Corinda State High School

BYOD Handbook 2026

Contents

Welcome to BYOD at Corinda

Corinda State High School aims to strengthen its *future focused* vision with the use and integration of technology. Our school's goal is to embed the use of rich interactive technologies to transform and support teaching and learning in the classroom. Our focus is to use technology to develop digital wisdom through collaborative creation, risk-taking, and the construction of deep understanding.

Our BYOD program has revolutionised learning at Corinda State High School, with its benefits evident across the school. These include:

- Learning that is portable, personal, collaborative, interactive and differentiated
- Learning that can be delivered anywhere at any time
- Learning that creates a much stronger connection between school and home

As a result, personal ICT devices are a key enabler for these learning experiences and have never been more vital to the student. Achieving a 1:1 ratio of student to device delivers greater consistency in the shift towards a contemporary learning environment and experience.

In order to facilitate this program, our students and their families are encouraged to purchase or bring their own device that meets the minimum specifications to use in the classroom.

What is BYOD?

Bring Your Own Device is a term used to describe a digital device ownership model where; students use their privately-owned devices to access the departmental networks and information management systems in an educational setting. BYOD allows for students in Years 7 – 12 to purchase their own laptop and use it at school. The program provides students with access to part of the school network, Internet, printing, digital textbooks and other educational platforms.

BYOD Support

To support the implementation of the BYOD program the school has provided dedicated charging stations, classroom support with IT technicians, the Hot-Swap laptop loan program and partnerships with carefully selected providers to assist parents with their decision making and technical needs.

All students' devices which are purchased for use in the school must meet the Software & Hardware requirements of the school (detailed further on in this document). All student devices must also be enrolled into Department of Education's InTune - This ensures it meets the minimum security specifications which allows the device to be set up for use within the school's network.

Parents and students are welcome to forward queries regarding support to school IT technicians at byodsupport@corindashs.eq.edu.au.

Using a Device at School

To use the device at school it is required that the device be set up and connected to the school's network. This provides students with secure access while working on the school network. Students are required to follow school policy for ICT use while on school grounds.

"Students will be safe, ethical, lawful, courteous, respectful, and conducive to good order of the school and the community."

Student devices are required to have up-to-date anti-virus and security software installed. All other software on the device must be licensed, and be for educational purposes. A licensed copy of Microsoft Office is available free to all QLD state school students (refer to school website).

The Executive Principal reserves the right to deny any student access to the school's network for any breaches of the school ICT policy.

BYOD Inclusions

The Technology Service Fee covers the Administering of BYOD Policy. This includes:

- Access to Printers and Photocopiers.
- Hot-Swap - this is a replacement school laptop for use while the student's personal device is being repaired (conditions apply)
- Access to specialist technologies such as (but not limited to) 3D Printers, Laser Cutters and Virtual Reality experiences.
- Additional technical support including:

SOFTWARE	HARDWARE
✓ Provide troubleshooting for any device that meets minimum requirements: Microsoft (Windows 11) or Apple (macOS) ✓ Advise 'best option' for repair of problem ✓ Provide assistance for school connectivity issues ✓ Provide support for school allocated software	✓ Provide support in fault diagnosing/warranty/ADP logging ✓ Non-warranty damage identification, possible cost associations and 'best option' suggestions ✓ Drop off point at ICT room for BYO repairs with third parties (family to arrange the repair at Corinda SHS)

Minimum Hardware & Software Requirements – Selecting a BYOD Device

Before acquiring a device to use at school, parents/caregivers and students should be aware of Corinda State High School's minimum hardware, operating system and software requirements. These specifications relate to the suitability of the device for class activities, student needs, and promoting a safe and secure access to the school's network.

Corinda State High School recommends that all devices used by students meet the minimum specifications outlined in this document to enable suitability for curriculum-based activities. Corinda State High School ICT technicians will make every effort to enable connectivity of devices that meet these minimum specifications, assuming there are no technical or other issues outside their control.

Be aware specific graphic intensive subjects such as Visual Arts, Multimedia or Industrial Graphics and Design subjects may require a device with higher performance standards. If your student is enrolled in these subjects, please contact the Head of Department for the subject or the ICT Team for more specific information. For more information regarding the BYOD program visit the school's website: https://corindashs.eq.edu.au/curriculum/bring-your-own-device

MINIMUM HARDWARE REQUIREMENTS FOR BYOD DEVICE

Years 7 to 12 Laptop

WINDOWS LAPTOP

- ☐ Windows 11 and above (NOT Windows 11S)
- ☐ 64bit capable CPU
- ☐ Dual Band Wireless (capable of 5GHZ Wireless)
- ☐ 8 GB RAM
- ☐ Minimum 128GB SSD

MAC LAPTOP

- ☐ MAC OS Big Sur and above
- ☐ Dual Band Wireless (capable of 5GHZ Wireless)

ESSENTIAL ACCESSORIES

- ☐ Protective Case for your laptop - Consider a "ruggedized" case

RECOMMENDED ACCESSORIES

- ☐ Accident Protection Insurance (with purchase or check your Home and Contents Insurance Policy)

HARDWARE RECOMMENDED FOR HIGHER PERFORMANCE

Visual Arts, Media, Engineering and Design subjects

Years 10 to 12 Laptop

WINDOWS LAPTOP	MAC LAPTOP
☐ Windows 11 and above (NOT Windows 11S) ☐ 64bit capable CPU ☐ Dual Band Wireless (Capable of 5GHZ Wireless) ☐ 8 GB RAM or higher ☐ 256GB SSD or higher ☐ Dedicated Video Card 2GB memory or higher	☐ MAC OS Big Sur and above ☐ Dual Band Wireless (capable of 5GHZ Wireless)

ESSENTIAL ACCESSORIES

☐ Protective Case for your laptop - Consider a “ruggedized” case

RECOMMENDED ACCESSORIES

☐ Mouse (wireless or corded)
☐ Accident Protection Insurance (with purchase or check your Home and Contents Insurance Policy)

We highly recommend to take this checklist with you when you are purchasing your device.

Click here for BYOD online shopping and vendor catalogues:
https://corindashs.eq.edu.au/curriculum/bring-your-own-device/purchasing-a-b-y-o-d-laptop

CORINDA STATE HIGH SCHOOL

MINIMUM SOFTWARE REQUIREMENTS FOR BYOD DEVICE

Years 7 to 12 Laptop

- ☐ Microsoft Office 365 – available for five free downloads (*)
  Possible to self-install, however ICT Staff can help install this software.
  Download via http://portal.office.com - Use your student ID and password to login.
  Windows Version contains:
  Word, Excel, PowerPoint, Access, Publisher, Outlook, OneNote, OneDrive & Teams.
  Mac Version contains:
  Word, Excel, PowerPoint, OneNote, OneDrive & Teams.

- ☐ PDF Reader –
  Possible to self-install, however ICT Staff can help install this software.
  Windows and Macs have built in PDF Readers.
  Recommended to install Adobe Reader (Free to download).
  https://acrobat.adobe.com/au/en/acrobat/pdf-reader.html

- ☐ Anti-Virus Software –
  Windows can use the free built in "Defender".
  Macs can use the free built in "XProtect".
  Recommended to install an additional Anti-Virus software.
  You can use a free or a paid Anti-Virus, but do not use a Trial of a paid Anti-Virus as these can become out-of-date when Trial ends.

- ☐ PaperCut Print Deploy (*) –
  Possible to self-install, however ICT Staff can help install this software.
  https://qedu.sharepoint.com/sites/2055/students/byod/SitePages/Papercut-for-BYOD.aspx - Use your student ID and password to login

(*) – Note must have EQ MISD Email address to login to download software

Responsibilities of Stakeholders: Students, Parents/Caregivers and the School

Corinda State High School will provide:

- BYOD program induction — including information on connection, care of device at school, appropriate digital citizenship and cybersafety.
- Network connection at school.
- Internet filtering (when connected via the school's computer network).
- Technical support.
- Printing facilities.

Students will:

- Participate in a BYOD induction program.
- Back up files by saving data to OneDrive.
- Charge device via appropriate methods.
- Abide by intellectual property and copyright laws (including software/media piracy).
- Ensure personal login account will not be shared with another student, and device will not be shared with another student.
- Not tell another student any of their passwords.
- Understand and sign the BYOD agreement.

Parents / Caregivers will provide:

- Internet filtering (when **NOT** connected to the school's network).
- Adequate warranty and insurance of the device.
- A protective case for the device.

Technical support, Licenses and Software

School technical support provided

All maintenance for the IT device, operating system, software and/or apps purchased by the family are the responsibility of the family. Corinda State High School will provide support to students on the BYOD program with assistance/advice on school required applications, configuration, and resolution of simple issues.

However, at no time can the school take responsibility for the BYOD device, data, backups, or its repair in any form.

BYOD repairs and school owned 'Hot-Swap' laptops

The school operates a device lending 'Hot-Swap' system to support student's learning in the event the student's laptop is damaged and requires a repair.

While the Hot-Swap device is on loan to the student, it remains the property of the school at all times. At the end of each school term, or at such time as the student ceases to be enrolled at Corinda State High School, the device must be checked-in with the school's ICT Support staff. If the device is not returned, financial compensation will be sought, and a property theft report will be submitted to police.

BYOD repairs Drop-In and Check-out procedure

The school provides a service for the student's BYOD device to be checked-in with the ICT Support area for repair by a third-party repairer. The repairer can then attend the school to repair the device. Such arrangements with a third-party repairer are solely the responsibility of the parent/carer and is to be organised prior to checking-in the device with ICT Support staff. School ICT Support staff will not organise the repair on behalf of the parent/carer.

Repairs fees for Hot-Swap laptops

School owned laptops are the property of the Department of Education and incur charges if damaged by the student whilst on loan. All costs associated with non-warranty repair of computer will be covered by the student and their parent/carer. Any damage that is accidental, malicious, negligent or intentional is considered a non-warranty repair.

Where possible, the school will claim Accidental Damage Protection (ADP) repairs on a device – in those instances the ADP excess fee will be passed onto the student and their parent/carer. ADP excess fees increase per "repair instance" as below:

- 1st ADP repair instance = $50
- 2nd ADP repair instance = $100
- 3rd (or more) ADP repair instance = $150

The cost of all non-warranty repairs that cannot be claimed as ADP, will vary depending on the computer model and the repair required. The school will arrange repair with a school allocated repair agent. Excluding full replacement of computer, indicative repair costs as of

August 2025 are $300 to $600 depending on computer model. These prices can change due to part availability and circumstances.

Security of BYOD – Damage / Theft Insurance

All BYOD laptops and devices must be marked with the student's name. We recommend that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact and disruption to learning should a device not be operational.

The student is responsible for taking care of and securing the device and accessories. Responsibility for loss or damage of a device at home, in transit or at school remains with the student. The school cannot be held liable for any damage or replacement costs incurred while the device is at school or travelling to and from school. This also includes any damage that may occur from staff or students tripping over device charging cables (charging in classrooms is prohibited and considered a breach of the school's student policy for ICT use).

Web Filtering

The Department od Education has a responsibility in ensuring the safety of students while using the internet at school and on any school-provided device. Personally owned BYOD laptops using non-school networks (Home, personal hotspots, etc) will not be protected by the school's web filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for such times the device is Internet connected in locations other than school. Parents/caregivers are responsible for appropriate Internet use by students outside the school.

Through the school's internet filtering system Symantec WebFilter, the type of content that students may be exposed to while online is restricted by the system's website categorisation process.

The department ensures websites and web applications are blocked if they are inappropriate, malicious, illegal, dangerous or conflict departmental policy. Students can speak with their teacher if they believe an evaluation of a website or web application should be completed.

Parents are reminded that filtering and monitoring systems are not foolproof and do not replace the need for parental supervision when children are online. Vigilance is vital regardless of the device your child is using to access the internet.

There are a number of online resources for parents and caregivers to help support their child's online experiences.

- eSafety Parents
- Cybersafety in Queensland state schools

Please remember, as a parent or caregiver you play an important role in helping your children have safe and positive experiences online. Be vigilant and keep an eye on what your child is doing.

Charging of Devices

All BYOD laptops and devices must be fully charged and ready for learning at the start of each school day. Charging in classrooms or other areas (that are not clearly designated as a charging area) is prohibited and considered a breach of the school's student policy for ICT use.

The school has provided Lockable Charging Towers around campus for students to use – these Lockable Charging Towers require the use of student's personally owned device chargers. Charging areas in the school are marked with clear signage – all other areas are prohibited for charging purposes. The designated charging areas must use the school provided power cables that are secured to the charging areas. Students are not permitted to plug in their own chargers at the designated charging areas for safety reasons.

In the rare instance that a student has been given direct instruction from a teacher to use a charging cable in a classroom (eg. During an exam and only to be approved by one of school leadership team or the IT Manager), any injury and/or damages that may occur from the use of the charger (including staff or students tripping over the device charging cable) is solely the responsibility of the student.

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. This forms part of the Corinda State High School enrolment procedures. The acceptable-use conditions and school policies apply to the use of the device and internet both on and off the school grounds.

Communication through Internet and online communication services must also comply with the Safe, Supportive and Disciplined School Environment and the Corinda SHS Responsible Behaviour Plan for Students.

While on the school network, 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 unauthorised programs and intentionally download unauthorised software, graphics, video or music
- Intentionally damage or disable computers, computer systems, school or government networks
- Use the device for unauthorised 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.

Cybersafety

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

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

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 recipients' computer
- Chain letters or hoax 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 organisation.

Parents, caregivers and students are encouraged to read the department's cybersafety and cyberbullying policies and guidelines:
https://www.qld.gov.au/education/schools/health/cybersafety/cybersafety-qss

Consent for the use of Online Services

The Use of Student Information

Corinda SHS may wish to utilise third-party web-based service providers (Online Services) to aid in students learning or school operations. For your student to use the service, the school/teacher will need to register them as a user. Registering with these providers may require student personal information to be disclosed to the provider of the service. These online services are private companies that are hosted onshore in Australia and/or outside of Australia. Outside of Australia means that data that is entered to register for these sites will be stored on servers that are not based in Australia and therefore are not bound by Australia's privacy laws.

Prior to students using online services, the school will send an Online Service Consent Form asking your permission for the registration and use of these sites by your student. While this form is commonly completed via QParents, they may also accompany resource levy and enrolment forms. Note: It is not compulsory for you to provide this consent.

Responsible use of BYOD devices

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.

- Students using the system must not at any time attempt to access other computers
- 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 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
- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights
- Parents and caregivers need to be aware that damage to mobile devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's behaviour policies
- The school will educate students on cyber bullying, safe Internet and email practices, and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

All material on the device is subject to audit by authorised 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.

Misuse and breaches

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.

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. This includes not trespassing in another person's files, home drive, email or accessing unauthorised network drives and 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 plagiarise 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 Intranet or Internet 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 without warning and be subject to prosecution from agencies to enforce such copyrights.

ICT Agreement

Students will be safe, ethical, lawful, courteous, respectful, and conducive to the good order of school and the community. As such:

- Students are not to touch, interfere or use any other students' device.
- ICT at Corinda SHS is to be used for educational activities conducted by the school.
- Your school email address is strictly for educational use and is not to be used to sign up for mailing lists or websites, e.g. social media sites and online shopping accounts. This account should be checked daily.
- At no time is any student permitted to record, photograph or film anyone else using either video or audio without the explicit permission of a teacher and that person.
- Tethering and hotspot technology is not permitted on the school grounds, all devices at all times must be connected to the Department of Education QLD network.
- All devices need to have a carry case as part of the ICT agreement.
- Devices must be fully charged and ready for learning at the start of each school day. Devices will not be charged in classrooms or other areas unless otherwise clearly designated as a charging area.
- Students are required to have a USB with their name on it to back up any work that they are completing while at school so if there is a hardware or software malfunction no work is lost.
- Students will 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.

- Students are not to disable any settings for virus protection, spam, Internet filtering and/or device management and Wi-Fi profiles installed by the school.
- No use of unauthorised programs and intentionally downloading unauthorised software, graphics, video or music.
- Students will not intentionally damage or disable computers, computer systems, school or government networks.
- Devices may not be used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- Anything you do on your device while at school may be accessed and monitored by staff to ensure students compliance with the ICT agreement.
- Personal accounts are not to be shared at any time and students are not permitted to let others use their personal account details.
- At no times should students reveal names, personal details or images of themselves and anyone else in their interactions with online communities and social networks.
- While at school the Department of Education provides internet filtering of inappropriate content. When devices are at home parents/caregivers are advised to monitor student online activity.
- Students are not to plagiarise or violate copyright laws.
- Breaching this agreement will result possible restrictions on your device and account and other appropriate measures as determined by the principal.
- In the case where a student has been found to lose or damage another student's device, normal school procedures apply. Students and the parents will be held responsible for any deliberate act that leads to damage or loss of another student's device. All disputes in these matters will be referred to the principal who is the final arbiter.
- Ongoing breaches to this agreement will result in a review of the student's participation in the school's technology program.