not possible to guarantee that students will not be exposed to inappropriate content at school. Students who seek to deliberately circumvent these filters will be considered to be in breach of this policy and will be sanctioned accordingly.

2.   Rationale

At Weetangera School we have invested considerable amounts of funding and resources into providing students with the best possible tools to assist in their learning. This has included the purchase of sets of tablets and Chromebooks, as well as interactive panels in every learning area. To ensure that these resources are properly cared for and used in a responsible manner we have come up with several procedures to follow when using the mobile ICT devices.

All students are entitled to develop the skills to successfully use various ICT devices as a part of their education, in safe and secure environment. The use of ICT devices comes with considerable amount of responsibility that will be shared with staff, students and parents.

This policy outlines:
- the roles and responsibilities taken on by staff in ICT support roles;
- support models;
- communication and consultation processes;
- escalation processes and complaints management; and
- acceptable usage by students and parents of ICT resources provided by Weetangera Primary School.

3.   Definitions

 ICT resources refers to the hardware, software, services and content and services provided by, or facilitated through Weetangera Primary School.

ICT Coordinator refers to a member/s of the teaching staff (delegated by the principal) that is responsible for the pedagogical leadership and strategic management of ICT at Weetangera Primary School.

Information Technology Officer (ITO): a non-teaching staff member responsible for the support and maintenance of ICT at Weetangera Primary School.

Parent refers to the person with legal parental responsibility for the student. This includes carers and legal guardians.

PEDs or Personal Electronic Devices refers to (but is not limited to) workstations, laptops, tablet devices and smart phones.

Peripheral Device: An item that can be connected to a computer, such as a printer or scanner.

Student(s) includes all those enrolled in years P-6.

Third Party Web Services refers to external web services used in an educational capacity that are not hosted within the Directorate's environment.

Users refers to students, parents, guardians and community members that access the Weetangera's ICT resources.

4. Appropriate use provisions

4.1.   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.

4.2.   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.

4.3.   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

4.4.   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.

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

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

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

4.8.   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.

5.   Logging and monitoring

5.1.   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.

5.2.   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.

5.3.   ACT Government monitors students 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.

5.4.   Shared Services ICT Security has access rights to logs of all of students' 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.

5.5.   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.

5.6.   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.

5.7.   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 student 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.

5.8.   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.

5.9.   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.*

6.   Reporting misuse, breaches and inappropriate material

6.1.   Weetangera School 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.

6.2.   Weetangera School 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.

6.3.   Where Weetangera 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.

6.4.   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.

6.5.   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.*

6.6.   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

7.   Access and security

7.1.   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. All parents/carers are required to sign an Acceptable Use Statement for use of ICT resources. 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.

7.2.   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.

7.3.   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.

7.4.   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.

8.   School responsibilities

8.1.   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.

8.2.   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.

9.   Management of Equipment

Tablets

- *Transportation* - When transporting tablets students must be supervised by a teacher. Please ensure students are carrying no more than three tablets to reduce damages that can be caused by dropping them. Remind students to be careful and to slow down when transporting the equipment.
- *Returning* - Ensure charging and locked.
- *App request procedure* - If you wish for an app to be uploaded onto the tablets, please email ICT Coordinator or Jim Watt with APP REQUEST in the subject box. Please provide a description of how it links to your curriculum, pedagogy and assessment.

Chromebooks

- *Device allocation* - Chromebooks will be allocated to students in Years 2-6 at the start of the school year once permission and care agreement has been signed by parents and students. Students will be responsible for the care of these devices. The Chromebooks are to remain on school site.

- *Returning* - Students are to ensure Chromebooks are returned to the charging cabinet at the end of each day and plugged in to charge. Teachers are responsible for ensuring the cabinet is locked at the end of each school day.

- *Faults* **-** If any Chromebook experiences problems, an email is to be sent to the ITO, with the word CHROMEBOOK and asset number in the subject box. A description of problem needs to be outlined.

10. Staff computers

Usage - Due to the sensitive nature of some of the data stored on Weetangera Primary School's Drives, students are not permitted to use staff logons.

Faults - Any laptop/notebook experiencing problems, please use the ICT Jobs Google Form for IT Coordinator.

11. Complaints

Where there are concerns regarding the application of this procedure or the procedure itself, people should:

- contact Weetangera Primary School's Principal in the first instance;

- contact the Directorate's Community Liaison section; or

- access the Directorate's Complaints Resolution policy, which is available on the Directorate's website.

12. Owner
Weetangera School **is responsible for this procedure.**

Date of Publishing: 10/8/2018

Date for Review: 10/8/2023

13. Attachments

Attachment A   Acceptable Use of ICT Statement – Parents and or Guardians

Attachment B   Primary School Acceptable Use of ICT Code of Practice for Students

Attachment C   Use of Third Party Web Based Educational Providers

Acceptable Use of ICT Statement – Parents and or Guardians

Overview

ACT Education Directorate public schools operate within various policy guidelines that support the rights and expectations of every member of the school community to engage in and promote a safe and inclusive educational environment. This environment includes, but is not limited to:

- the ACT Education Directorate's computer network
- Personal Electronic Devices (PEDs) that connect to its networks
- online applications hosted within the ACT Education Directorate's secure environment (e.g. Digital Backpack, Oliver) as well as online and/or cloud environments outside of the ACT Education Directorate's secure online environment.

According to the *Australian Curriculum: Information and Communication Technology (ICT) Capability*: "To participate in a knowledge-based economy and to be empowered within a technologically sophisticated society now and into the future, students need the knowledge, skills and confidence to make ICT work for them at school, at home, at work and in their communities." The ACT Education Directorate recognises the need for students to engage with ICT resources and that the safe and responsible use of these technologies – including online behaviour – is best taught in partnership with parents and/or guardians.

To ensure the security of the network and users, the ACT Education Directorate may authorise access to user logs in the event that there is a potential breach of the conditions of this policy, which may pose a threat to:

- System security
- Privacy of staff and students
- Privacy of others
- Legal liability of the ACT Government
- Student welfare

By signing this statement, you acknowledge the procedures and guidelines outlined in the *Communities Online: Acceptable Use of ICT– Parents and Students* Policy and agree to your child accessing ICT resources in ACT schools.

Acceptable Use of ICT Statement - Parent and or Guardian Consent

I have read and understand the *Communities Online: Acceptable Use of ICT– Parents and Students Policy* and its associated procedural documents: *Acceptable Use of ICT Guidelines and Use of Third Party Web Based Educational Services Guidelines.* I understand the need for my child to be a safe and responsible user of ICT resources – including the use of PEDs, and support the ACT Education Directorate in the implementation of the policy guidelines as outlined in the *Communities Online: Acceptable Use of ICT Resources* Policy. I have discussed this information with my child.

I agree to my child having access to school computers, local applications, and network drives

☐Yes or ☐No (please tick one)

Note: if you select No, this will automatically prevent your child from accessing any of the other services below.

- Internet   ☐Yes or ☐No (please tick one)

- Internal (school) email   ☐Yes or ☐No (please tick one)

- Digital Backpack   ☐Yes or ☐No (please tick one)

Name of child (printed):_____

Parent and/or Guardian (Name printed):_____

Parent Signature: _____ Date: _____

Primary School Acceptable Use of ICT Code of Practice for Students

When using ICT resources at Weetangera Primary School (including the student network, internet, email, Digital Backpack, laptops, IWBs etc):

• I will use school computers only with the permission of a teacher.

• I will follow all instructions from teachers when using school computers.

• I will not let anyone else know my passwords or usernames.

• I know that I am responsible for anything that happens when my account is used.

• I know that the school and the Education and Training Directorate receives information about anything that I send or receive.

• I will tell my teacher if I think someone has gained access to my account.

• I will make sure any email I send or any work that I wish to have published is polite and carefully written and presented.

• I will respect other students' work and ensure appropriate feedback about individual responses.

• I will not read other people's emails.

• I will not tell anyone my address or telephone number or the address or telephone number of anyone else or send photographs of myself or others.

• I will use material from other websites only if I have permission to do so.

• If I use material in my work that I have found on the internet, I will say where it comes from.

• If I see or receive any information on the computer that makes me feel uncomfortable or is inappropriate will tell a teacher straight away, or report it using the Cyber Safety Button on the Digital Backpack.

• I will not damage or disable the computers, computer systems or computer networks of the school.

I have read and understand the Weetangera Primary School's Communities Online – Acceptable Use and Management of ICT policy. I understand that disciplinary action may be taken if I do not follow this agreement, which may include loss of access to the internet, school network or the use of ICT for a period of time.

Student:
I agree to follow the Code of Practice and any other relevant rules that are set by Weetangera Primary School.

Name: **Class**:

Signed: **Date**

Use of Third Party Web Based Educational Providers

Dear parent or guardian

Weetangera School is committed to providing a technology rich environment for our students as our community believes the use of Information and Communication Technology (ICT) is fundamental in assisting teaching and learning in all areas of the school curriculum.

The use of web based learning resources and cloud based storage has risen steadily over the last decade and are increasingly being used by teachers across the Directorate to improve student learning outcomes.

Teachers make decisions designed to assist students in their learning. Sometimes it is beneficial for the student to utilise services provided by third party web based providers. Types of services provided by these service providers include online content creation, collaborative tools, online educational games and various administrative programs for tracking student assessment data.

As our school wishes to register with a number of web based service providers that require some personal information about a student in your care, I am obliged under *the Information Privacy Act 2014* to advise you of the reasons for collecting the information, what will be done with it, the consequence of not collecting it and who else may have access to it.

If you fill in this form, Weetangera School will use the information provided to observe your wishes in respect of enabling your child's access to *(insert names of third party websites)*. These sites have been identified as being a useful component in the teaching programs in many classes at *(insert school's name)*. To assist you in deciding whether to give consent, the sites identified are listed below/overleaf with the description of the type of service/program together with the website address and a link to the provider's privacy policy and terms and conditions of use. You are not required to consent – this is a matter entirely at your discretion.

If you do not consent to supply us with this information your child will not use these sites.

Normally we will not use or disclose this information for another purpose, without your consent, unless you reasonably expect us to use or disclose the information for a related purpose.

The Directorate has a privacy policy that explains how we handle personal information, including how we handle privacy complaints. The policy is available on the Directorate's website on the Publications and Policies page

Please indicate your consent/non-consent for each of the services listed by ticking the appropriate option, signing this form and returning it to the school to record on your child's file.

Yours sincerely,
Principal Signature
Principal Name
Principal
_____ School
XX Month YEAR

Provider Details and Information	Consent Provisions
Name of Provider: Type of Service: Website: Student Information Collected: **(insert what information is collected by the provider, how it is used and to whom it is usually disclosed, including whether it is usually disclosed overseas)** Terms & Conditions Link(s): Privacy Policy Link:	☐**Consent** ☐**Non-consent**
Name of Provider: Type of Service: Website: Student Information Collected: **(insert what information is collected by the provider, how it is used and to whom it is usually disclosed, including whether it is usually disclosed overseas)** Terms & Conditions Link: Privacy Policy Link:	☐**Consent** ☐**Non-consent**

Please return this form once completed.

Student's Name:
_____

Parent/Guardian's Name:
_____

Parent/Guardian's Signature:
_____

Date: _____