Ongerup Primary School
ICT Acceptable Use Policy and Electronic Communications Guidelines

Ongerup Primary School aims to provide students and staff with the latest Information Communication and Technologies (ICT) hardware, infrastructure, and online services to enhance teaching and learning.

Technology is a tool for learning, change, collaboration, and communication. The ability to locate, analyse, synthesise, and communicate appropriate information of good quality is essential in today's information rich society.

It is expected that all students access the school's ICT infrastructure in a responsible, efficient, ethical, and legal manner, whilst conforming to the guidelines outlined in this document. The use of Ongerup PS computer facilities, network and the internet is a privilege, not a right. It is conditional on students or staff complying with the ICT Acceptable Use Policy and Electronic Communications Guidelines.

ICT Acceptable Use

Ongerup Primary School ICT facilities are provided to students and staff though a variety of computer hardware, peripherals, software, and networks, including the school Intranet, Internet, and Email.
Restrictions and policies are put in place to encourage students and staff to interact with ICT in an educational context, to maximise educational outcomes and to ensure the safety and integrity of students, staff, and community members.

Students will agree to follow the principles of ICT Usage at Ongerup Primary School:

- Use digital technologies only with the permission of a teacher and follow all instructions from teachers when using school devices.
- Recognise that ICT is a privilege, not a right.
- Students using the school's ICT must not break State or Federal law. A summary of these laws is attached and form our Policy and Guidelines.
- Students will not let anybody else know their password. Students will not let others logon and/or use their account and will not access other people's online services accounts.
- Students know that they are responsible for anything that happens when their online services account is used and will tell their teacher if they think someone is using their online services account.
- Students know that the school and the Department of Education may see anything sent or received using email or online file storage services. The school has the right to check all written, graphic, and other materials produced, communicated, stored, or accessed on devices by students. This includes students' emails.
- Students will make sure that any email sent, or any work published online, is polite, carefully written, well presented and is not harmful to other students (i.e. it does not contain material that is pornographic, racist, sexist, inflammatory, hateful, obscene, or abusive nature or which promotes illegal activities or violence).

- If students use other people's work (including items taken from the Internet) as part of research and study, they will always acknowledge them.
- Students will obtain permission from the copyright owner for the use of their works if included for an entry for a competition or any other uses other than for private research and study.
- If students find any information that is inappropriate or makes them feel uncomfortable, they will tell a teacher about it.
- Students will not reveal personal information, including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- Students will not damage or disable the computers, computer systems or computer networks of the school, the Department of Education, or any other organisation.
- Students will be mindful of the possible problems caused by sharing or transmitting large files online, and for sharing other people's copyright online e.g. music and video files.
- Students will not interfere with computer settings, databases, or the work of any other student.
- Students will not download any programs or applications without the permission of their teacher.
- Students will not participate in unauthorised live chat groups, social media, or inappropriate games.
- Students must seek and be granted permission before accessing YouTube.
- Any student who attempts to deliberately seek out, create or receive material that is racist, sexist, abusive or offensive will have their access denied for periods from 1 week to 1 term.

If these principles of use are breached students risk having disciplinary or legal action taken against them, or their parent/carer.

A copy of the ICT Acceptable Use Agreement (K-2 or 3-6) is made available to all students and their parents/carers at the commencement of each school year or at the time of enrolment. Students will receive classroom instruction about the guidelines, policy and agreements and the rules for device use. The Acceptable Use Agreement needs to be discussed with parents and carers, signed by both parties, and returned to school. Any students who have failed to return the required documentation will not be permitted to use the school network or school devices.

Devices are not to be used by students for recreational or personal use whist on school premises. They are to be used as tools to enhance the curriculum. This is a directive from the Department of Education.

School Owned Devices – Loss or Damage

In the event of accidental damage, students must report the incident to their teacher.
In the event of any deliberate damage (such throwing an iPad or running with a laptop) parents/carers of the student will be required to cover the cost of repairing/replacing the device.
In the event where a third party is involved in an incident of damage, the matter will be referred to the principal to resolve.

Mobile Phones & Smart Watches/Devices

In accordance with the Department of Education's policy, students from Kindergarten to Year 6 are not permitted to have mobile phones in their possession during the school day. Any phones brought to school need to be handed in to the office on arrival and collected at the end of the day. The only exception to this is if the student needs their phone to monitor a health condition as part of a school approved documented health care plan.
Smart watches or other devices are to be put in 'aeroplane mode' so phone calls and messages cannot be sent or received during the school day.
Parents and carers who need to contact their child for any reason can do so by phoning the school.

Electronic Communications Guidelines

Students are expected to utilise school devices and networks in a manner that ensures the integrity of the school is maintained. The following information forms the Electronic Communications Guidelines for the use of school owned devices.
The Department of Education (DoE) provides each student with a unique login for school infrastructure. This is referred to as a Student Connect Account. The school is responsible for the collection of student Acceptable Use Agreements as well as the education of students regarding the risks associated with online activates.

Student Passwords/Passcodes

All students will be provided with a unique password at the commencement of the school year. These passwords are for the individual student ONLY and should never be given to another student at the school. Students are solely responsible for protecting their individual passwords. Sharing passwords could hold 'innocent' students liable in the event of misconduct. Students who use another student's password will be deemed in breach of the school's Acceptable Use Policy. Passwords may be changed throughout the school year if the integrity of their password has been compromised. A new password can be issued by their classroom teacher.

School Email

The Department of Education provides each student with their own email address (in the format of studentname.surname@education.wa.edu.au) that may be accessed at school or home through Connect. Ongerup PS currently does not utilise this service.
If this situation changes, the school will utilise this service in conjunction with learning opportunities in accordance with the Australian Curriculum.
Students should be aware of the following expectations when accessing DoE email:

- Students should be sensible in their email usage and not contribute to Spam or Junk.
- Students always consider that email correspondence is public. Even 'private' email can be shared or screenshot and sent to others.
- Do not criticise, abuse, or anger others.
- Be sensitive in what is written and conveyed.
- Never divulge personal details though email or online.

Shared Files

Students have access to an area on the school server to save documents. The students 'My Documents' folder requires a username and password to gain access. Staff have access to monitor student files, and they must be used in accordance with the school Acceptable Use Policy.

Printing

Ongerup Primary School aims to be an environmentally conscious school and students must only print when there is a direct requirement.

Digital Health and Wellbeing

Digital Health and Wellness is the branch of digital citizenship that focuses on using technology safely and appropriately. In the technological world we live in today our society is becoming dependent on the use of internet. It is becoming increasingly necessary to inform our students and children about the dangers involved with frequent internet use. A balance between the use of digital technologies and physical activities is essential. Students and parents must commit to a balanced, healthy lifestyle by only using digital devices when relevant during the school day and at suitable times at home.

Three core principles that responsible digital citizens should practise are:

1. ENGAGE positively.
2. KNOW your online world.
3. CHOOSE consciously.

The Australian Government and the Office of the E-Safety Commissioner have a range of services and resources that support digital citizenship and can be accessed to guide decision making at home.
Reference: https://www.esafety.gov.au/

Policy/Procedures/Strategy/Curriculum

Department of Education - Students online in Public Schools Policy
Department of Education - Students online in Public Schools Procedures
Department of Education - ICT Vision for Teaching and Learning in Public Schools – 2020 to 2024
Department of Education - ICT information and communication technologies strategy 2020 to 2024
School Curriculum and Standards Authority Digital Technologies Curriculum
School Curriculum and Standards Authority General Capabilities Vision/Strategy

Applicable Legislation

- Copyright Act 1968 (Commonwealth)
  Students may copy or otherwise deal with copyright material for the purpose of study or education. However, generally only the author of original material has the right to reproduce, copy, publish, perform, communicate to the public and make an adaptation of the copyright material. Reference: http://www.comlaw.gov.au/Details/C2012C00835
- Equal Opportunity Act 1984 (WA)
  This Act precludes:
    - Discrimination against persons on grounds of sex, marital status or pregnancy, family status, sexual orientation, race or political conviction, impairment or age in education
    - Sexual harassment and racial harassment in the workplace and in educational institutions, and
    - Promotes community recognition and acceptance of the equality of all persons regardless of their race, sexual orientation, religious or political convictions, impairments or ages.

  Reference: http://www.eoc.wa.gov.au/AboutUs/TheEqualOpportuntiyAct.aspx
- Censorship Act 1996 (WA)
  Students must not use a computer service to transmit, obtain or request an article knowing that it contains objectionable and restricted material. It is an offence to possess or copy indecent or obscene articles or child pornography. Students should be aware for their own protection that people who deal with such material commit an offence.
  Reference:
  http://www.slp.wa.gov.au/legislation/statutes.nsf/main_mrtitle_151_homepage.html
- Criminal Code (WA)
  Students should be aware that it is illegal to show offensive material to children under 16, and that if someone does show them offensive material that person is committing an offence. Racist harassment and incitement to racial hatred are also criminal offences. Reference: http://www.comlaw.gov.au/Details/C2012Q00003
- Cybercrime Act 2001 (Commonwealth)
  Unauthorised access to or modification of data held in a computer and unauthorised impairment of electronic communication eg 'hacking' or infecting computer systems with a virus, are illegal
  Reference: http://www.comlaw.gov.au/Series/C2004A00937
- Privacy Act 1988 (Commonwealth)
  Students should respect that the personal information of others is private. This Act covers the collection, use and disclosure, quality, and security of personal information.
  Reference: http://www.comlaw.gov.au/Series/C2004A03712