Cloncurry State School P-12

Technology/Devices Program

07 4742 8333

administration@cloncurryss.eq.edu.au

https://cloncurryss.eq.edu.au/

CONTENTS

Further Information: Email: tcald46@eq.edu.au

OVERVIEW

Cloncurry State School (P–12) aim to support digital learning, students from Years 3–12 may participate in the school's 1-to-1 device program, using school-approved iPads (years 3 – 9) or Laptops (years 7 – 12). Devices must be used responsibly, solely for educational purposes, and in accordance with the school's ICT Acceptable Use Agreement. Students are expected to keep devices charged daily at school provided charging stations, maintain devices in good condition, and follow all cyber safety guidelines. Parents are responsible for device costs and repairs. Misuse may result in restricted access

Ipads:

From Years 3–6, students use iPads to build digital skills through school-based programs like Office 365, focusing on data entry, safe online practices, NAPLAN preparation, and navigating department platforms with confidence.

In Years 7–9, students expand their digital capabilities by using platforms like OneNote and Microsoft Teams to access curriculum content, complete assessments, and collaborate on classroom projects. They also explore real-world applications of digital technologies, gaining insight into how these tools are used across various industries and careers.

Laptops:

In Years 10–12, students use laptops to access online curriculum, complete senior assessments, and engage in independent study. With access to distance education and digital platforms, they can tailor their learning pathways, explore specialized subjects, and prepare for further education, training, or employment in a connected world

Devices remain the property of Cloncurry State School for a period of 4 years and must remain at school during this time unless specific agreements have been met, at the end of this 4-year period students will be given the opportunity to purchase their device at a lower cost.

Year 12 students or any student finalizing their schooling must be made aware that upon their oneschool changing to a discontinued status they will *no longer be able to access any departmental programs – including school based email addresses.*

Alignment with Queensland Department of Education Policies

Cloncurry State School's 2026 iPad & Laptop Program is designed in accordance with the policies and procedures outlined by the Queensland Department of Education (QDoE). These policies ensure that all ICT practices within schools uphold the highest standards of privacy, security, asset management, and responsible digital citizenship.

The following departmental policies underpin this program:

- Information Management, Privacy and Security Policy
  This policy outlines the responsibilities for protecting personal and sensitive information, ensuring secure access to ICT systems, and maintaining confidentiality across all digital platforms.
  https://ppr.qed.qld.gov.au/pp/information-management-privacy-and-security-policy

- ICT Asset Management Procedure
  This procedure governs the acquisition, use, maintenance, and disposal of ICT assets. It ensures that devices provided to students are managed responsibly and in line with departmental expectations.
  https://ppr.qed.qld.gov.au/pp

- Technology and Information Management Policies
  This category includes a range of policies that support safe and effective use of technology in schools, including acceptable use, consent management, and cyber safety.
  https://ppr.qed.qld.gov.au/

By participating in this program, students and parents acknowledge their responsibilities under these policies and agree to uphold the standards set by both the school and the department

Support Provided by School

- Cloncurry State School's program will support printing, filtered Internet access, and file access and storage while at school as well as technical support for diagnosis of hardware/software issues school owned devices
- We also provide a liaison service with distance education providers and outside school services.

Responsibility for Care of Device

- The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines.
- Responsibility for loss or damage of a device at home, in transit or at school belongs to the student.
- Advice should be sought regarding the inclusion in your home and contents insurance policy for loss and for accidental damage if the laptop is purchased from a store retailer and not via one of our vendor portals.
- Any damage to a device, whether issued to the individual or assigned to another person, may result in the individual being held liable for the costs of repair or replacement.

Software

Main Programs

When a student/parent signs the agreements, the school will provide information and support with respect to the following software packages where agreements have been entered into between Education Queensland and the vendors for the purpose of providing student software for personally owned devices:

- *Microsoft Office* – Every student in Education Queensland schools is entitled to download and install Microsoft Office onto all student devices
- *Adobe Creative Cloud* – Our students can obtain a free license for a range of programs in this suite, if required in their school subjects only. This is organized by liaison with classroom teachers at the beginning of the year and again mid-year.
- *Tracking programs*– In order to minimise risk and in accordance with loss prevention protocols, Computrace tracking software has been installed on all devices. Any suspected theft of a device, or any activation or alert generated by the Computrace system, will be reported to law enforcement authorities for investigation and potential recovery action.

Suggestions of additional software you may wish to install

- *Antivirus software* - Although Windows 11+ devices have *Microsoft Defender* as default virus protection, you may wish to install an alternative antivirus program such as Avast or AVG. Please ensure only 1 antivirus suite is installed – having more than one will cause conflicts. **N.B.** If you install a third-party antivirus, *Microsoft Defender* will automatically "step down"

GENERAL INFORMATION

Responsibilities of Stakeholders Involved in the Program

The School

- Laptop program induction — including information on connection, care of device at school, appropriate digital citizenship and cybersafety
- Network connection at school
- School network and cloud storage
- School email address
- Internet filtering (when connected via the school's computer network)
- Technical support for all students (BYOD limitation as laptop is not school owned)
- Free software - Microsoft Office (all students) and Adobe products (if required in subject)
- Approved online memberships – e.g. Education Perfect, etc.
- Printing facilities and limited print credit
- Provide appropriate charging station per class.
- Asset management- school maintains internal register of all ICT assets and who they are assigned to.

Student

- Participation in specific device program induction
- Acknowledgement that core purpose of device at school is for educational purposes
- Care and safe handling of device
- Appropriate digital citizenship and online safety
- Security and password protection – password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals
- Maintaining a current back-up of data – especially assessment
- Charging of device – it is expected that students make sure their device is charging when placed in stations
- Abiding by intellectual property and copyright laws (including software/media piracy)
- Internet filtering (when not connected to the school's network)
- Ensuring device will not be shared with another student for any reason
- No use of mobile phones to hot-spot to deliberately circumvent the cyber protections put in place for students on campus by Education Queensland

Parents and caregivers

- Acknowledgement that core purpose of device at school is for educational purposes
- Internet filtering (when not connected to the school's network)
- Encouraging and supporting appropriate digital citizenship and cyber safety with child
- Ensuring that the child develops the habit of charging the laptop overnight in readiness for the next day's lessons and remembers to bring the device

Web Filtering

At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the school's *Student Code of Conduct*. (school website)

To protect students (and staff) from malicious web activity and inappropriate websites, Education Queensland operates a comprehensive web filtering system with their schools. Any device connected to the Internet through the school network will have filtering applied.

The filtering system provides a layer of protection to students and staff against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- scams and identity theft

Whilst this filtering approach represents global best-practice in Internet protection measures, despite internal departmental controls to manage content on the Internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Students are required to report any Internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET network must also be reported to the school.

Privately owned devices have access to home and other out of school Internet services which may not include any Internet filtering. Parents/caregivers are encouraged to install a local filtering application (compatible with the school's BYOx network) on the student's device for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate Internet use by students outside the school.

In relation to this, students and parents need to be aware of the following:

- Students are not permitted to hot-spot their phones for Internet connectivity, as this negates the very benefits that are designed to protect them from being vulnerable whilst online at school. Students caught doing this will face consequences.
- It is totally unacceptable for students to download programs onto their computer that are designed to circumvent the filtering protection provided by Education Queensland on the school campus.
- Using VPN (Virtual Private Network) software **will** conflict with the school wireless connectivity process – i.e. they will not be able to access the Internet or necessary network drives whilst on campus.

Digital Citizenship

- Students should be conscious creators of the content and behaviors they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

- Students should be mindful that the content and behaviors they have online are easily searchable, accessible and may form a permanent online record into the future.

- Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioral guidelines, such as when in a class or the broader community.

- Parents are requested to ensure that their child understands this responsibility and expectation. The school's behavior policies also support students by providing school related expectations, guidelines and consequences.

Data Security and Back-ups

- Students must understand the importance of backing up data securely. Should a hardware or software fault develop, important assignment work may be lost.
- The student is responsible for the backup of all data. While at school, students are able to save data to the school's network which is safeguarded by a scheduled nightly backup and therefore strongly encouraged as the most reliable form of backup.
- Education Queensland also provides every student with approximately 2TB of secure cloud storage (*OneDrive*) which of course is accessible on and off campus.
- Whilst other forms of back-up such as USB drives, external hard drives are an option, these do not have the security and reliability of *OneDrive* and the school server. They are volatile in the sense that they can be damaged, data corrupted and are easily misplaced.
- Students who are part of the school iPad/laptop program should also be aware that in the event that any repairs need to be carried out on the laptop relating to the hard drive, data stored on the laptop could be lost.

Acceptable Computer and Internet Use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the relevant policies of Education Queensland.

Communication through internet and online communication services must comply with the *Student Code of Conduct* available on the school website.

There are conditions that students are required to adhere to. Students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- use unauthorized programs or intentionally download unauthorized software, graphics or music
- intentionally damage or disable computers, computer systems or Queensland DET networks
- use the device for unauthorized commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of Internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

- Passwords must not be obvious or easily guessed; they must be kept confidential, and changed when prompted or when known by another user.
- Student Passwords must be 10 digits long, contain at least; one capital letter, one lower case letter, one number, and one symbol. Passwords containing user's name or chronological letters or numbers will not be accepted.
- Personal accounts cannot be shared. Students should not allow others to use their personal account for any reason. Students should log off at the end of each session to ensure no one else can use their account or laptop.

Cyber-safety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver as soon as is possible.

Students must also seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Bullying Reporting – All students are strongly encouraged to report any incidents of online or physical bullying. Reports can be also made confidentially through Stymie at https://about.stymie.com.au/. The school takes all reports seriously and will take appropriate action in line with its anti-bullying policy.

Students are also encouraged to explore and use the '*Cyberbullying help button*' on school devices to talk, report and learn about a range of cyber safety issues. Cyber safety is also addressed in Futures lessons throughout the year.

Students must never initiate or knowingly forward emails, or other online content, containing:

- a message sent to them in confidence
- a computer virus or attachment that is capable of damaging the recipient's computer
- chain letters, hoax emails or phishing emails
- spam (such as unsolicited advertising).

Students must never send, post or publish:

- inappropriate or unlawful content, which is offensive, abusive or discriminatory
- threats, bullying or harassment of another person
- sexually explicit or sexually suggestive content or correspondence
- false or defamatory information about a person or organization.

Misuse and Breaches of Acceptable Usage

- Students should be aware that they are held responsible for their actions while using the Internet and online communication services.
- Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access Internet and online communication services.
- The school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, Internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users.
- The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible Use

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

- Portable devices on campus should be primarily used for engagement in class work and assignments set by teachers, conducting general research for school activities and projects and communicating or collaborating with other students, teachers, parents, caregivers or experts for educational purposes.
- Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.
- Parents and caregivers need to be aware that damage to portable devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's behavior policies.
- The school will educate students on cyber bullying, safe Internet and email practices. Students have a responsibility to incorporate these safe practices in their daily behavior at school.
- All material on the device is subject to audit by authorized school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.

When using any device, students **MUST NOT**:

- use the device in an unlawful manner
- create or participate in circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or Internet filtering that have been applied as part of the school standard
- download (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory/derogatory or bullying language
- download viruses/other programs capable of breaching the Department's network security
- use the mobile device's camera or recording functions inappropriately, violating the privacy of other individuals
- covertly use Bluetooth functionality during lessons or exams
- hotspot their phone to bypass the school's protective filtering designed to ensure cyber safety
- at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission.

Data Breach Protocols and Monitoring Tools

Cloncurry State School is committed to protecting the privacy and security of student and staff information in accordance with the Queensland Department of Education's **Information Management, Privacy and Security Policy**. In the event of a suspected or confirmed data breach, the school will follow a structured response protocol to ensure timely containment, investigation, and reporting.

Breach Response Process

1. **Detection and Reporting**
    - Any suspected breach (e.g. unauthorized access, data loss, or exposure of personal information) must be reported immediately to the school's ICT Coordinator or Principal.
    - Students and staff are encouraged to report breaches via email or in person and may also use confidential reporting platforms such as Stymie.
2. **Initial Assessment**
    - The school will assess the nature and scope of the breach, including the type of data involved, affected individuals, and potential risks.
3. **Containment and Mitigation**
    - Access to affected systems or devices may be restricted.
    - If applicable, location tracking software (e.g. Computrace) will be activated to assist in recovery of lost or stolen devices.
4. **Notification**
    - Affected individuals will be notified as soon as practical.
    - The breach may be escalated to the Department's Cyber Security Unit and/or law enforcement if required.
5. **Review and Prevention**
    - The school will conduct a post-incident review to identify root causes and implement measures to prevent recurrence.
    - Updates to protocols and staff/student training may follow.

Monitoring and Classroom Management Tools

To support safe and secure digital learning environments, the school uses the following tools:

- **Location Monitoring Software**
  All school-owned devices are equipped with Computrace or equivalent tracking software to assist in theft prevention and recovery.
- **Classroom Management Software**
  Teachers may use classroom management platforms to monitor student activity during lessons, ensuring appropriate use of devices and adherence to curriculum tasks. These tools allow for:
    - Real-time viewing of student screens
    - Restriction of access to non-educational content
    - Messaging and guidance during class activities

These tools are used strictly for educational and safety purposes and comply with departmental privacy and security standards.

Privacy and Confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's device. Students must not trespass in another person's files, home drive, email or accessing unauthorized network drives or systems.

Additionally, students should not divulge personal information via the Internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

Intellectual Property and Copyright

Students should never plagiarize information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the Internet or Intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws and be subject to prosecution from agencies to enforce such copyrights.

PARENTAL CONFIRMATION FOR 2026

For the commencement of each school year, all parents/carers and students will be required to complete this information/consent form which will can be reviewed on the School's Website.

Acknowledgement and Agreement

I have read and understood the terms, conditions, and responsibilities outlined in this document. I acknowledge that failure to comply with these requirements may result in consequences as described, and I agree to abide by the policies and procedures stated herein.

By signing below, each party confirms that the information provided is accurate, that they understand their obligations, and that they accept the terms of this agreement.

Student Name: .....

Grade Level: .....

Student Signature: .....

Date: .....

Parent/Carer Name: .....

Relationship to Student: .....

Parent/Carer Signature: .....

Date: .....

Principal Name: .....

Principal Signature: .....

Date: .....

Deputy Principal Name: .....

Deputy Principal Signature: .....

Date: .....

Note: This agreement is a binding acknowledgement between the student, the student's parent/carer, and the school. All parties should retain a copy for their records.

Introduction to the Online Services Consent Form for Cloncurry State School P-12

Our school uses tools and resources to support student learning, including third party (non-departmental) online services hosted and managed outside of the Department of Education network.
Online services, including websites, web applications, and mobile applications, are delivered over the internet or require internet connectivity. Examples may include interactive learning sites and games, online collaboration and communication tools, web-based publishing and design tools, learning management systems, and file storage and collaboration services.
This letter is to inform you about the third-party online services used in our school and how your child's information, including personal information and works, may be recorded, used, disclosed, and published to the services (if you provide your consent for this to occur).
The Online Services Consent Form is a record of the consent provided.
About the online services: After evaluation, the principal has deemed specific third-party online services appropriate for school use. These online services are listed on the consent form.

Third party online service providers are external to the school, and the services may be hosted onshore in Australia or offshore outside of Australia. Data that is entered into offshore services may not be subject to Australian privacy laws. When considering whether to provide your consent, we encourage you to read the information provided about each online service, including the terms of use and privacy policy, which outline how information and works will be used and under what circumstances they may be shared.

Student information

The consent collected by the form covers both student personal information (e.g. name, date of birth) and school-based information (e.g., student username, email, year level) as outlined on the form.
Where permitted by the service provider, de-identified information will be used and/or efforts will be made to limit the amount of personal information disclosed and stored within online services (e.g., when registering accounts, only mandatory information will be disclosed).

Student works

Works might include materials such as student projects, assignments, portfolios, images, video or audio. Where student works will be created within, stored or published to the online service (in some cases, published information or works will be viewable by the public), this will be indicated in 'additional consent requirements' in Section 5 of the Online Services Consent Form.

Parent information

Where your personal information (e.g. parent email, name, contact details) will be disclosed to the online service, this will be indicated in the additional consent requirements in Section 5 of the Online Services Consent Form.

Purpose of the consent

Third party online services are used for various purposes. The purpose of use for each service is outlined in Section 5 of the Online Services Consent Form. For example, teachers may use online services with students to support curriculum delivery, complete learning activities and assessment, facilitate class collaboration, and create and publish class work (e.g. projects, assignments, portfolios). The Online Services Consent Form records your consent for your child to register accounts, use, and, where specified, publish their work to these services. The form also collects your consent for school staff to collect, store, and transmit information to online services in order to manage school operations and communicate with parents and students.
It should be noted that, in some instances, the school may be required or authorised by the Education (General Provisions) Act 2006 (Qld) or by law to record, use or disclose the student's personal information or materials without consent.

Voluntary consent provision

It is not compulsory to provide consent. If your consent is not given, this will not adversely affect any learning opportunities provided by the school to your child.

Consent may be limited or withdrawn

You can withdraw your consent at any time by notifying the school in writing (by email or letter). The school will confirm the receipt of your request via email if you provide an email address. You may also limit your consent by providing consent for some, but not all, online services listed on the form. Requests to limit consent in relation to how the 'Information covered by this consent form' and the 'Approved purpose' (Section 2 and 3 of the form) are applied to a specific service, will be treated as "do not consent", as the school cannot guarantee correct implementation of individual requests.
Due to the nature of the internet, it may not be possible for all copies of information (including images and student works that have already been disclosed or published) to be deleted or restricted from use if you request it. The school may remove content that is under its direct control, however, information and works that have

already been disclosed and published cannot be deleted, and the school is under no obligation to communicate changes to your child's consent circumstances to online service providers.

Duration of consent

The consent applies for the period of time specified on the form. You may review and update your consent at any time by notifying the school in writing (by email or letter).

There may be circumstances where the school issues a new consent form to seek additional consent e.g. in the event that new online services are identified for use.

Who to contact to return the form, express a limited consent, withdraw consent or ask questions regarding consent, please contact:

IT Support, 07 4742 8331, email: admin@cloncurryss.eg.edu.au

Online Services Consent Form

Privacy Notice

The Department of Education is collecting the personal information on this form in order to obtain consent regarding the use of online services. This information and completed form will be stored securely. Personal information collected on this form may also be used by or disclosed to third parties by the Department where authorized or required by law. If you wish to access or correct any of the personal information on this form, or discuss how it has been dealt with, please contact your student's school in the first instance.

This form is to be completed by:

- A Parent/carer (*); or
- A student over 18 years; or
- A Student with independent status.

(*Note: Where a student who is under 18 years is able to consent, they may also provide consent in addition to the parent.)

1. IDENTIFY THE PERSON TO WHOM THE CONSENT RELATES

a. Full name of student_____

2. INFORMAT/ON COVERED BY THIS CONSENT FORM

The consent collected by the form covers the following student personal information (identifying attributes):

i. Student name (first name and/or last name)
ii. Sex/Gender
iii. Date of Birth, age, year of birth

AND the following school-based information (generally, non-identifying attributes*): Student school username

i. Student school email
ii. Student ID number
iii. School
iv. Year Group
v. Class
vi. Teacher
vii. Country

*In cases where registration and/or use requires a combination of school-based information (non- identifying) and personal information, or a combination of school-based information, the school-based information may become identifiable.

- If an online service records, uses, discloses and/or publishes student works, parent information or additional student information (such as photographs of students), not listed above (Section 2a.), the school will specify it as part of the additional consent requirements on the form. Examples may include:
  - Student assessment
  - Student projects, assignment, portfolios
  - Student image, video, and/or audio recording
  - Sensitive information (e.g., medical, wellbeing)
  - Name and/or contact details (e.g. email, mobile phone number) of student's parent

3. APPROVED PURPOSE

This form records your consent for the recording, use, disclosure and publication of the information listed in item 2 above, and any information or student works listed under the 'additional consent requirements', and to transfer this information and works within Australia and outside of Australia (in the case of offshore services) to the online service providers for the following purposes:

- For your child to register an account for the online services

- For your child to use the online services in accordance with each service's terms of use and privacy policy 0ncluding service provider use of the information in accordance with their terms of use and privacy policy)
- For the school to:
    - administer and plan for the provision of appropriate education, training and support services to students,
    - assist the school and departmental staff to manage school operations and communicate with parents and students.

4. TIMEFRAME FOR CONSENT

The consent granted by this form is for the duration of the student's current phase of learning (i.e. Years P-3, 4-6, 7-9 and·10-12). Consent is obtained upon enrolment and renewed when students move into a new phase of learning (e.g. minimum every four years).

CONSENT FOR ONLINE SERVICES

For each online service listed below, please indicate your choice to give consent to not give consent for the information outlined in Section 2 to be disclosed to the online service in accordance with the purpose outlined in Section 3, and for the timeframe specified in Section 4**.**

Name of Provider: ClassDojo
Type of Service: Class Dojo is a behaviour monitoring website for students which enables parents to track student progress.
Website: https://www.classdojo.com/
Terms of Use: https://www.classdojo.com/en-gb/terms/
Privacy Policy: https://www.classdojo.com/en-gb/privacy/
File Storage: Cloud based servers in the USA.

Name of Provider: Reading Eggs
Type of Service: Early childhood online literacy and numeracy program
Website: https://readingeggs.com.au/
Terms of Use: https://readingeggs.com.au/terms
Privacy Policy: https://readingeggs.com.au/privacy
File Storage: Cloud based server in the USA.

Name of Provider: Clickview
Type of Service: Online video and resourcing learning platform
Website: https://www.clickview.net/
Terms of Use:
https://www.clickvieweducation.com/en-au/legal/terms-and-conditions
Privacy Policy:
https://www.clickvieweducation.com/en-au/legal/privacy-policy
File Storage: Australia and USA based file servers

Name of Provider: Mosyle Manager
Type of Service: iPad service provider and mobile device manager
Website: https://school.mosyle.com/
Terms of Use:
https://school.mosyle.com/legal/terms
Privacy Policy:
https://school.mosyle.com/legal/privacy
File Storage: Cloud based server in the USA

Name of Provider: SmartLab
Type of Service: Literacy and Numeracy, science and mathematics diagnostics and learning platform
Website: https://www.mysmartlab.com.au/
Terms of Use:
https://www.mysmartlab.com.au/terms-of-service/
Privacy Policy:
https://www.mysmartlab.com.au/privacy-policy/
File Storage: Cloud based server in the Australia and Microsoft Azure

---

Name of Provider: Scratch
Type of Service: Scratch.mit is a website teaching instructional coding.
Website: https://www.scratch.mit.edu
Terms of Use:
https://scratch.mit.edu/terms_of_use
Privacy Policy:
https://scratch.mit.edu/privacy_policy/
File Storage: Local storage on school server.

Name of Provider: Literacy Planet
Type of Service: Literacy Planet is a fun and engaging online learning resource for progression in Literacy.
Website: https://www.literacyplanet.com
Terms of Use:
https://literacyplanet.com/au/about/privacy-policy/parents-terms
Privacy Policy:
https://www.literacyplanet.com/au/about/privacy-policy/
File Storage: Cloud based servers in Sydney, Australia

Name of Provider: Mathseeds
Type of Service: Mathseeds is used to teach core maths and problem-solving skills.
Website: https://mathseeds.com.au
Terms of Use: https://readingeggs.com/terms
Privacy Policy: https://readingeggs.com/privacy
File Storage: Cloud based servers in the USA.

Name of Provider: Canva
Type of Service: Canva is an online design and publishing tool
Website: https://www.canva.com/
Terms of Use: https://readingeggs.com/terms
Privacy Policy:
https://www.canva.com/policies/privacy-policy/
File Storage: Cloud based servers in the USA and any country with Canva subsidiaries or affiliates, including Australia.

Name of Provider: Minecraft Education
Type of Service: Canva is an online design and publishing tool
Website: https://education.minecraft.net/en-us
Terms of Use: https://edusupport.minecraft.net/hc/en-us/articles/4405348643092-Minecraft-Education-End-User-License-Agreements-EULA
Privacy Policy: https://www.microsoft.com/en-gb/privacy/privacystatement
File Storage: Microsoft Azure

Name of Provider: Stymie
Type of Service: Online anonymous reporting system
Website: https://about.stymie.com.au/
Terms of Use: https://about.stymie.com.au/terms-of-use/

Privacy Policy:
https://about.stymie.com.au/privacy-policy/
File Storage: Microsoft Azure

Name of Provider: Youtube (only available for distance ed. students ages 16+)
Type of Service: Video sharing platform
Website: https://www.youtube.com/
Terms of Use: https://www.youtube.com/t/terms
Privacy Policy:
https://policies.google.com/privacy?hl=en-GB
File Storage: Cloud based google server

Name of Provider: Quizlet
Type of Service: interactive flash cards, practise tests and study games
Website: https://quizlet.com/au
Terms of Use: https://quizlet.com/tos
Privacy Policy: https://quizlet.com/privacy
File Storage: Cloud based servers in the USA

Name of Provider: Risk Assess
Type of Service: online risk assessment tool for primary and secondary schools
Website: https://www.riskassess.com.au/
Terms of Use:
https://www.riskassess.com.au/info/terms
Privacy Policy:
File Storage: Cloud based server in Australia

Name of Provider: Food allergy Training
Type of Service: online risk assessment tool for primary and secondary schools
Website: https://foodallergytraining.org.au/
Terms of Use:
https://foodallergytraining.org.au/mod/page/view.php?id=22
Privacy Policy:
https://foodallergytraining.org.au/mod/page/view.php?id=20
File Storage: Cloud based google server

Name of Provider: Gimkit
Type of Service: Online revision games
Website: https://www.gimkit.com/
Terms of Use: https://www.gimkit.com/terms-of-service
Privacy Policy: https://www.gimkit.com/privacy
File Storage: US based database

Name of Provider: Kahoot
Type of Service: Online revision games
Website: https://kahoot.it/
Terms of Use: https://trust.kahoot.com/terms-and-conditions/?utm_name=controller_app&utm_source=controller&utm_campaign=controller_app&utm_medium=link&lang=en
Privacy Policy: https://trust.kahoot.com/privacy-policy/?utm_name=controller_app&utm_source=controller&utm_campaign=controller_app&utm_medium=link&lang=en
File Storage: Cloud based server in the USA

Name of Provider: Blooket
Type of Service: Online revision games
Website: https://www.blooket.com/
Terms of Use: https://www.blooket.com/terms
Privacy Policy: https://www.blooket.com/privacy
File Storage: Cloud based server in the USA

Name of Provider: Phet simulations
Type of Service: interactive science and math simulations
Website: https://phet.colorado.edu/
Terms of Use:
Privacy Policy:
https://phet.colorado.edu/en/privacy-policy
File Storage: Online SSL

Name of Provider: My QCE
Type of Service: Curriculum and assessment
Website: https://myqce.qcaa.qld.edu.au/
Terms of Use:
https://myqce.qcaa.qld.edu.au/disclaimer
Privacy Policy:
https://myqce.qcaa.qld.edu.au/privacy
File Storage: Department of education QLD

Name of Provider: Quartex (evolution mining)
Type of Service: Industry onboarding
Website: https://quartexsoftware.com/
Terms of Use:
Privacy Policy:
https://quartexsoftware.com/privacy-policy/
File Storage: Australian based servers

Name of Provider: Ausport
Type of Service: Online referencing and sporting pathways
Website: https://www.ausport.gov.au/
Terms of Use:
Privacy Policy:
https://www.ausport.gov.au/legal_information/privacy_policy
File Storage: Australian Based Database

Name of Provider: Adobe creative cloud
Type of Service: toolkit
Website: https://www.adobe.com/au

Terms of Use:
https://www.adobe.com/au/legal/terms.html
Privacy Policy:
https://www.adobe.com/au/privacy.html
File Storage: Cloud based server in the USA

Name of Provider: Pearson
Type of Service: resources and textbooks
Website: https://www.pearsonplaces.com.au/
Terms of Use: https://www.pearson.com/en-au/legal/terms-of-use.html
Privacy Policy: https://www.pearson.com/en-au/privacy-center.html
File Storage: London based database

Name of Provider: Oxford
Type of Service: resources and textbooks
Website: https://www.oxforddigital.com.au
Terms of Use:
https://www.oxforddigital.com.au/terms.html
Privacy Policy:
https://www.oxforddigital.com.au/privacy.html
File Storage: Cloud based google server

Name of Provider: Cambridge
Type of Service: resources and textbooks
Website: https://www.cambridge.org/go/
Terms of Use:
https://www.cambridge.org/legal/website-terms-of-use
Privacy Policy:
https://www.cambridge.org/legal/privacy
File Storage: Cloud based storage in UK

Name of Provider: Grok Academy
Type of Service: Online Coding tool
Website: https://groklearning.com/
Terms of Use:
https://groklearning.com/policies/terms/
Privacy Policy:
https://groklearning.com/policies/privacy/
File Storage: Cloud based server in Australia

Name of Provider: Hour of Code
Type of Service: Coding resources
Website: https://hourofcode.com/au
Terms of Use: https://code.org/en-US/terms-of-service
Privacy Policy: https://code.org/en-US/privacy
File Storage: Cloud based server in the USA

Name of Provider: Onguard
Type of Service: training and safety - machinery
Website: https://onguardv3.com.au/
Terms of Use:
https://onguardv3.com.au/manage/license-agreement
Privacy Policy:
https://onguardv3.com.au/manage/license-agreement
File Storage: Australian based Database

Name of Provider: Cengage
Type of Service: Online textbooks and ebooks
Website: https://au.cengage.com/
Terms of Use:
https://au.cengage.com/student/terms-of-service/
Privacy Policy: https://au.cengage.com/privacy/
File Storage: EU based databases

Name of Provider: Dibels
Type of Service: Measuring and assessing the acquisition of literacy skills
Website: https://dibels.amplify.com/
Terms of Use:
amplifycom.wpengine.com/customer-terms
Privacy Policy: https://amplify.com/customer-privacy/
File Storage: US cloud based server and google based servers

Name of Provider: Maths Online
Type of Service: Revision for mathematics
Website: https://www.mathsonline.com.au/
Terms of Use:
https://www.mathsonline.com.au/terms-conditions
Privacy Policy:
https://www.mathsonline.com.au/privacy-policy
File Storage: Aus based servers

Name of Provider: DayMap
Type of Service: Communications and school management system
Website: https://daymap.net/
Terms of Use:
https://www.mathsonline.com.au/terms-conditions
Privacy Policy: https://daymap.net/privacy-policy/
File Storage: Microsoft Azure

Third Party Website Consent Agreement

Student's name: _____ Year level: _____
Please **tick your box of choice** for your child's information being provided to each of the third-party providers for the provision of an educational service.

	Do consent / Do not consent
Class Dojo	☐ / ☐
Reading Eggs	☐ / ☐
ClickView	☐ / ☐
Scratch.mit	☐ / ☐
Mosyle MDM	☐ / ☐
Mathseeds	☐ / ☐
Literacy Planet	☐ / ☐
Minecraft Education	☐ / ☐
SmartLab	☐ / ☐
Canva	☐ / ☐
Stymie	☐ / ☐
Youtube	☐ / ☐
Food Allergy Training	☐ / ☐
Quizlet	☐ / ☐
Risk Assess	☐ / ☐
Gimkit	☐ / ☐
Kahoot	☐ / ☐
Blooket	☐ / ☐
Phet	☐ / ☐
My QCE	☐ / ☐
Quartex	☐ / ☐
Ausport	☐ / ☐
Adobe	☐ / ☐
Pearson	☐ / ☐
Oxford	☐ / ☐
Cambridge	☐ / ☐
Grok Academy	☐ / ☐
Hour of Code	☐ / ☐
Onguard	☐ / ☐
Cengage	☐ / ☐
Maths Online	☐ / ☐
Dibels	☐ / ☐
Daymap	☐ / ☐

As a parent or guardian of this student, I have read the terms of use and privacy policy of each of the websites listed. I understand that my student's personal information will be provided to these third-party software providers for the purpose of my student's registration and use of the software programs and some of this information may be stored outside of Australia.

_____ _____
Parent/Guardian's Name Parent/Guardian's Signature

____/____/____
Date