Rupanyup Primary School

ICT POLICY

Rationale:

The Rupanyup Primary School network is provided for all staff and students to promote educational excellence by facilitating resource sharing, innovation and communication. All students are given full access to the network. Any such facilities must be regarded as privileges that may be withdrawn for misuse of the resources.

Aims:

Computing facilities are provided primarily for the educational benefit of students and the professional development of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

Implementation:

1. **General Policies**
   - Use of devices/internet resources for educational benefit has priority over other (recreational) uses.
   - Appropriate language must be used in all communications including email messages, chat and web pages.
   - No user may deliberately or carelessly waste computer resources (eg. unnecessary printing) or disadvantage other users (eg monopolising equipment, network traffic etc.)
   - Consideration must be given to avoiding inconvenience to other students e.g. headphones must be used when listening to sound.

2. **Device Hardware**

Electronic devices are expensive, sensitive and must be treated carefully.
Students must not:

- Do anything likely to cause damage to any equipment whether deliberately or carelessly.
- Steal equipment
- Vandalise equipment
- Interfere with networking equipment such as hubs
- Attempt to repair equipment
- Remove any covers or panels
- Disassemble equipment
- Disable the operation of any equipment. This includes deliberately disabling another person's device.

Students must also report other people for breaking these rules.

3. **Software and operating systems**

Computer software and operating systems must be set up properly for devices to be useful. Students using school equipment will not:

- Change settings (including screen savers, wallpapers, desktops, menus, standard document settings etc.
- Bring or download programs, including games to school or run them on school devices.
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any computer, or duplicate such software.
- Deliberately introduce any virus or program that reduces system security or effectiveness.

4. Networks

Students are responsible for the security of their login and password.

Students must not:

- Attempt to log into the network with any user name or password that is not their own, or change other people's password.
- Reveal their password to anyone except the network administrator or classroom teacher if necessary. Students are responsible for everything done using their accounts.
- Use or possess any program designed to reduce network security.
- Attempt to alter any person's access rights.
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

5. Printing

Students must minimise printing at all times by print previewing, editing on screen rather than on printouts and spell-checking before printing. Students must not load paper into printers without permission.

6. Internet Usage

Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way.

Because the internet is an unsupervised environment, the school has a responsibility to ensure that, as far as possible, material obtained from the internet is not inappropriate or offensive. To this end, filtering software has been placed on the internet links. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene school rules or rules imposed by parents/guardians.

The school is aware the definitions of 'offensive' and 'inappropriate' will vary considerably between cultures and individuals. The school is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally or unintentionally, being obtained or displayed.

It is the responsibility of the school to:-

- Provide training on the use of the internet and make that training available to everyone.
- Make users aware of the school Internet Access Policy
- Take action to block the further display of offensive or inappropriate material that has appeared on the internet links.

7. Email

Email is a valuable tool for personal and official communication both within the college network and on the internet. Students and staff are encouraged to use it and take advantage of its special features. As with all privileges its use involves responsibilities.

The following accepted practices should be followed within all communications:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities.
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours. Therefore no messages should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- Do not reveal your personal address or the phone numbers of students or colleagues.
- Note that email is not guaranteed to be private. System administrators do have access to all files including mail. Messages relating to illegal activities may be reported to the authorities.

Students will not:

- Send offensive mail
- Send unsolicited mail to multiple recipients (Spam)
- Send very large attachments
- Use email for any illegal, immoral or unethical purpose
- Attempt to disguise their identity or the true origin of their mail.
- Forge header messages or attempt to use any mail server for deceptive purposes.
- Use any mail program designed to send anonymous mail.

8. World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and content. The school will exercise all care in protecting students from offensive material, but the final responsibility must lie with students in not actively seeking out such material.

Students will not deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or sexual discussion intended to provoke a sexual response
- Violence
- Information on, or encouragement to commit any crime
- Racism
- Information on making or using weapons, booby-traps, dangerous practical jokes or 'revenge' methods
- Any other material that the student's parents or guardians have forbidden them to see.

If students encounter any such site, they must immediately minimise the page window and notify a teacher. They must not show anyone else.

- The internet must not be used for commercial purposes or profit
- The internet must not be used for illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain.
- It is inappropriate to act as if you were about to break the law e.g. by attempting to guess a password or trying to gain unauthorised access to remote computers. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.
- Interactive use of the internet should ensure that there is no possibility of the transmission of viruses or programs which are harmful to another user's data or equipment
- Copyright is a complex issue that is not fully resolved as far as the internet is concerned. It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another user's document without their prior knowledge and permission. This includes the use of images and text. It is safest to assume all content on web sites is the legal property of the creator of the page unless otherwise noted by the creator.

9. Device Misuse

All ICT devices must be used in accordance with this policy. Students must not:

- Use abusive or obscene language in any communication
- Steal, or deliberately or carelessly cause damage to any equipment
- Attempt to get around or reduce network security
- Send "spam" (bulk and unsolicited email)
- Reveal personal information in any communications
- Deliberately enter, or remain in, web sites containing objectionable material
- Knowingly infringe copyright laws
- Store or share pornography or any other inappropriate content on their device
- Record (audio and/or visual) or photograph anyone without their express permission
- Publish anything on the Internet (including social media) that you do not have the right to publish
- Use programs that use excessive bandwidth, including but not restricted to: video communication services such as Facetime/Skype, video viewing services such as Netflix/YouTube, any downloading services

10. Possible Penalties

More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- Temporary ban on use of devices
- Removal of email privileges
- Removal of internet access privileges
- Detention
- Confiscation of device during class/until the end of the day
- Paying to replace damaged equipment
- Suspension
- Criminal charges may be laid with the police

Evaluation: This policy will be reviewed as part of the school's three-year review cycle.

Ratified by School Council	Date:	21/11/17
Signed:	Principal:	J Powell
	School Council President:	M Downer

Acceptable Usage Agreement

For the use of Rupanyup Primary School learning technology resources

Before you may use computer facilities at Rupanyup Primary School, you must sign this contract that binds you to the following conditions (Year 2 and above). If you break any of the conditions, appropriate penalties will be applied.

Your name:_____

The *ICT Acceptable Use Policy & Procedures* document has been explained to me, and I agree to obey the guidelines and conditions in it.

Signed: _____

Date: _____

This section must be completed by the parent or legal guardian of the student.

I, the parent/guardian of _____ have read and understand the *ICT Acceptable Use Policy & Procedures* document. I agree that my child shall observe these guidelines and conditions.

Name of parent or legal guardian _____

Signature of parent or legal guardian _____

Date: _____