



# Digital Technologies and BYOxLink Acceptable Use Agreement





## Contents

Use of Digital Technologies at Bundaberg North State High School.....	3
ICT in the Australian Curriculum .....	4
Student Access to ICT Services, Facilities and Devices at Bundaberg North State High School.....	4
Responsibilities for Using the School’s ICT Services, Facilities and Devices.....	5
Acceptable/appropriate use/behaviour by a student.....	5
Unacceptable/inappropriate use/behaviour by a student .....	6
Web Based Services Consent .....	6
Permission to Use Cloud, Web Based and App Services.....	6
Bring Your Own Device (BYOD) and BYOxLink .....	8
Security of BYOD, Damage/Theft – Insurance, Behaviour .....	9
Data security and back-ups .....	10
Office 365 .....	11
BYOxLink – Conditions of Use.....	12
Frequently Asked Questions .....	13
Digital technologies and BYOxLink Agreement .....	15
Student:.....	15
Parent or Guardian:.....	16

## Use of Digital Technologies at Bundaberg North State High School

The ability to use technology is becoming increasingly important in the workforce of the 21<sup>st</sup> Century. In order to support learners in developing these skills Bundaberg North State High School integrates the use of Information and Communication Technologies (ICT) into the classroom to enhance the learning experience. It is a tool that enhances pedagogy, facilitates the creation and sharing of knowledge and allows differentiation in learning.

The use of Digital Technologies is more than retrieving information. They:

- Enhance independence and self-initiated learning among students,
- Extend student learning beyond the classroom,
- Promote the development of 21st Century teaching and learning,
- Enable the delivery of ICT as an Australian Curriculum general capability.

## ICT in the Australian Curriculum

ICT is represented in the Australian Curriculum as a general Capability:

- Competence in ICT
  - Students develop ICT competence as they learn to use ICT effectively and appropriately when investigating, creating and communicating ideas and information at school, at home, at work and in their communities. (ACARA, 2010)
- Students develop ICT competence when they learn to:
  - Investigate with ICT
  - Create with ICT
  - Communicate with ICT
  - Operate with ICT

## Student Access to ICT Services, Facilities and Devices at Bundaberg North State High School

Bundaberg North State High school supports the Department of Education's Digital Strategy of investing in contemporary learning, with near seamless access to information and digital technologies, anywhere, anytime on any device.

Essential tools for providing these innovative educational programs include the intranet, internet, email and network services (such as computers, printers, and interactive projection systems) that are available through the department's ICT networks. These technologies are vital for the contemporary educational programs provided in our school.

Staff, students and parents have a duty of care to ensure that these technologies are used appropriately, protected from harm, and that users are not exposed to material that is considered offensive or illegal.

Student access to ICT services, facilities and devices is granted by the school Principal. Continued access is conditional to students abiding by the terms and conditions outline in this Handbook. The Principal reserves the right to restrict student access to the school's ICT services, facilities and devices if the access and usage requirements are not met or are breached. However the restricted access will not disrupt the provision of the student's educational program.

The Department of Education monitors access to, and use of, its network, including internet, email and cloud based storage facilities. This monitoring occurs to identify inappropriate use, to protect system security, and to maintain system performance in determining compliance with state and department policy requirements. The department may conduct security audits and scans, and restrict or deny user and/or device access to the network if there is any suspicion that the integrity of the network might be at risk.

## Responsibilities for Using the School's ICT Services, Facilities and Devices

Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in this handbook and in the school's Student Code of Conduct. In particular:

- Students **must not** under any circumstances, access personal files belonging to others, software, or areas of the network which are not designated for their use.
- Students **must not** give their password to other students, or use another user's name and password to access the network under any circumstances. Sharing of passwords is a security risk.
- Software copyright is to be observed at all times. Only software purchased or approved by the school and installed by the school can be used on school provided devices. It is illegal to copy or distribute school owned software. Software from home or other sources is not to be copied, installed or used on school owned devices.
- Students may store educational files on the school server and department provided cloud storage (OneDrive) areas. The use of portable storage devices (USB Drives) is also permitted for the transfer of school related files to and from these storage areas. The storage and transfer of unauthorised software and other inappropriate material (such as pirated movies, music or personal photos) is not permitted under any circumstances.
- The use of the Department Managed Internet Services (MIS) which encompasses Internet, Intranet and email services, is provided for educational purposes. Deliberate attempts to look for and use material that is illegal, or which would be considered offensive, disrespectful, threatening or discriminatory is not permitted. The downloading of materials other than that deemed school related, is not permitted. This includes the downloading of music, movies and other large multimedia files.
- The access to and use of online collaboration and video conferencing services such as Microsoft Teams and The Learning Place Blackboard Collaborate Ultra are only to be used under strict staff supervision.
- Students must not post or use inappropriate language or harass others when communicating online.

## Acceptable/appropriate use/behaviour by a student

It is acceptable for students to use technologies while at school for:

- Assigned class work and assignments set by teachers
- Developing appropriate literacy, communication and information skills
- Authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
- Conducting general research for school activities and projects
- Communicating or collaborating with other students, teachers, their parents or experts in relation to school work

- Accessing online references such as dictionaries, encyclopaedias, etc.
- Researching and learning through the department's eLearning environment

At all times, students must be courteous, considerate and respectful of others when using Technologies.

## **Unacceptable/inappropriate use/behaviour by a student**

It is unacceptable for students while at school to:

- Use Technologies in an unlawful manner
- Download, distribute or publish offensive messages or pictures
- Use obscene, inflammatory, racist, discriminatory or derogatory language
- Use language and/or threats of violence that may amount to bullying and/or harassment, or stalking
- Insult, harass or attack others
- Deliberately waste printing and internet resources
- Wilfully damage computers, printers or network equipment
- Commit plagiarism or violate copyright laws
- Ignore teacher directions regarding the use of social media, online email and internet chat
- Send chain letters or spam email (junk mail)
- Share their own or others' personal information and/or images which could result in risk to themselves or another person's safety
- Knowingly download viruses or any other programs capable of breaching the department's network security
- Use in-device cameras inappropriately, such as in change rooms or toilets
- Invade 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
- Use Technologies (including those with Bluetooth functionality) to cheat during exams or assessments
- Take into or use Technologies at exams or during class assessment unless expressly permitted by teaching staff.

## **Web Based Services Consent**

### **Permission to Use Cloud, Web Based and App Services**

Cloud, Web Based and App Services are used to support curriculum delivery at Bundaberg North State High School. Clickview and Adobe Creative Cloud are examples of these services.

All web based services in use have undergone a risk assessment by the Queensland Government Service Centre. Principal approval and parental consent is required prior to the use of these services. Teachers in charge of these activities will have read the risk assessment and will constantly monitor use and immediately cancel the activity should any concern be raised.

Students and parents are asked to report any concerns with any web based activity to their respective teachers immediately.

A number of precautions will be taken when creating logins for Cloud, Web based and App services. These include:

- The student's first name and first two initials of the surname eg for John Brown use – **johnbr** – for a student log in will be used.
- Where a first name and surname are required as separate fields, as above, **johnbr** as a first name and the word **student** as a surname will be used.
- Students will be told not to use their school password as the password for any of these services.
- The use of the name Bundaberg North State High School will be minimised. Where possible, the use of BNSHS will be used.
- No photos of students will be uploaded.
- Wherever possible, the use of avatars, personas or fictional characters when interacting within a Cloud, Web Based or App will be utilised.
- If an email address is required, students' school email addresses will be used to register and identify students on these services.

A list of the services in use will be published in the school newsletter periodically. In order to keep our records up to date, permission for the use of web based services will be sought annually.

### **Giving parental consent**

There will be two options for parents/caregivers to provide consent for their student/s.

The preferred option is the completion of the [online consent](#) found on our school website (computers and technology page).

If parent/caregivers are unable to access the survey, please contact the school on 41300222 to obtain a form for completion and return to the school.

## **Bring Your Own Device (BYOD) and BYOxLink**

Bundaberg North State High School aims to have all students functioning efficiently as 21<sup>st</sup> Century Learners and Citizens. The world reliance on Technology is ever increasing and the ability to use technology is becoming ever more important in the workforce. In order to support learners in developing these skills, Bundaberg North State High School is now a BYOD school with an expectation that every student will bring a device to school that meets the minimum specification to enhance their learning.

Families that are unable to provide a device for their child are requested to make an appointment with either the Principal or Junior School Deputy Principal to discuss options.

**The BYOD device from home must fit the minimum hardware and software specifications as outlined on the school website.**

By participating in the Bundaberg North State High School BYOD and BYOxLink Program, students will be supplied with:

- Wireless connectivity for BYO devices to authorised sections of the school secured network through the BYOxLink portal.
- Access for BYO devices to Managed Internet Service (MIS) services including Internet, the school Intranet (SharePoint), supervised email, Department managed Cloud Storage (OneDrive), and online O365 applications.
- Access to learning materials,
- Access for BYO devices to school printers and school network storage through the gateway whilst connected to the school network.

**Parents are required to supply and are responsible for:**

- Supplying a device that meets the minimum hardware and software specifications as outlined on the school web site.
- Any repairs to the supplied device,
- Ensuring the device Operating System (OS) software is regularly updated as required by the device manufacturers



## **The IT Department at Bundaberg North State High School:**

- Will provide assistance connecting your chosen device to the BYOxLink network and provide continued support with this connection
- Will provide limited ongoing support with Office 365 software.
- Will not provide software or hardware repairs to privately owned BYOxLink connected devices.

## **Security of BYOD, Damage/Theft – Insurance, Behaviour**

Suggestions about ensuring the laptop is safe at school include:

- Keeping the laptop with you at all times – It is each student’s responsibility to keep their laptop with them at all times.
- Consider engraving the device – Engraving the bottom of the laptop with the student’s name ie First Name and Surname has helped school staff to locate lost laptops and return them to their owners.
- Home and Contents Insurance – Check with your Home and Contents Insurance company regarding damage or theft of the device.
- Inappropriate Behaviour – While the school will continue to deal with inappropriate behaviour in line with existing policies, the School is not liable for any damage or replacement costs incurred while the device is at school or travelling to and from school. Any student who does damage or steal another student’s laptop may be disciplined according to the School’s Student Code of Conduct.
- Short term storage in a locker – A limited number of lockers are available for student hire for the temporary storage of their laptop. Application forms for requesting a locker are available from the School Administration Office.

## **Data security and back-ups**

Students must ensure they have a process for backing up data securely. Failure to do so may result in the loss of assignments and the products of other class activities, should a hardware or software fault occur.

The student is responsible for the backup of all data stored on their BYO Device. While at school, students may save data to the school’s network, which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being uploaded to the department's ICT network.

Alternatively, students may backup their data to the school provided cloud storage (OneDrive). This can be accessed through the MIS portal. Students should, in the first instance, seek assistance from their teacher for help accessing OneDrive.

## Office 365

All students in Queensland have free access to 5 student downloads of the full suite of Microsoft Office 365 suite. Office 365 allows students and staff to create and share classwork, assessment and other curriculum documents which students can access anywhere via an internet connection 24/7. The software can be downloaded by following the directions on the school website.

## BYOxLink – Conditions of Use

When using a privately-owned device at Bundaberg North State High School, or connecting it to the school network, we agree that:

- The device must at all times be connected to the BYOxLink Gateway when on School premises and in use. When connected to the BYOxLink Gateway, all activities will be logged. School Digital Technologies and BYOxLink guidelines are to be followed at all times.
- The device will only be used for educational purposes when connected to and using School services.
- Bundaberg North State High School will only provide technical support to enable connectivity to the School network via the BYOxLink portal that provides access to student files required for class, internet and printing services.
- It is the responsibility of the student to ensure that the private device is secured when not in use. Bundaberg North State High School takes no responsibility for theft, loss, vandalism, damage or unauthorised access to private devices.
- BYOD devices must not be charged using School power outlets or by plugging into school owned computers. All private devices must be brought to school fully charged. Chargers in classrooms are a safety concern as they are a tripping hazard and may also damage devices.
- It is the responsibility of the student to back up data on the private device e.g. to external hard drive, USB or cloud storage (OneDrive). The school will not take any responsibility for loss of student data.
- Any software purchased or provided under Education Queensland agreements must be removed from the private laptop as per the conditions of the agreement. This includes if the student leaves Bundaberg North State High School. Any privately owned software installed on the laptop must be age appropriate, follow copyright legislation and not cause offence.

- Bundaberg North State High School and the Education Department reserves the right to restrict access and use of any private device used on the School grounds, whether it is connected to the school BYOxLink portal or not. Access to the School network and permission to use the private device on School grounds will be withdrawn as a consequence of any inappropriate use and/or security breach. Only Cloud Based services provided by the school are to be used whilst connected to the school Gateway. Other Cloud Based Services such as iCloud or Dropbox must not be used at school to store, send or access information at school.
- Bundaberg North State High School reserves the right to ask any student to close or turn off their device due to inappropriate use.

## Frequently Asked Questions

### **Will I need to bring the device to school every day?**

Yes. Laptops are essential tools in each classroom.

### **How do I protect my BYOD device?**

It is the student's responsibility to have their device with them at all times. Protective equipment such as bags or cases need to be organised by the parent and student to keep these devices safe while at school, and travelling to and from school. It is the responsibility of the student to look after the device while at school and kept securely in bags. Lockers are available from the Administration Office for temporary storage of devices.

### **Do I need to back up?**

Yes. It is the student's responsibility at all times to back up all files. The school assessment policy states that loss of data due to technology problems is not an acceptable reason for assessment extensions.

### **We already have a device at home; can I use it at school?**

Yes, providing it meets the hardware and software minimum specifications listed in this document.

### **Will every device work inside the Education Queensland network?**

No. Some devices with low specifications have been found to not connect to the EQ network. These devices may have difficulty with the security filters used by the Department of Education Queensland.

### **Will the school assist me with network connection settings at school?**

Instructional Videos and documents are available to students on the School website and student Sharepoint site. Students can request individual assistance by completing the [IT Support Request form](#) on our school website, or by attending BYOxLink support sessions at school during 2<sup>nd</sup> break.

### **Will the school protect the device from virus attacks?**

Virus protection remains the responsibility of the owner.

**Do I need 4G cellular?**

Private 4G services are not to be used at school. The school has an effective wireless network available and it is The Department of Education Queensland's policy that whilst at school, the school internet connection must be used.

**Does the school provide software for my BYOD device?**

The Microsoft Office Suite is available free of charge for five student downloads at home. Specialist software required for some subjects will be provided to students enrolled in those courses.

**Can I take my BYOD device to IT for repair?**

The IT Department cannot perform any software or hardware repairs on a privately-owned device.

**Will the school assist me with home internet connection settings and issues?**

No. Your home internet provider or local computer technician can assist you with these enquiries.

**Will the teacher be able to provide technical support in class?**

No. The IT Department is available during 2<sup>nd</sup> break to assist students in resolving connection issues with the network.

**Can I bring my charger to school?**

It is the student's responsibility to attend school every day with a fully charged laptop.

**What is deemed inappropriate?**

All illegal (unlicensed) software; pirated music or videos; defamatory documents, or images, or any content not suitable for viewing by persons under the age of 18 are deemed inappropriate.

## Digital Technologies and BYOxLink Agreement

### Student:

I understand that the school's information and communication technology (ICT) services, facilities and devices provide me with access to a range of essential learning tools, including access to the internet. I understand that the internet can connect me to useful information around the world.

While I have access to the school's ICT services, facilities and devices: I will use it only for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.

Specifically in relation to internet usage, should any offensive information appear on my screen I will close the window and immediately inform my teacher quietly, or tell my parents/guardians if I am at home.

If I receive any inappropriate emails at school I will tell my teacher. If I receive any at home I will tell my parents/guardians.

When using email or the internet I will not:

- reveal names, home addresses or phone numbers – mine or that of any other person
- use the school's ICT service, facilities and devices (including the internet) to annoy or offend anyone else.

I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT services, facilities and devices inside or outside of school hours.

I understand that if the school decides I have not followed expectations for using its ICT services, facilities and devices, appropriate action may be taken as per the school's Student Code of Conduct, which may include loss of access to the network (including the internet) for a period of time.

I have read and understood this handbook and the [Student Code of Conduct](#)

I agree to abide by the above expectations.

\_\_\_\_\_ (Student's name)

\_\_\_\_\_ (Student's signature) \_\_\_\_\_ (Date)

## Parent or Guardian:

I understand that the school provides my child with access to the school's information and communication technology (ICT) services, facilities and devices (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information from around the world; that the school cannot control what is available online; and that a small part of that information can be illegal, dangerous or offensive.

I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend upon responsible use by my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT services, facilities and devices. Furthermore I will advise the school if any inappropriate material is received by my child that may have come from the school or from other students.

I understand that the school is not responsible for safeguarding information stored by my child on a departmentally-owned student computer or mobile device.

I understand that the school may remotely access the departmentally-owned student computer or mobile device for management purposes.

I understand that the school does not accept liability for any loss or damage suffered to personal mobile devices as a result of using the department's services, facilities and devices. Further, no liability will be accepted by the school in the event of loss, theft or damage to any mobile device unless it can be established that the loss, theft or damage resulted from the school's/department's negligence.

I believe \_\_\_\_\_ (name of student) understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT services, facilities and devices (including the internet) under the school rules. I understand where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the Student Code of Conduct. This may include loss of access and usage of the school's ICT services, facilities and devices for some time.

I have read and understood this guideline and the [Student Code of Conduct](#)

I agree to abide by the above policy.

\_\_\_\_\_ (Parent/Guardian's name)

\_\_\_\_\_ (Parent/Guardian's signature) \_\_\_\_\_ (Date)

The Department of Education through its [Information privacy and right to information](#) procedure is collecting your personal information in accordance with the [Education \(General Provisions\) Act 2006 \(Qld\)](#) in order to ensure:

- appropriate usage of the school network
- appropriate usage of personal mobile devices within the school network.

The information will only be accessed by authorised school employees to ensure compliance with its [Information privacy and right to information](#) procedure. Personal information collected on this form may also be disclosed to third parties where authorised or required by law. Your information will be stored securely. 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 child's school. If you have a concern or complaint about the way your personal information has been collected, used, stored or disclosed, please also contact your child's school.