RIPLEY VALLEY
State Secondary College

Achieving excellence together

ICT and Technology Acceptable Use Policy

This Policy applies to all who use the Ripley Valley State Secondary College Systems and Network

Contents

Introduction

The Ripley Valley State Secondary College ICT environment is provided for staff, students and visitors to help enable teaching and learning.

Staff and students are given access to the data network with an individual account allowing Internet access. Access to the Internet is filtered and monitored. Usage is recorded for each individual account. These facilities should be regarded as a privilege which may be withdrawn if misused.

General Policy Overview (compliance guideline)

1. Use of computer/internet resources for educational purposes has priority over all other uses.
1. Recreational use is allowed before and after school hours.
2. Individuals are expected to use the school ICT resources in a responsible and considerate manner. Each individual will be held responsible and accountable for their actions
3. Appropriate language is expected in all communication, including electronic communication. Inappropriate content, words or phrases may be captured by the internet filter and highlighted to the Principal, or Principal's delegate
4. No individual may deliberately or carelessly waste or damage computer resources (e.g. unnecessary printing) or disadvantage other users e.g. by monopolising or compromising equipment, network traffic etc.
5. Consideration must be given to assure convenience to others. For example:
   - *use headphones to listen to sound or music under direct teacher supervision*
   - *When accessing computer labs log-out and leave computer ready for the next user to log in*
   - *When accessing computer labs do not leave programs running on computers when you leave*
   - *When accessing computer labs clean up any mess and not leave rubbish or paper lying around computers*
   - *When accessing computer labs replace furniture to normal positions when you leave*

6. Information Security and Privacy is important from a personal and school wide perspective. An individual may access information on a need-to-know basis and may not share information outside the area of its intended use.
   - *It is considered to be a breach of Information Security if information that is not relevant to an individual's area of responsibility is encountered*
     - *Such information is to be ignored and not referred to in future*
     - *Each instance of Information Security breach is to be reported to the Head of Digital Technologies & eLearning.*

Computer Hardware and Software

Computer facilities are expensive and care must to be taken to ensure availability for all. It is important computer equipment is treated with respect and care.

Individuals must not:

- Do anything likely to cause damage to equipment, whether deliberately or carelessly, including (but not limited to):
  - Steal, damage, deface any equipment
  - Interfere with networking equipment such as Access Points, switches, hubs and network cables

Individuals must not, without permission from The Head of Digital Technologies & eLearning or Delegate

- Attempt to repair equipment
- Unplug cables or move equipment
- Remove any covers or panels or disassemble any equipment
- Disable the operation of any equipment

Computer operating systems and other software must be set up properly for computers to be useful.

Staff, Students and visitors must not:

- Change computer settings (including screen savers, wallpapers, desktops, menus, standard document settings etc.) without permission
- Bring or download unauthorised programs, including games, to the school or run them on school computers. Games are not permitted to be run on student laptops during school hours. **Unauthorised Online internet games are banned during school hours.**
- Copy any copyrighted software to or from any computer, or duplicate such software without licence to do so.
- Format shift digital content (video/audio/other), unless in accordance with Copyright law

Ripley Valley State Secondary College Computer Network Access and Use

Network accounts are to be used only by the authorised owner of the account. If you find a computer logged in, you should log that user out and restart the computer and do nothing else within that person's account. It is the responsibility of staff and students to make backup copies of their work, and save work to the provided OneDrive account. The school will exercise due care with backups but will not be held responsible for lost data.

Throughout the school year staff and students will be responsible to keep their folders on the network in a clean, organised, uncluttered manner. At the end of each year the student drive will be cleaned up and student work deleted. Consequently, students have a responsibility to take a copy of their work before the end of year. It is important individuals are responsible and frugal with the use of network storage.

Information Security and Privacy (applies to VISITORS and STAFF)

The security and privacy of information is important. Individuals have differing access to information depending on their role within the school. Information Security and Privacy is important from a personal and school wide perspective. An individual may access information on a need-to-know basis only and may not share information outside the area of its intended use.

- It is considered to be a breach of Information Security if information that is not relevant to an individual's area of responsibility is encountered.
- Such information is to be ignored and not referred to in future.
- Each instance of Information Security breach is to be reported to the Director Information Services

Publication of information in any form identifying Ripley Valley State Secondary College students or its employees must be performed with care and must be in accordance with RVSSC Privacy Policy (refer RVSSC website).

Posting to social media needs to be in accordance with the RVSSC Staff Code of Conduct and aligned with RVSSC Social Media Policy (refer RRVSC Website**)**

Password Management

1. The Network Administrator, in consultation with the school's ICT Learning Integrator(s), shall guide all staff, secondary students and visitors to comply with the following password management principles:

PASSWORD ATTRIBUTE	SUGGESTED MINIMUM STANDARD
Length of password	At least 8 characters
Password complexity – Mix of Characters	At least one Capital letter; at least one lower case; at least one number or at least one symbol (,.!@#$%^&*)
Number of unsuccessful login attempts before the account is locked out	10 attempts for students
Duration of lockout period	Must notify computer technicians to have password reset.
Period after which a password must be changed	180 days (every 6 months) - Users also have the ability to change their own passwords at any time
Reusability of old passwords	A password that has been used before cannot be used again

2. A person issued with a password has a responsibility to change it immediately after he/she:

a) Has been issued with the initial default password
b) Has used the same password for more than six months
c) Is advised by ICT staff to change it
d) Has reason to suspect the password has been observed or compromised

3. A person must not:

a) Share the password with anyone
b) Write the password down in an insecure location
c) Ask another user for their password for ANY reason.

If access to their files is required then a written request to the Principal or delegate is required.

4. A breach of points 2 or 3 of this policy may result in the suspension of the user account.

Computer and Network Use

Individuals must not:

- Attempt to log into the network with any user name or password that is not their own, or change any other person's password
- Reveal their password to anyone except the Network Administrator.
- Use or possess any program designed to reduce network security. Refer to Use of Proxies section on the next page
- Attempt to login to any other students laptop, other than their own
- Attempt to alter any person's access rights, including their own
- Store the following types of files in student drive or Home Drive, without permission from the Head of Digital Technology & eLearning
    - Program files (EXE, COM, BIN etc.)
    - Music, Picture and Video files, unless they are specifically required by a subject and do not breach copyright law
    - Inappropriate material – pictures or text including inappropriate filenames
    - Material in breach of Copyright

Use of Personal Devices on the School Network

For Students

Use of Personal Devices including Non-School owned Laptops, iPads/other Tablets, Mobile Phones and Smart Watches is not permitted on school premises. Access to Ripley Valley State Secondary College network on any personal device is not permitted without permission from the Principal or delegate. Refer to the Electronic Device Policy in the Responsible Behaviour Plan for further details.

For Staff

Use of Personal Devices including Laptops, iPads/other Tablets and Smart Watches requires written permission from the Principal to be connected to the school network. Please see Head of Digital Technologies & eLearning for further information.

For Visitors

With notice, a generic login can be provided for visitors to access limited internet. Please see Head of Digital Technologies & eLearning or School Technicians for further information.

Printing

A Print job may be sent to the ‘Find me- Black’ or ‘Find me-Colour’ queue and released from any Photocopier in the school. Students have access to the Library Photocopier. Staff have access to the Administration and Library copiers.

In the interests of our environment, the use of printing is to be minimised by: print previewing, editing on screen and spell-checking before printing. Students must not load paper into printers without permission. Paper that is pre-used, torn, creased, damp, irregularly shaped or sized should never be used in any printer, laser or ink jet. Any damage resulting from inappropriate use may be charged to the account of the person responsible.

Students receive an allocation of $10 per year for printing. Any unused amount is not rolled over to the next year. Printing costs are as follows: 10c/page for A4 mono; 50c for A3 mono; 50c for A4Colour; and, $1.00/page for A3 colour. Students can top up their printing account through student services.

Staff and students are issued with a Photo ID card that can serve as a Print Release card. Simply follow the instructions on the printer to set up your Photo card as a print release card.

Email

Electronic mail is a valuable tool for personal and official communication both within the school’s network and on the Internet. Education Queensland is the owner of all emails created from Education Queensland email accounts. Staff must use their school email for all school related matters including (but not limited to) contact with: parents; peers; professional associations; others for the purposes of improving educational outcomes for students. Staff members are able to access other email services for private (non-school) matters on a limited basis in their own time. School related email communication is a priority. Students are restricted to school provided email.

Some tips for good use of email:

- 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 communication. No message should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.

- Do not reveal your personal home address or the phone numbers of staff or students without consent Note: email is not private. Education Queensland is the owner of emails created in the schools environment. With permission from the Principal, a senior member of the ICT team may access all files including mail if requested for legal matters. Messages relating to illegal or inappropriate activities may be reported.

Individuals will not:

- send offensive or inappropriate email
- send email with large attachments, any mail with attachment >10MB is blocked
- send unsolicited mail to multiple recipients ("spam").

Student and Staff Data Management

Students and Staff are responsible for their own data. All data saved on the device (E.g. in MY DOCUMENTS) is not backed up, and cannot be guaranteed. Students and Staff are responsible for backing up their data using their Office 365 OneDrive storage or another approved method. Ripley Valley State Secondary College will not be held responsible for any lost data.

Assessment Extensions for Students will not be given for lost data. It is a requirement that all Assessment are to be created and saved in OneDrive.

Ripley Valley State Secondary College is not responsible for the cost of data recovery if required, and will not supply extensive technician time in recovering lost data.

Students and Staff School Network Drives (Student Drive, or ‘G’ Drive for Staff) is not for personal storage. Student and Staff devices are government devices. Illegal music and music is not to be saved on devices at all, and all illegal material found will be immediately deleted.

Internet Access and Usage

Access to internet on the school network is a privilege. Internet access is expensive and has been provided to assist students' education. Students must use it in an appropriate and unauthorised manner. It is not intended for entertainment. Student’s internet access is filtered through Education Queensland and monitored by delegated staff using AB Tutor.

Filtering software has been placed on the school’s network so that it monitors and records details about Internet usage. All web access by students is tracked and logs are kept for a period of time. Students who utilise more than their fair share of Internet data/bandwidth may have their Internet Accounts suspended. Students are allowed 5G per month. This allowance is reset each month. Please see the Head of Department – Digital Technologies & eLearning for all ‘Bandwidth Increase’ requests.

World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and media. The school will exercise care in protecting students from inappropriate material, but the final responsibility rests with students in not actively seeking out such material. It is conceivable that, especially for senior students, information is required for curriculum purposes that may appear to contravene the following conditions, i.e. some sites may be blocked by the internet filter when required for learning. In such cases, it is the responsibility of students and teachers to request access to the Head of ICT the need to access such sites.

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
- Gambling
- Dating
- Social media during school hours without approval
- Violence or racism or discrimination against minority groups
- Information on, or encouragement to commit any crime
- Any other inappropriate content

The only exception is if it forms part of an approved classroom lesson and is supervised by the teacher, with appropriate parental consent. If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher.

Acceptable Social Media

Access to social media such as: Podcasts, WiKi's, Blogs, content communities (YouTube) are permitted if it is for educational use. All social media access is banned for all students under the age of 14. All social media access is blocked on the school network.

Unacceptable Social Media

The following types of social media are not permitted for students unless there is an educational reason:

- virtual game worlds

- On-line gaming

- The following types of social media are not permitted for any students: Twitter, Tumblr, Facebook, Instagram and Myspace, SnapChat, dating sites, anything deemed inappropriate by the Principal (or delegate).

Proxies

The use of proxy servers (proxies) or similar methods to bypass the school's content filtering software is considered a major breach of the ICT AUP and Student Responsible Behaviour plan.

Torrents

Torrents are used to enable downloading, distributing and sharing large amounts of data over the internet. Use of torrents is not permitted on Ripley Valley State Secondary College's network, and is considered a major breach of the ICT AUP and Student Responsible Behaviour plan.

Ripley Valley State Secondary College Acceptable Use Policy (*Summary and Agreement)*

This document defines the Acceptable Use Policy for students involved in the Ripley Valley State Secondary College Technology Program. Its main purpose is to encourage the mature and responsible use of the facilities available to the students through the provision of clear usage guidelines. Students authorised to use the school's computer systems also have Internet and Electronic Mail access.

Ripley Valley State Secondary College deems the following to be responsible use and behaviour by a student:

It is expected that students will use school computers and network infrastructure for:

- assigned class work and assignments set by teachers;
- developing appropriate literacy, communication and information skills;
- authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by the school;
- conducting general research for school activities and projects;
- communicating or collaborating with other students, teachers, parents or experts in relation to school work;
- Accessing online references such as dictionaries, encyclopaedias, etc.
- researching and learning through the Department's e-learning environment, and tools including class notebook, OneDrive and other third party websites agreed to with all parties (please refer to the Third Party Website agreement form)

Ripley Valley State Secondary College deems the following to be irresponsible & unacceptable use and behaviour by a student:

- use the IT resources in an unlawful manner
- access, download, create, store, display, distribute or publish inappropriate, offensive or dangerous information, images or messages;
- transmit personal information about any member of the school community;
- cyberbully, insult, harass or attack others or use obscene, threatening or abusive language;
- deliberately waste printing and/or internet resources;
- Damage or disrupt any equipment, software or system performance.
- use the network for any illegal activity, including plagiarism or violating copyright laws (e.g. use, have possession of &/or sharing of illegally downloaded games, music or video content)
- participate in unsupervised internet chat;
- send chain letters or unwanted or spam e-mail (junk mail);
- access personal 3G/4G networks during school time;
- knowingly download viruses or programs capable of breaching the Department's network security;
- handle or use another student's device without permission or teacher authorisation
- download any files (including, but not limited to MP3, MPEG) unless specifically authorised to do so by the teacher;
- carry out any commercial activity;
- use devices or the network for production of advertisement or political lobbying;
- access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission and without them present, or teacher authorisation;
- vandalise or interfere with data of other users on the network;
- gain unauthorised access to resources;
- post anonymous messages;

- share personal information or agree to meet any person met through the internet;
- not reporting unsolicited email messages particularly from unknown persons;
- send unauthorised personal information such as a home address or telephone number through the internet
- Transmit any material in violation of any government regulation. This includes, but is not limited to, material under copyright, threatening or obscene material, or material protected by trade secret.
- Use technology for production of advertisement or political lobbying.
- Carry out any unlawful copying of software, music, games or video content. This includes, but is not limited to, sharing such data via USB, CD, airdrop or email.

In addition to this, Ripley Valley State Secondary College states that:

- Users are responsible for the security, maintenance and integrity of their individual devices and their network accounts. Students and their parents/guardians are required to register their personal device/s with Ripley Valley State Secondary College prior to connecting to the school network and use their MIS details (e.g. jsmit23) to protect their account.
- Under no circumstances should passwords be divulged to any other user on the system. If users have any reason to suspect that their account security may have been compromised or tampered with, it should be reported immediately to the Systems Technician &/or the Head of Department – Digital Technologies & eLearning.
- Accidental damage to a device is the owner of the device’s responsibility. Students and their parents / guardians will be held responsible for the wilful and deliberate misuse or inappropriate behaviour resulting in damage to another student’s device. In the event of a dispute regarding the cause of damage to a device, the principal or nominated delegate will be the arbitrator.
- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.
- Students must get teacher permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.
- The school will educate students regarding cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to behave in line with these safe practices.
- Laptops are to be carried in the Ripley Valley State Secondary College provided laptop case at all times. All devices must be clearly identified (e.g. school provided label) at all times.
- Devices must have 3G/4G disabled in the school environment if the device has that capability.
- Devices are not prohibited to connect their device to their personal hotspot, or other unfiltered WIFI or internet during school hours.

Please return this page, signed by student and parent/guardian, to Ripley Valley State Secondary College.

Ripley Valley State Secondary College ICT and Technology Acceptable Use Policy Agreement 2020
Student Agreement
***By signing this document, I hereby acknowledge that I have read this agreement with a parent, and I completely understand what I have read. I accept all terms outlined in this agreement, and agree to follow all the rules that I have read*.**

Student Name:	
Students Grade:	
Students Signature:	

Parent Agreement
By signing this document, I hereby acknowledge that I have read this agreement with my child, and I completely understand what I have read. I accept all terms outlined in this agreement, and recognised that I am responsible for my child's use of technology at home.

Parent Name:	
Parent's Signature:	

This policy must be returned to the Head of Department – Digital Technologies & eLearning so access to technology can be granted.