

Information and Communication Policy



1. Rationale

The use of digital technologies is a mandated component of the National Australian Curriculum. The use of digital technologies is part of the Digital Technologies domain and is part of the general capabilities.

The college seeks to prepare students for the demands of an ever-changing and digitally connected world through facilitating learning about technology and using it to achieve powerful learning and teaching and improve student learning outcomes.

The college will seek to do this in a manner that does not compromise student wellbeing through overuse or misuse. Its use by the members of the college community is to be based on clear ethical and practical boundaries to ensure that devices and the ever-developing technology is used safely for the benefit of all.

2. Scope of Application

This policy is applicable to the following entities:

- On school grounds and any location used by the school for events, activities, excursions, camps.
- Online environments such as, but not limited to, Microsoft Teams and all other online platforms utilised by the college.
- It applies during school hours, after school hours, weekends and school holidays.
- It applies to all members of the school community.

3. Interpretation

Within this policy, unless specifically defined otherwise, the following terms shall have these meanings:

<i>Parent</i>	means step-parent, legal caregiver or guardian.
<i>College</i>	mean Red Rock Christian College.
<i>Deepfake</i>	is a synthetic media created using artificial intelligence, where a person's likeness is used to create images or videos, often resulting in false representations. This technology can create realistic but fake content, which can sometimes be difficult to distinguish from authentic material.

4. Aims

- Digital learning will enhance learning rather than detract from a focussed and productive learning environment.
- Teachers are discerning in what is accessed through the internet, aware of what students are doing at all times and clear about protocols and ethical usage.
- Guidelines for ethical use are clear and well-known by staff and students.

Key Outcomes for Students to become literate learners who:

Information and Communication Policy

- Want to be connected.
- Are discriminating (is it of value? Will it help to achieve set goals?)
- Empowered and critically literate.
- Are informed seekers and navigators.
- Understand they are part of a global community and that learning is unrestricted by classroom walls.
- Are demanding of content, teaching quality and access to resources.
- Think, analyse and construct knowledge.
- Understand the risks and become wise users, not addicted users.

5. Policy

This policy seeks to provide clear guidance and protocols for the ethical and integration of digital devices and Information and Communication Technology within the teaching and learning programs of the college.

5.1 It is our Policy that:

- a. the use of ICT is managed through a 'whole-of-college-community' approach.
- b. the use of ICT may be used only for subject-related content and activities, and at the direction of the teacher.
- c. the use of ICT including all social media platforms during school hours and out of school hours impacting on the safety, wellbeing or reputation of other members of our college community or on the college will be deemed a breach of this policy.
- d. ICT education strategies are implemented within the college with a focus on teaching age-appropriate skills and strategies that empower staff, students and parents to be safe and effective learners.
- e. Staff act as positive role models in the use of ICT (phones included).
- f. Parents should not contact students through digital devices including but not limited to apps/phones/watches/computers.
- g. The college reserves the right to monitor traffic and review all content sent and received on the college systems or devices brought to the college by students and staff.

5.2 School Services

- The college engages COMPNOW to manage the ICT infrastructure of the college.
- Access to the college network is provided through a filtered service. The filter is designed to restrict access of inappropriate material as well as provide spam and virus protection.
- Approval must be sought before connecting privately owned ICT equipment and devices to the College network to avoid risk of malware.
- The college uses the programs Office 365/Teams, Compass and Adobe Creative Suite.
- All student and staff logins and passwords are to be kept confidential to prevent others accessing their accounts.
 - Primary students are allocated a password which is kept by their teacher.
 - Secondary students enter a new password when they first login.
- The college provides iPads for use in the Year Prep - Year Two classrooms. These are shared devices and are managed by the college.
- The college provides laptops for use in the Year 3 classroom. These are shared devices and are managed by the college.

5.3 Bring Your Own Device

- From Year 4 (2025), students are responsible to bring their own device every day.
- Devices must be compatible with the usage required. Parents are provided with the required specifications at the time of enrolment.
- Students must ensure their computer is fully charged before school.
- Families are responsible for the maintenance and upkeep of their child's computer.
- Students are responsible for the care and appropriate use of their computer when at school.
- Families are responsible for the cost of damages and insurance covering damages, theft or loss.
- Families are responsible for installing appropriate filters/firewalls/security features to prevent students accessing inappropriate material at home.

5.4 Guiding Principles for Ethical Use

Adapted from the TECH SMART acronym: Christopher McGilvery, Angelo State University

T – take care of technology equipment and software programs. Look after your equipment, especially if it is provided by the college. Be careful and discerning what you download, click on and share with others.

E – Explore carefully: identify appropriate and safe sites for learning and research. Many websites contain inaccurate, false or harmful content. When appropriate, a teacher will provide a list of websites. Learn how to evaluate websites and assess whether the content is trustworthy and accurate.

C – Copyright and related laws will help ensure learners follow the rules in using, sharing content. Using another person's data, words or ideas without acknowledgement is a form of stealing.

H – Harassment and cyberbullying are not tolerated. Do not use the internet or social media to say or represent cruel, hurtful or untrue things about another person, including staff. Do not post images of another person, including staff without their permission. Report cyberbullying to your teacher or Head of School if it occurs.

S – Social Media: protect your identity. Without seeing faces, people can easily overshare in a digital world. Authorities and future employers look up candidates' social media accounts to see how they represent themselves in public.

M – Manners matter. Respect the 'netiquette' of digital interaction. 'Netiquette' comprises the rules of an online community. Sloppy writing in online forums, device distraction while in conversation, and sending unsolicited email are a few examples of poor netiquette. Understand what makes good and bad netiquette and practice good manners online.

A – Always give credit to the original source of data and information. Like citing references in written assignments, recognise the importance of using online citations to respect copyright laws and avoid plagiarism.

R – Responsibility is a choice. Aim to be effective, thoughtful and ethical digital creators. Learn how to use technology responsibly, allowing teacher oversight. Choose to be responsible in the way you use the resources or the internet and digital devices.

Information and Communication Policy

T – Think before you click. Think about technology's purpose in all digital interactions. Be wise and thoughtful about what you are creating online before you click or write. Be aware that looking at porn or violence online damages your thinking and reduces your empathy and care for others. Think before you click.

5.6 Acceptable Behaviours

- Only use their devices for education purposes while on school grounds or attending school events.
- Use and store their devices with care.
- Bring their laptop every day, fully charged.
- Take responsibility for backing up and storing data/assignments/research. One Drive is encouraged to store and manage their files.
- Check their email regularly.
- Appropriate copyright is applied, and the source of information used or published is acknowledged.
- All use of IT networks, services, internet, and devices must be in keeping with the values of Red Rock Christian College.
- Report any inappropriate use of the devices to a teacher/Head of school or principal.
- Log off before leaving the device unattended.

5.7 Breach of Acceptable Behaviours

- While at the college, using a network or internet connection other than the college network is not allowed this includes VPNs, hot-spotting off a phone – using personal data on a phone.
- Students must not share passwords.
- Students must not access the profile of other students without permission on any platform including but not limited to COMPASS.
- Personal Devices must not be shared with other students.
- Participation in non-educational activities such as the purchase and/or sale of products or services
- Capturing voice records, video or images of other students or staff in the school toilets and changing rooms, regardless of permission.
- Capturing voice records, video or images of other students or staff in the gym, classroom and school grounds other than for reasons outlined in 5.2 Exceptions of the Mobile Phone Policy 6.13.1
- Illegal activities such as threatening the safety of others or behaving in criminal activity.
- Accessing or attempting to access inappropriate, age-restricted, or objectionable material or internet sites.
- Writing or sending images real or created, including deepfakes that are threatening, abusive, bullying, offensive, sexually explicit through any digital means.
- The use of the internet will be monitored by the college. Students are not to attempt to bypass the college settings or attempt to access any part of the network that they do not have permission to access.
- The device must not be used to store or access anything that might be dangerous or offensive. Examples of this would be swearing, pornographic material, racist, violent or hate material.

Information and Communication Policy

Breaches of this policy will be met with consequences including but not limit to loss of use of devices, suspension, expulsion, police involvement or legal action as appropriate to the breach.

Note: It is a criminal offence to use our Personal Digital Devices to menace, harass, or offend another person, and almost all calls, messages, emails and social media activity can be traced.

References

This section provides information on other documents that provides support or authority for the policy – either in forming the position or as additional or related content.

- 3.1 Behaviour Response Policy
- 3.2 Bullying Policy
- 4.8 Social Media Policy
- 6.13.1 Mobile Phone Policy
- <https://online.nwmissouri.edu/programs/education/msed/curriculum-instruction/ethics-technology-use-classroom/>
- <https://www2.education.vic.gov.au/pal/digital-learning/policy>

Review

The policy will be reviewed biannually. A review will be conducted by the responsible officer, drawing upon input and feedback from:

- School Leadership.
- Directors of Learning and Curriculum Leaders.
- Interested Parties.
- External changes, such as changes to legislation, good practice.

Policy Information

Document Title and Number	Information and Communication
Classification	Section 6 Curriculum and Co-Curricula
Prepared By	Principal, Karen McCoy & Leadership
Authorised By	Karen McCoy
Date Approved	23 June 2023

Information and Communication Policy

Date Issued	26 July 2023
-------------	--------------

Version History

Release Date	Summary of Change
1/5/2025	Includes term deepfake
26/11/2024	Section 5.7 - includes VPN
12/11/2024	Recording of others - Breach
20/02/2024	Change BYOD to Year 4
01/06/2023	Major changes to structure and content
01/08/2012	Acceptable use Policy