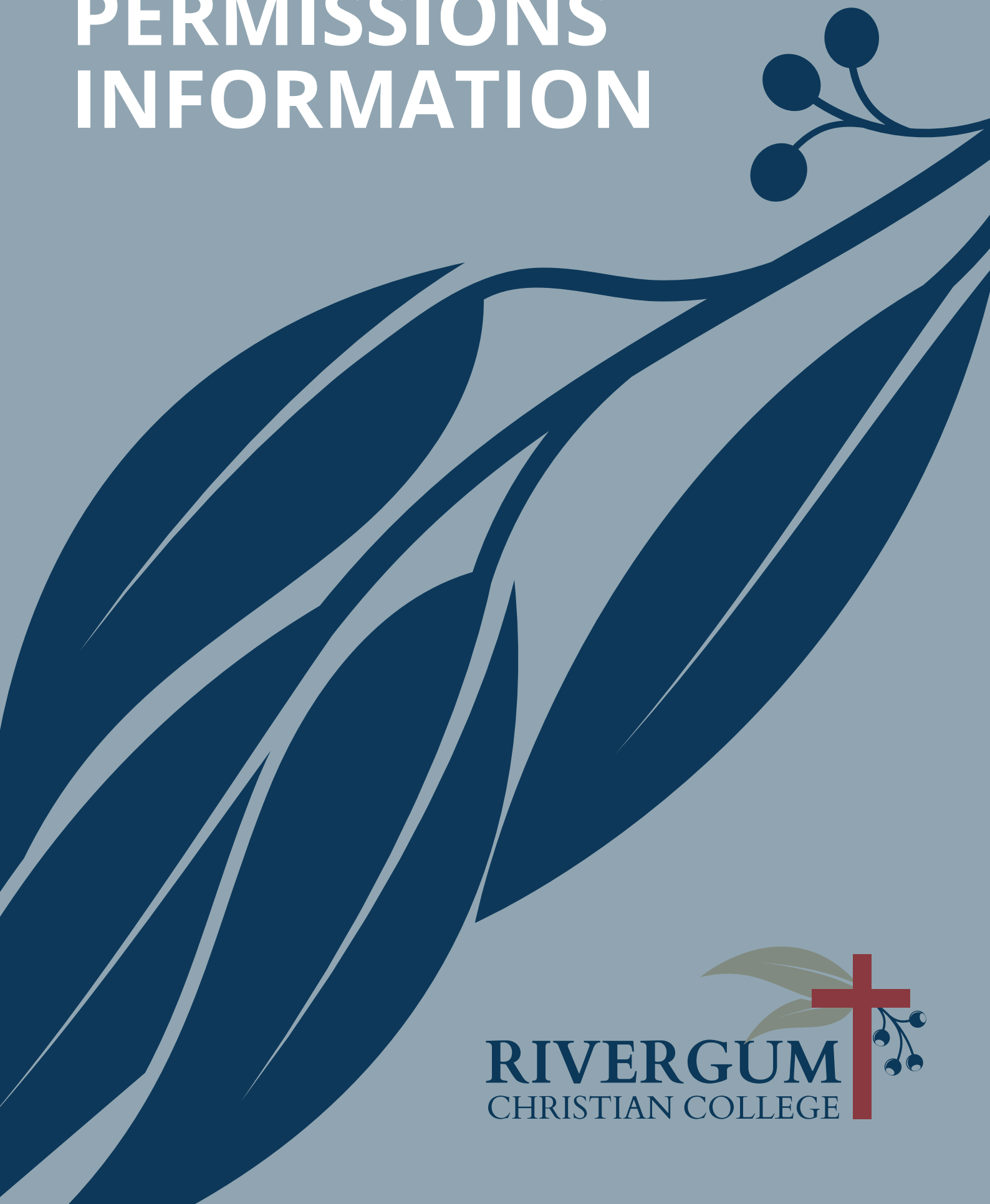
PARENT PERMISSIONS INFORMATION



RIVERGUM
CHRISTIAN COLLEGE

What is this guide?

This guide contains essential information about permissions and acknowledgements required before your child can fully participate in school activities for 2026.

To ensure a smooth start to the year, we ask all parents and caregivers to review the information in this document:

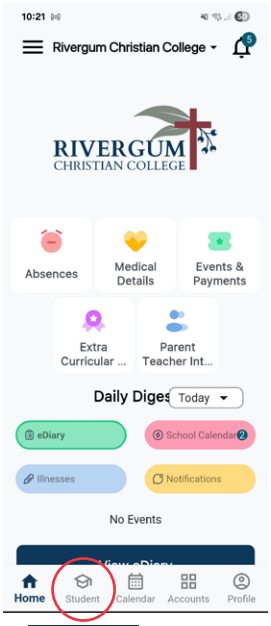
- ICT Agreement
- Parent Permissions
- Terms of Use for CCTV and Facial Recognition Services

Please take time to read through each section carefully, as students will not be able to receive devices, use technology, or attend local activities until these permissions are completed.

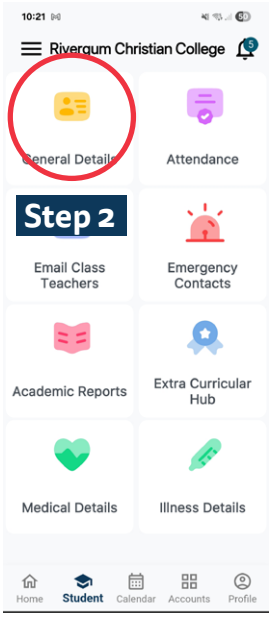
All responses must be submitted via the Orbit App by Sunday 25 January, 2026.

Please see our handy visual guide on how to access these permissions.

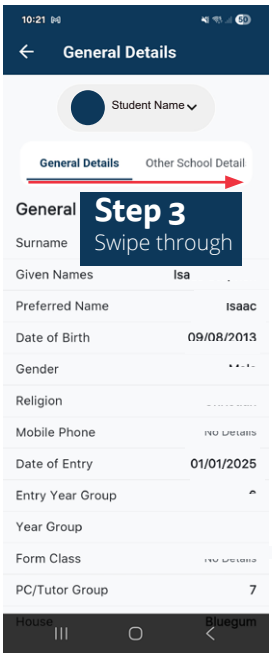
If you have any questions or concerns about any of these policies, please don't hesitate to contact the school office.

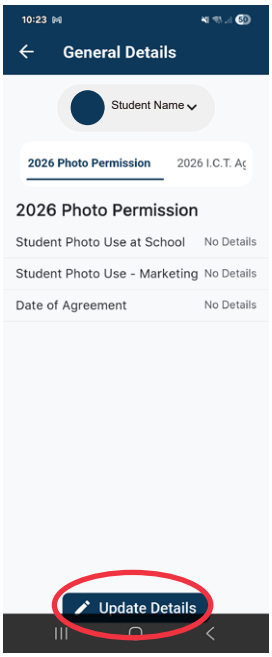


Step 1



Step 2





Each section will have the ability for you to 'Update Details'. Please swipe through to find all sections.

You'll need to action:

- ICT Agreement
- Parent Permissions

Once you've updated your details, no further action is required.

ICT Agreement

1. Agreement for Student Device Usage

This agreement outlines the terms under which RCC provides access to a school-issued laptop and other technology based educational products and services.
All Students are allocated a device while enrolled at RCC. The school will ensure that each student has access to an appropriate device necessary to complete their required school-based studies. The school follows a typical three-year device lifecycle for secondary students and generally provides new devices to students in Years 7 and 10. This ensures students have reliable performance and battery life throughout their studies.

School-Supplied Device Terms

1. The device, with accompanying software, is provided to students while enrolled at RCC. Additional educational software may be installed at the school's discretion.

2. The student is the custodian of the device, not the owner.

3. The guardians/students must report any dissatisfaction with the device's condition within two days of receipt. Failure to do so implies acceptance.

4. The device must be kept in good working order. Guardian/Student are liable for repair charges as stipulated in this agreement.

5. Guardians/students are responsible for the wilful damage caused to the device.

6. Guardians/students are responsible for any serious network-level abuse, such as intentional hacking or the installation of malicious software on any school owned device. Any damage to the device or the school's network resulting from neglect or inappropriate actions will be evaluated by the school's insurer and/or the school, and associated costs may apply.

7. Only the allocated student may use the device.

8. Supervision of the device outside school hours is the Guardians responsibility.

9. Devices, software, and accessories must be returned upon request by the school.

10. Devices maybe confiscated at the direction of school leadership.

11. Upon a student's withdrawal from RCC, the device must be returned on or before the student's last day. If a device is not returned within 2 weeks of exit, the guardians account will be charged for the Complete Device Replacement.

2. ICT Usage Expectation

The school provides a range of information and technology resources to support student learning throughout their enrolment. These include, but are not limited to, devices issued through the school's laptop program, interactive smart panels in classrooms, tablets, cameras, and other tools used for educational purposes. Access to school-owned devices and the school network is a privilege, not a right.

General Expectations

- All students must use school technology responsibly and appropriately.
- Devices are to be used only during lessons and with teacher permission.
- Recreational use (e.g., music,) is not permitted, unless approved by staff.
- Photos or videos must not be taken without consent of the individual.
- No media is to be shared or posted online without explicit school approval.

Examples of Inappropriate Use (not limited to):

- Downloading, streaming, or installing copyrighted or unauthorised content, including software.
- Tampering with software or hardware settings on school devices.
- Attempting to bypass internet filters, including by using personal hotspots or VPNs.
- Storing or accessing inappropriate content (e.g., offensive, explicit, or illegal material).
- Sharing personal information or media of others without consent (e.g., posting photos of other students).
- Copying work or accessing files that do not belong to you without permission.
- Using another student's login credentials.
- Accessing inappropriate websites, such as those containing violent or pornographic content.
- Misusing the network for non-educational or disruptive activities.
- Engaging in cyberbullying, harassment, or any form of digital misconduct.

Consequences for Misuse

- Temporary loss of access to devices and/or the school network.
- Disciplinary action, which may include suspension or expulsion.
- Additional consequences in line with the school's student behaviour management policies.
- Serious breaches (e.g., cyberbullying, illegal activity) may be referred to the eSafety Commissioner or other government authorities as required by law.
- A misuse charge may be issued at the discretion of the Principal or Deputy Principal.

3. Device Chargers

School-issued devices are insured and maintained through the school's approved repair partner.
All repairs are carried out by this servicing provider to ensure the use of genuine parts, upholding manufacturer warranties, and maintaining safe operation of the device. As these devices remain the property of the school and may be resold in the future or given to another student, only approved and authentic components are used.

Device Charge Schedule

Item	Charge
Complete Device Replacement	$1000
Cracked or Broken Screen	$500
USB C Power Adaptor	$60
Laptop Stylus Pen	$60
Intentional Misuse Charge. For example, students installing games resulting in unintentional installation of malicious software. To be charged at discretion of the principal or deputy principal.	$50-100
Other Damage (e.g. keys, graffiti)	Assessed case-by-case

4. Software & Application

RCC maintains a broad range of applications for students to use while students are enrolled. Some of these products can be used on personal devices. Students can use their school Microsoft account to access these products. Please refer to the relevant third-party privacy statement when using this software on home computers.

The following applications are preinstalled on student laptops:

- Office 365 suite (Outlook, OneDrive, Word, Excel and PowerPoint)
- Adobe Creative Cloud (Portal allows installation of Photoshop, Illustrator, Premiere Pro and other Adobe products as students require.)
- Antivirus and Endpoint Protection
- Canvas (via web browser)

Additional applications can be found and installed by the student without teacher or school IT Department permission via the Microsoft Company Portal.

The following applications can be found via Company Portal:

- MuseScore, GameMaker, Audacity, Blender 3D, Autodesk Fusion, Visual Studio, etc.

VET Subjects Software

Additional software may be installed for senior students undertaking Vocational Education and Training (VET) subjects, in consultation with the VET Coordinator and IT Manager. However, the school does not guarantee the functionality of these applications and will not provide technical support for their use. All installations are provided as-is, and the school accepts no responsibility for any issues that may affect participation in external training courses.

Students enrolled in VET subjects are strongly encouraged to check the software requirements of their specific courses. In some cases, VET programs may require the use of specialised computers, and students may need to attend sessions at the VET provider's computer labs to access the necessary resources, or alternatively, purchase a high-specification computer for use at home.

Microsoft OneDrive – Student Cloud Storage:

To support effective data management, each student is provided with 200GB of Microsoft OneDrive storage for their entire schooling.

- Storage is expected to be sufficient for most users.
- Students must periodically delete unnecessary files.
- Storage is not for anything that is personal in nature.
- Senior students in multimedia courses may request an additional 50–100GB, subject to leadership approval.

General Software Usage

- All additional software must be approved by the IT Manager.
- The school may remove software that affects device performance.
- Devices may be reset if needed. Students should save all work to OneDrive.
- The school does not take responsibility for personal software or data stored.

5. eSafety - Web Filtering and Device Monitoring

RCC employs a range of third-party technologies to help maintain a safe online learning environment for students using school owned internet-connected devices. These third-party platforms use a combination of artificial intelligence, heuristics, manual categorisation, and prevailing societal

norms to filter web content. However, due to the vast and constantly evolving nature of the internet, the school cannot guarantee that all inappropriate material will be blocked at all times. Just as at home, students may occasionally encounter unsuitable content.

What providers such as Microsoft or other third-party platforms classify as "appropriate" may not always align with our Christian values. The school takes this into careful consideration and applies due diligence in configuring and reviewing these systems. **Web filters and device monitoring settings are regularly reassessed and adjusted to better reflect the expectations of our school community.**

The platforms mentioned below generate automated reports for key school leaders and student welfare staff when concerning activity is detected — activity such as access or attempted access to inappropriate content, signs of cyberbullying, or indicators of self-harm. The school takes these reports seriously and will respond with care and diligence in line with our behaviour management and wellbeing policies.

Web Filtering

The school currently uses two types of web filtering systems to help protect students online. Microsoft Defender for Endpoint provides a lightweight, always-on filter that remains active even when students are offsite. Microsoft Defenders primary focus is cybersecurity—blocking sites commonly associated with malware and viruses, such as those related to pornography or gambling—it is not designed to serve as a comprehensive school web filter.
In contrast, the on-site web filtering system offers more holistic protection, with broader content filtering tailored to the educational environment. It also provides teachers with greater flexibility to grant access to specific websites that may be required for learning activities.

Device Monitoring

The school uses device monitoring software to support teachers in managing student devices and monitoring computer use. This platform helps keep students focused on their learning and minimises distractions from non-educational activities. It also allows staff to observe online behaviour, identify students who may be at risk, and respond to emerging concerns.
Teachers are able to view and monitor student device activity between 8:00 AM and 4:00 PM, Monday to Friday, regardless of whether the device is connected to the school network, home Wi-Fi, or a personal hotspot.

Duty of Care

It's important to understand that although our systems can report 24/7 all year round, the school is only able to monitor and act on reports or alerts during school hours. Any alerts or indicators of self-harm triggered outside of these times — such as on weekends or during school holidays — fall outside the school's responsibility. While we will always do our best to support student wellbeing, parents and carers remain responsible for monitoring and responding to their child's online activity outside of school. The school's duty of care does and cannot not extend into the student's home or online platforms that are not managed by the school.

Therefore, the school is not responsible or liable for content and activity that students view or do outside of school hours and/or online platforms. Parents should also be aware that these systems and processes are not full proof, and alerts or indicators maybe missed by staff and our third-party systems.

The safety and well-being of our students is our top priority. We have a comprehensive duty of care policy that outlines our responsibilities to protect students from harm. This includes providing a safe physical environment, ensuring adequate supervision, providing tools to safeguard students online, in addition to allowing students to self-report.

In line with the eSafety Commissioner's best practices, we encourage students to use their school-issued devices in open family spaces under parental supervision. Refer to www.esafety.gov.au for further information.

6. Cyber Security

Identify Management

RCC uses Microsoft 365 as the main identify management solution and productivity suite for both Staff and Students. Microsoft 365 shares Students' names and school-based emails as needed to complete authentication requests with our third-party providers.

Student Multi Factor Authentication (MFA)

Students are not subject to corporate MFA, however students can only log into Microsoft services and other school resources on school-owned devices. This limits access and adds a layer of protection.

Logins from overseas are blocked. If overseas access is needed, prior approval from the Principal is required. Educational Platforms that support the use of student's school owned Microsoft accounts for authentication, for example Adobe Creative Cloud, Autodesk Fusion and Typing Tournament may not require MFA or school-owned devices. Therefore, students are permitted to use school Microsoft accounts on home devices for these applications.

Senior Students access on personal devices

Some senior students (e.g., VET students) may need to access Microsoft services on personal devices (e.g., for TAFE course evidence). In these cases, MFA is required to access Microsoft services such as OneDrive and email on personal devices. Senior students can visit the IT Department for MFA setup.

7. General Use and Use of Devices

General Use

- Devices must be kept in cases when not in use.
- Avoid exposure to sunlight, moisture, and food/drinks.
- Students must purchase their own mouse and

headphones.
- No stickers or decorations are permitted on devices or cases.
- All damage or issues must be reported to IT.
- Travel and Storage
- Permission is required to take devices outside South Australia.
- Lock devices in lockers during recess, lunch, or when not in use.
- Devices must go home each night and be fully charged.

Lost or Damaged Devices

- Lost or found devices must be reported to the IT office.
- Devices left unattended or in unlocked lockers may be confiscated.
- No loan devices are available for students who forget theirs.
- Repeated or serious negligence may result in loss of device privileges.

Identification

- Devices are labelled with a barcode and serial number linked to the student.
- Barcode stickers must remain on the device.

8. End of Year Process

At the end of each school year, all student laptops and chargers must be returned to the school for inspection. This allows the IT Department to check for damage, assess general wear and tear, and carry out any necessary warranty or school-covered replacements. In most cases, **repairs and replacements due to normal use are covered at no cost to families.**

As part of our duty of care, all devices and chargers are also inspected to ensure they continue to meet electrical safety standards for both school and home use.

Test and Tag Process

- All chargers are tested and tagged by a certified technician as part of our annual compliance checks.
- Chargers with expired or missing test and tag labels must be returned to the IT Department for replacement.
- New chargers, typically issued with new laptops in Years 7 and 10, may not have a test and tag label. New electrical equipment may be used without tagging during its initial period, provided it has not previously been used in a workplace and shows no signs of damage.

Important Notes

- Please ensure laptops and chargers are returned in a reasonable condition. General wear and tear will be covered under school warranty processes.
- Deliberate damage, neglect, or misuse may result in a charge for replacement.
- Devices and chargers must be returned by the specified date to ensure timely processing and preparation for the following school year.

9. ICT Privacy Statement

At Rivergum Christian College (RCC), we are committed to protecting the personal information of our students, parents, and staff. We collect, store, and use this information to support learning, wellbeing, and the efficient operation of our school.

Our Student Management System, **TASS**, serves as the central source of truth for all student and family records. TASS is **ISO 27001 certified**, which meets industry standards for data security, and stores all information in secure **Australian-based data centres**.

In addition to TASS, the school makes use of various trusted third-party platforms to deliver essential educational and administrative services. These platforms include Microsoft 365, Apple School Manager, Google Workspace for Education, and a range of learning, wellbeing and administration applications. Where required to deliver their function, these platforms may store or process limited student and parent data—such as names, contact details, student IDs, or learning activity.

RCC takes due care and diligence in selecting and reviewing these third-party services and where possible ensuring that all data they process stays in Australian based data centres. However, we cannot always guarantee how large corporations will handle the school's data. For example, Microsoft stores core education data—including email, documents, and Teams communications—in secure Australian-based data centres. However, depending on the service or feature in use, limited data may be processed or accessed by Microsoft systems or support staff outside of Australia as per Microsoft terms of service.

Refer to the schools Privacy Policy for further information.

Permissions

Photo and Video

The following is in regards to our photo and video permissions for your child. We take the upmost care ensure that media of your child is safely handled and in accordance with your consent.

We have two levels of permissions:

- Use at School (Internal)
- Use for Marketing (External)

This allows us to take photos and videos of your child and, depending on your selection, use them in the following ways:

School Photo Use at School

This type of consent relates to publishing photographs, film or recording within the school community. The main purpose is to communicate internally to families within the life of the school. This includes the Yearbook.

Student Photo Use for Marketing

This type of consent relates to publishing photographs, film, or recording to the external community. The main purpose is to both communicate with our wider community and to promote the school. All photos published are available externally, including social media and our school newsletter. The school will always endeavour to follow child protection legislation. For example, a child's photo would not be published with their full first and last name to protect them from identification.

Terms of Use for CCTV and Facial Recognition Services

Rivergum Christian College (RCC) is committed to ensuring the safety and security of our students, staff, and property. To support this commitment, we use closed-circuit television (CCTV) systems and a facial recognition system. These technologies are employed solely for the purposes of security, safety, and the prevention of unauthorised use of images, including ensuring that student images are not used for marketing purposes without explicit consent.

1. CCTV Usage

Purpose

Our premises are monitored by CCTV cameras to safeguard our community, deter potential misconduct, and assist in investigations, if necessary.

Notification

Clear signage is posted on and around our property to notify all visitors, students, and staff that CCTV is in operation. By entering our premises, you are deemed to have acknowledged and consented to being recorded for security purposes.

Data Handling

All recordings are securely stored on site at RCC and access is restricted to authorised personnel only. Footage will be retained in accordance with our data retention policies and applicable law.

2. Use of Facial Recognition System

Purpose and Scope:

Facial recognition systems allow us to safely store and manage all our media in one central secure location. Our system features facial recognition system implemented to create a secure profile based on facial features when a photo is uploaded. This feature is used exclusively to verify the identity of students and to ensure that images are not used for marketing or other external purposes without prior and explicit consent.

Consent

As part of our ongoing security measures, RCC will take photographs of students on our premises, which will then be processed using the facial recognition system to create a facial recognition profile. By coming on site and allowing photographs/video to be taken, you consent to the process of having your child's photo taken on school grounds, as well as to the creation, storage, and use of the associated facial recognition profile for the purposes described.

Sensitive Information

The system processes biometric data (i.e., facial features) and associated photographic information, which are classified as sensitive personal data. Such data will be handled in strict accordance with applicable data protection laws.

Data Security and Retention

All facial recognition data is securely stored on site at RCC and is accessible only to authorised personnel for the purposes described herein. Data will be retained only as long as necessary to fulfil its intended purpose or as required by law.

3. Data Privacy and Security

Access and Control

Access to any recorded footage or processed biometric data is limited to individuals with authorised responsibilities for security and safety.

Legal Compliance

RCC complies with all relevant privacy and data protection laws.

Updates to Data Use

Any changes to our use of CCTV or the facial recognition system will be communicated through updated versions of these Terms of Use. Continued use of our services or premises constitutes acceptance of such changes.

4. Limitations of Liability

While we take all reasonable measures to ensure the accuracy and security of the data collected via CCTV and facial recognition, RCC shall not be held liable for any unauthorised access or use of such data resulting from events beyond our control.

While we take every effort to work with external providers, we shall not be held liable for incorrect data use or management on their behalf. Rest assured, we will take every step to mitigate risk.

5. Acknowledgement and Acceptance

By entering our premises or submitting your image via any of our platforms, you acknowledge that you have read, understood, and agreed to the terms outlined above regarding the use of CCTV and the our facial recognition system.

RIVERGUM
CHRISTIAN COLLEGE

Our faith is in Christ

128 Distillery Road
Glossop, SA 5344
08 8583 2304
rivergum.sa.edu.au