Cybersafety ................................................................................................................................. 13
Cybersafety Guidelines ............................................................................................................. 13
Responsible use of BYOD devices ............................................................................................ 13
  Responsible use of BYOD as learning devices ...................................................................... 13
Misuse and Breaches of Acceptable Usage ............................................................................... 15
Privacy and Confidentiality ...................................................................................................... 15
Intellectual Property and Copyright ......................................................................................... 15
ICT Agreement Parent/Teacher/Student Reference: ............................................................... 16
Corinda State High School ........................................................................................................ 17
Student Laptop BYOD Program 2019 ...................................................................................... 18
Responsible Use Agreement ...................................................................................................... 18
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.

At Corinda State High School we believe that technology can play a significant role in transforming the teaching and learning space. eLearning is the backbone of any successful school operating in the 21st Century. We strive to move beyond simply viewing technology as a substitution to redefining the way in which learning takes place. With this approach, the teacher’s role moves beyond transferring information, to facilitating the construction of deep and meaningful understandings through the use of collaborative creation.

As we move toward the future the school has made significant progress with the Bring Your Own Device (BYOD) strategy. We introduced this policy in 2016 and it has proved to be very positive with a large number of students taking up the opportunity to bring their own device. The improved accessibility for students allows for an even better support network to be built. This improves the academic outcomes of all students. As the program continues the benefits can be seen across the school, these include:

- Learning that completely transforms what has occurred in approaches to learning in traditional classroom environments
- Learning that is portable, personal, collaborative, interactive, instructive, differentiated, and contextual
- 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 the 1:1 ratio and in keeping with global, national and state trends, Corinda State High School commenced the BYOD program with all students in 2016. All students and their families are encouraged to purchase or bring their own device that meets the minimum specifications to use in the classroom.

**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, enhanced BYOD support, 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 are required to pass through the tech department. This ensures it meets the minimum specifications and is able to be set up for use within the schools network.
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 Principal and the Head of Department of Information Services reserve the right to deny any student access to the school’s network for any breaches of the school ICT policy.

If you have any questions please contact the Head of Department for ICT by email: byodsupport@corindashs.eq.edu.au

About the Program - What is BYOD?
Bring Your Own Device is a term used to describe a digital device ownership model where; student and or staff 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, and ICT class resources.

To connect to the school network devices are required to meet the minimum specifications outlined in this document.

Benefits of BYOD
- A solution to maintain a 1:1 model for our students, providing them with access to technology 24/7
- Greater capacity to participate and deliver inquiry/project based learning with greater student choice and differentiation
- Students are comfortable and confident using a device they are familiar with
- Students can personalise their device to suit their own learning
- Allows a greater range of parental choice in the purchase of devices
- Creates a diverse community of devices helping to enhance awareness of emerging technologies
- Exposes staff to a wide range of platforms which further develops ICT capabilities
- Promotes reciprocal learning between staff and student in a contemporary learning environment.
**BYOD Cost**

All students are required to pay an annual fee of $120.00. This fee includes:

- Additional system connectivity of personal device – WIFI connection and access to network services
- Additional licensing management of software – such as the Adobe Suite, and the distribution of software
- Hot-Swap - this is a replacement school laptop for use while the student’s personal device is being repaired for up to 10 school days per year (conditions apply)
- Additional technical support including:
  - Provide troubleshooting for any device that meets minimum requirements. Windows Operating Systems (Win 10), Apple Mac Operating systems (Mac OSX)
  - Advise ‘best option’ for repair of problem
  - Provide assistance in school connectivity issues
  - Provide support for school allocated software.
  - Provide assistance and 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.

**BYOD Checklist**

- Have a device that meets the minimum requirements: Windows 10, 64bit capable CPU, Dual Band Wireless, 4 GB Ram, 128GB+HDD or MAC OS (Sierra and above) with Dual Band Wireless – a minimum specifications checklist is provided for your convenience on page 6
- Install basic software as per software minimum specifications checklist on page 7
- Student and Parent/Guardian are to complete and sign the Responsible Use Agreement Form (page 17), and return it to the Students Services Office with payment of the BYOD levy $120.00, (Annual Fee).
- Student take their device and receipt to the IT Department to prepare your device to connect to the school network.

**Minimum Hardware & Software Requirements – Selecting a BYOD Device**

**Device selection**

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.
The Corinda State High School BYOD program supports printing, filtered Internet access, file access, and storage through the department’s network while at school. Additionally, the BYOD program includes school technical support and charging of devices at school using dedicated charging stations.

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. An attempt will be made to connect devices that do not meet the minimum specifications, but parents and students should be aware that connectivity may not be possible.

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.

On Page 5 is the minimum specification for all students and higher performance recommendation. Take this with you as reference when you purchase your device.

Corinda SHS BYOD Landing Page: Support and Help Documents:
https://corindashs.eq.edu.au/Facilities/Computersandtechnology/Pages/Computersandtechnology.aspx

3rd Party and Vendor BYOD Portal – Online Shopping and Catalogue Vendor Pages:

Software Portals for BYOD Devices:
BYOD School Connection App:

Office 365 for BYOD:
https://corindashs.eq.edu.au/Supportandresources/Formsanddocuments/Documents/Program%20forms/Student%20laptop%20BYOd%20program/Office365%20At%20Home.pdf

For more information regarding the BYOD Program visit the school’s website
https://corindashs.eq.edu.au/Facilities/Computersandtechnology/Pages/Computersandtechnology.aspx
Corinda State High School
BYOD Device Minimum Specifications

**TAKE THIS CHECKLIST WITH YOU WHEN PURCHASING A DEVICE**

HARDWARE MINIMUM REQUIREMENTS
Years 7 to 12 Laptop

<table>
<thead>
<tr>
<th>WINDOWS LAPTOP</th>
<th>MAC LAPTOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Windows 10 and Above (NOT Windows 10S)</td>
<td>☐ MAC OS Sierra and Above</td>
</tr>
<tr>
<td>☐ 64bit capable CPU</td>
<td>☐ Dual Band Wireless (Capable of 5GHZ Wireless)</td>
</tr>
<tr>
<td>☐ Dual Band Wireless (Capable of 5GHZ Wireless)</td>
<td></td>
</tr>
<tr>
<td>☐ 4 GB Ram</td>
<td></td>
</tr>
<tr>
<td>☐ 128GB+ HDD (SSD Recommended)</td>
<td></td>
</tr>
</tbody>
</table>

RECOMMENDED ACCESSORIES
☐ Protective Case for your laptop - Consider a “ruggerised” case
☐ Mouse (wireless USB Chargeable or corded)
☐ Accident Protection Insurance (with purchase or check your Home and Contents Insurance Policy)

HARDWARE RECOMMENDED REQUIREMENTS
– Graphics & Industrial Design, Visual Arts
Years 10 to 12 Laptop

<table>
<thead>
<tr>
<th>WINDOWS LAPTOP</th>
<th>MAC LAPTOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Windows 10 and Above (NOT Windows 10S)</td>
<td>☐ MAC OS Sierra and Above</td>
</tr>
<tr>
<td>☐ 64bit capable CPU</td>
<td>☐ Dual Band Wireless (Capable of 5GHZ Wireless)</td>
</tr>
<tr>
<td>☐ Dual Band Wireless (Capable of 5GHZ Wireless)</td>
<td></td>
</tr>
<tr>
<td>☐ 8 GB Ram</td>
<td></td>
</tr>
<tr>
<td>☐ 256GB+ HDD (SSD Highly Recommended)</td>
<td></td>
</tr>
<tr>
<td>☐ Dedicated Video Card 2GB Memory or higher</td>
<td></td>
</tr>
</tbody>
</table>

RECOMMENDED ACCESSORIES
☐ Protective Case for your laptop - Consider a “ruggerised” case
☐ Mouse (wireless USB Chargeable or corded)
☐ Accident Protection Insurance (with purchase or check your Home and Contents Insurance Policy)
**USE THIS CHECKLIST WHEN INSTALLING SOFTWARE**

## SOFTWARE MINIMUM REQUIREMENTS

### Years 7 to 12 Laptop

- **Corinda SHS BYOD App**
  - [https://corindashs.eq.edu.au/Supportandresources/Formsanddocuments/Documents/Program%20forms/Student%20laptop%20BYOd%20program/BYO.zip](https://corindashs.eq.edu.au/Supportandresources/Formsanddocuments/Documents/Program%20forms/Student%20laptop%20BYOd%20program/BYO.zip)

- **Microsoft Office 2016 or Microsoft 365**
  - Download via [http://portal.office.com](http://portal.office.com). Use your student ID and password to login
  - **Windows Version** – Office 2016 contains
    - Word, Excel, PowerPoint, Access, Publisher, Outlook, OneNote
  - **Mac Version** – Office 2016 contains
    - Word, Excel, PowerPoint, OneNote

- **PDF Reader** – Windows or Adobe Reader (Free to download)


- **Anti-Virus Software** (Windows can use the free Defender) and ensure it is continually updated
Responsibilities of Stakeholders – Students, Parents/Caregivers, and the School

Corinda State High School

- BYOD program induction — including information on connection, care of device at school, workplace health and safety, appropriate digital citizenship, and cybersafety
- Network connection at school
- Internet filtering (when connected via the school’s computer network)
- Technical support (please consult Technical support table)
- School-supplied software e.g. Adobe, Microsoft Office 365
- Printing facilities.

Students

- Participation in BYOD program induction
- Acknowledgement that core purpose of device at school is for educational purposes
- Care of device
- Appropriate digital citizenship and online safety (for more details, see ACMA CyberSmart)
- 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
- Charging of device
- Abiding by intellectual property and copyright laws (including software/media piracy)
- Ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason
- Understanding and signing the BYOD Agreement.

Parents/Caregivers

- Acknowledgement that core purpose of device at school is for educational purposes
- Internet filtering (when not connected to the school’s network)
- Encourage and support appropriate digital citizenship and cybersafety with students (for more details, see ACMA CyberSmart)
- Some technical support (please consult Technical Support table)
- Required software, including sufficient anti-virus software
- Protective case for the device
- Adequate warranty and insurance of the device
- Understanding and signing the BYOD Agreement.
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 triage 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.

**Software and Licenses**

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. Parents/Caregivers or Technicians may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. Software may need to be removed from the device upon cancellation of student enrolment, transfer or graduation.

Some software is required to assist with teaching your student at Corinda SHS, e.g. ClickView, graphics applications, PDF, VLC video player, subject specific software, etc. Technicians may also need access to the device to assist with triage support of the device and these applications. The following table provides an overview of the licences and support. Please note these may change as the school upgrades software.

**Software, License and Support Table:**

<table>
<thead>
<tr>
<th>License Provided by School Fees</th>
<th>School Support</th>
<th>Parents/Caregivers</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems/ Windows/MAC</td>
<td>X</td>
<td>triage support</td>
<td></td>
</tr>
<tr>
<td>Office 365 – Word, Excel, PowerPoint, One Note, Outlook, etc</td>
<td>✓</td>
<td>✓</td>
<td>check vendor support when purchasing</td>
</tr>
<tr>
<td>PDF Reader</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Adobe Creative Cloud (Photoshop/ Illustrator)</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Corinda SHS BYOD Program</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Internet Access Support</td>
<td>n/a</td>
<td>filtered Internet and support</td>
<td></td>
</tr>
<tr>
<td>Wireless Access</td>
<td>n/a</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Readcloud/Clickview (Digital Resources)</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BYOD Hardware – Laptop Repairs</td>
<td>n/a</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Corinda State High School
BYOD – Bring Your Own Device
Exceed Your Expectations
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. To access a loan device, evidence is required to show the student’s device has been logged with a repairer for repair (typically a receipt showing support or ticket number).

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 the school year, 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 IT Tech Support staff. If the device is not returned, financial compensation will be sought. It is also a requirement of using the device that students provide authorised school staff with access to the device and personal holdings associated with the use of the device if requested.

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 IT Tech 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 is solely the responsibility of, and is to be organised by the parent/carer prior to checking-in the device with IT Tech Support staff.

1. Check-in the BYOD laptop with a technician and provide verification of the work to be carried out by a third party repairer
2. Student may obtain a Hot-Swap school laptop whilst BYOD laptop is checked-in for repair
3. A check-in slip will be provided to the student and verified by email when device is secured into the ICT Tech room
4. An email will be sent to the student when the computer has been repaired by the third party and the Hot-Swap is to be returned and exchanged when collecting the student’s BYOD Laptop.

Repairs Fees for Hot-Swap Laptops
School owned laptops are the property of the Department of Education and Training and incur charges if damaged by the student whilst on loan. An accidental damage repair incurs a $100 excess fee per incident; and if the laptop is lost or stolen, and not recoverable, a fee of $300 will be charged. This fee will also apply to malicious damage.
General Device care

Security of BYOD – Damage/ Theft Insurance
All BYOD laptops and devices must be engraved 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.

It is highly recommended to ensure the device is included on your Home and Contents Insurance for accidentally damage and theft.

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.

The school will continue to deal with inappropriate behaviour in line with existing policies and any student who damages or steals another student’s laptop may be disciplined according to the Corinda SHS Responsible Behaviour Plan for Students.

General Precautions
- Food or drink should never be placed near the device
- Plugs, cords, and cables should be inserted and removed carefully
- Devices should be carried within their protective case where appropriate
- Carrying devices with the screen open should be avoided
- Ensure the battery is fully charged each day
- Turn the device off before placing it in its bag
- Avoid extreme temperatures
- Avoid using in areas that are hazardous (e.g. wet, dusty, muddy, etc.)

Protecting the Screen
- Avoid poking at the screen — even a touchscreen only requires a light touch. Do not use any object other than a finger or purpose built stylus
- Don’t place pressure on the lid of the device when it is closed
- Avoid placing anything on the keyboard before closing the lid
- Avoid placing anything in the carry case that could press against the cover
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth
- Don’t clean the screen with a household cleaning product.
**Web Filtering**

The Internet has become a powerful tool for teaching and learning, however students need to be careful and vigilant regarding some web content. At all times students will be required to behave in line with the requirements of the Responsible Behaviour Plan for Students and school policies. To help protect students and staff from malicious web activity and inappropriate websites, Corinda State High School operates a comprehensive web filtering system. Any device connected to the Internet through the school network will have filtering applied.

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

- Inappropriate web pages
- Spyware and malware
- Peer-to-peer sessions
- Scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school’s filtering approach represents global best-practice in Internet protection measures. However, despite internal departmental controls to manage content on the Internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information requires responsible use by the student.

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.

The personally owned BYOD laptops have access to home and other out-of-school Internet services and those services may not provide Internet 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.

Parents, caregivers, and students are also encouraged to visit the Australian Communications and Media Authority’s CyberSmart website for resources and practical advice to help young people safely enjoy the online world.

**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 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.

Passwords

Use of the school’s ICT network is secured with a user name and password. The 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, (a student should not share their username and password with fellow students).

• The password should be changed regularly, as well as when prompted by the department or when known by another user

• Personal accounts are not to 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 device

• Students should also set a password for access to their BYOD device and keep it private

• Parents/caregivers may also choose to maintain a password on a personally-owned device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls, with such use being the responsibility of the parent/caregiver.

Digital Citizenship

Students should be conscious creators of the content and behaviours 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 behaviours they have online are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural 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 Responsible Behaviour Plan also supports students by providing school related expectations, guidelines and consequences.
Cybersafety

Cybersafety Guidelines

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 guide for parents and caregivers.

Responsible use of BYOD devices

Responsible use of BYOD as learning devices

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

The following are examples of responsible use of mobile devices by students:

- Use mobile devices for:
  - Engagement in class work and assignments set by teachers
  - Developing appropriate 21st Century knowledge, skills and behaviours
  - Authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
  - Conducting general research for school activities and projects
  - Communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
  - Accessing online references such as dictionaries, encyclopaedias, etc.
  - Researching and learning through the school’s eLearning environment
  - Ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate and respectful of others when using a mobile device.
- Switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
• Use the personal mobile device for private use before or after school, or during recess and lunch breaks.
• Seek teacher’s approval where they wish to use a mobile device under special circumstances.

The following are examples of irresponsible use of devices by students:
• Using the device in an unlawful manner
• Creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
• Disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
• Downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
• Using obscene, inflammatory, racist, discriminatory or derogatory language
• Using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
• Insulting, harassing or attacking others or using obscene or abusive language
• Deliberately wasting printing and Internet resources
• Intentionally damaging any devices, accessories, peripherals, printers or network equipment
• Committing plagiarism or violate copyright laws
• Participating in unsupervised Internet chat
• Sending chain letters or spam email (junk mail)
• Accessing private 3G/4G networks during lesson time
• Knowingly downloading viruses or any other programs capable of breaching the department’s network security
• Using the mobile device’s camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
• Invading someone’s privacy by recording personal conversations or daily activities and/or the further distribution, e.g. forwarding, texting, uploading, Bluetooth use, etc., of such material
• Using the mobile device, including those with Bluetooth functionality, to cheat during exams or assessments
• Using mobile devices at exams or during class assessment unless expressly permitted by school staff.

In addition to this:
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
• Systems, accounts or unauthorised network drives or files or to access other people’s devices without their permission and without them present
• 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
Corinda State High School
BYOD – Bring Your Own Device

Exceed Your Expectations

- 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 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.

Corinda State High 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.

**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 Parent/Teacher/Student Reference:

**STUDENTS WILL BE:** SAFE / ETHICAL / LAWFUL / COURTEOUS / RESPECTFUL / CONDUCIVE TO THE GOOD ORDER OF SCHOOL AND THE COMMUNITY

- Students are not to touch, interfere or use any other student’s device
- ICT at Corinda SHS is to be used for educational activities conducted by the school
- Devices must be maintained and kept free from food and drink and any images and decoration on devices must be appropriate and align with the school policies
- 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 Education QLD network through either Wi-Fi, LAN or 3G. All other data network connections must be disabled before coming to school
- Electronic messaging, file transfers and communication may be used for educational purposes under the direction of your teacher
- 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. This should be a part of their daily homework routine
- 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. Parents are encouraged to access government resources on https://www.esafety.gov.au/ and http://cybersmart.gov.au/ and discuss online safety and privacy with their student
- While at school the Education Department 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.
Corinda State High School

Student Laptop BYOD Program 2019

Responsible Use Agreement

The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER:

• I have read and understood the Student BYOD Policies and Procedures and the School Responsible Behaviour Plan. (Both documents available via School website).
• I agree to abide by the guidelines outlined by BYOD Policies and Procedures.
• I am aware that non-compliance or irresponsible behaviour, as per the intent of the BYOD Policies and Procedures and the School Responsible Behaviour Plan, will result in consequences relative to the behaviour.
• I agree to Corinda State High School adding School related software to the BYOD Device.

Student’s Name:   Year Level:   EQID No:
(Please print)

Student’s Signature:  Date:

Parent / Caregiver’s Name:
(Please print)

Parent / Caregiver’s Signature:  Date: