BYOx Program
Parent Handbook

Bremer State High School – *Effective 2021*

Version 3 – January 2021

We Believe. We Strive. We Achieve.

BREMER
STATE HIGH SCHOOL

BYOx Overview

The way in which we learn, access, share and manage information is changing rapidly. There is an increasing need for students to access external learning content, collaborate with others in their educational pathway, and be proficient with the use of computer technologies. As a school we have a responsibility to prepare our young people for the future world that they enter into.

Bring Your Own 'x' (BYOx) is a new pathway supporting the delivery of 21st century learning. The BYOx acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally owned mobile devices are used. The 'x' in BYOx represents more than a personally owned mobile device; it also includes software, applications, connectivity or carriage service.

Bremer State High School understands that it is a tool that enhances teaching and learning experiences, allows for the creation and sharing of knowledge, and allows students to learn at their own pace. The use of technology is more than a method of searching for information.

We have chosen to support the implementation of a BYOx model because:

- BYOx recognises the demand for seamless movement between school, work, home and play
- Our BYOx program assists students to improve their learning outcomes in a contemporary educational setting
- The program enhances independence and self-initiated learning amongst students
- The program will assist students in learning how to become responsible when using technology
- The program will give students the skills and experiences that will prepare them for their future studies and careers

BYOx at Bremer State High School

In 2021 all Year 11 students as well as previously on-boarded Year 12 and Year 7, 8 and 9 Science Extension Pathway students, will be required to participate in the BYOx program. This program requires students to bring a digital device such as a laptop or tablet to school to support their learning. **NB: Mobile phones and android devices are not acceptable.**

Students using their own device will be:

- Operating in a digital classroom – Accessing lesson material, assessment and a dedicated student working space that can be used to collate notes, conduct research and online learning
- Using software and processes that are consistent with industry practice, preparing our learners for career development and the workforce
- Have the opportunity to receive electronic feedback on learning and assessment from teachers

Note: Consistent with the current model (BYOX), students in other year levels may bring a device to support their learning once their caregiver has signed the BYOx Student Charter.

Device Selection

In order to provide a consistent experience for students, it is important the device meet the **minimum** specifications outlined below. This will ensure the device is able to connect to the Bremer State High School network, printing systems, and is suitable for class activities.

If financial circumstances allow, the recommended specifications (right column) will allow for increased speed and capabilities. This will offer your child a better experience and last longer.

	Minimum Specifications (Good)	**Recommended Specifications (Better)**
Platform	Microsoft Windows laptop, Apple iOS or Mac Device	
Screen Size	11”-15” display – consider portability and weight	12”-15” display – consider portability and weight
Processor	It is recommended that the CPU (processor) is at least an Intel Pentium Processor or AMD Phenom 1.6Gigahertz (GHz) or faster 2-core.	
RAM	4 GB	8 GB or higher
Hard Drive	128 GB Solid State Hard Drive (note: we recommend a solid-state hard drive (SSD) for performance) Older style Hard Drives do not offer the same performance and are more likely to fail when moved around. However, if this is your only option, min 128GB would be best.	256 GB Solid State Hard Drive (note: we recommend a solid-state hard drive (SSD) for performance).
Operating System	Microsoft Windows 10, iOS and MacOS Note: The version of Windows called “Windows 10S” is not compatible with our network. NOT Supported: Android, Windows RT, Chromebook and distributions of Linux	
Wireless	Wi-Fi 802.11ac/n or better (**Wireless Network 5Ghz**). The term “Dual Band” covers this. If “Single Band” make sure it is the **Wireless Network 5Ghz** radio band. The above specs are a ‘must have’ otherwise the device will not connect to our network.	
Battery	Sufficient to last 6+ hours on balance power mode	

Extra considerations:

- Protective hard case to reduce the risk of a broken screen (do not be tempted to buy a soft laptop sleeve).
- Onsite warranty (next business day is recommended – having to send a PC away for a couple of weeks for a warranty repair can be frustrating).
- Accidental damage protection / insurance – may be offered at time of purchase.
- Back-up storage device (USB or External Hard Drive) to back up files on the laptop.

Purchasing Considerations:

It is recommended that parents/caregivers contact a range of computer vendors and consider the 'total cost of ownership' including warranty, technical support arrangements and hardware components which will contribute to the life of the laptop. The cheapest laptop to buy is generally not the best option in the end.

The school takes no responsibility for any private laptop purchasing and/or finance arrangements. All issues with laptop purchases or technical issues must be taken up with the vendor/supplier.

What if I cannot afford a device?

Please see the Bremer State High School BYOx Equity Policy for information regarding financial hardship and equity devices.

Software Requirements:

Software installation is the responsibility of the parent/caregiver (or student in independent). Valid licences are required for all software present on the device.

Access to the department's ICT network is provided only if the mobile device meets the department's security requirements, which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device.

Minimum Software Requirements

Office 365 Suite

'Microsoft Office Advantage' allows students to install the Office suite of software (e.g. Word, Excel, PowerPoint etc.) for FREE. Instructions to download, install and activate this software are available from http://education.qld.gov.au/learningplace/help/home-computer-support.pdf

Virus Protection

All devices that connect to the Bremer SHS network must have an active and up to date antivirus Free examples include:

- Microsoft Security Essentials
- Avast Free Antivirus
- Avira Free Antivirus

Device Connectivity:

Student private laptops connect to the Bremer State High School network through a Department of Education approved technical solution (BYOx Connect) that ensure security requirements are met. Under this solution, students are able to access the school network for file access and management, filtered internet and printing services.

Students will need to have an administrator account on their device in order to initially connect to the approved technical solution. After the device has been connected, the account can be converted back to a standard user account. This is to facilitate the security checks and certificate installations that need to take place in order to ensure devices are safe and secure.

Parents/guardians should be aware the private laptops enable access to home and other out of school networks and internet services, which may not be secure or include filtering. Bremer State High School takes no responsibly for security issues or content accessed by students using private network or internet services on private devices at any time.

Device Charging:

It is the responsibility of the student to bring their laptop to school fully charged every day. Failure to bring laptops fully charged each day will impact on student learning and their ability to participate in class activities. Students will NOT be able to charge laptops in classrooms or the library. This is primarily due to workplace health and safety issues (eg cables being a trip hazard, power cables not "tested and tagged"). However, if a student requires their laptop to be charged (e.g. if it's an older laptop that doesn't hold its charge) there will be a charging station in the library that students will be able to access before school and at break times to charge their laptops securely. Due to the number of charging stations available, this will be on a first in/first served basis.

Technical Support:

Bremer State High School IT Technicians will provide support for connectivity of laptops to the school network. Every attempt will be made to connect devices which meet the minimum specifications, assuming there are no technical or other issues outside their control. All other technical issues will be the responsibility of the parent/caregiver and student. Vendor and technical support turnaround times should be considered when purchasing and seeking repairs for devices.

Technical Support:

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
Bremer State High School	✓ school provided internet connection	(dependent on school-based hardware arrangements)	✓ (some school-based software arrangements)
Device vendor		✓ (see specifics of warranty on purchase)	

Device Care:

Students bring their own device for use at Bremer State High School at their own risk. The school will not be responsible for any loss, theft or damage to the device or data stored on the device. In circumstances where a device is damaged by abuse or malicious act of another student, the school will apply consequences in accordance with the Bremer State high School Responsible Behaviour Plan, however Bremer State High School is not liable for the reimbursement or replacement of the device.

Parents and students should consider whether their device requires insurance and whether specific accidental loss and breakage insurance is appropriate for the device. It is advised 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.

Suggestions for students to keep the laptop secure at school:

- Keep the laptop with you at all times. Do NOT leave it in your bag outside of classrooms
- Short-term storage in a locker – short-term storage lockers will be provided in the Library and F block for any student to use for the TEMPORARY storage of their laptops (e.g. safekeeping during a practical lesson or at lunchtimes). Students can safely secure their laptop for the duration of the practical lesson and remove it at the end. NOTE: locks left on a locker at the end of the day may be removed
- Consider engraving the device – this will help identify any lost devices

General precautions

- Food or drink should never be placed near the device
- 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

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch
- Do not carry the device by the screen – carry it holding the base of the laptop
- Do not 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
- Do not clean the screen with a household cleaning product

Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost. The student is responsible for the backup of all data. All files must be scanned using appropriate anti-virus software before being downloaded to the department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents might not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

Through the “Microsoft Office Advantage”, students have access to OneDrive for Students. This is a cloud-based service that is linked to their Office 365 Suite and school log in details. It is recommended that all students back up their files in their OneDrive.

Monitoring and Reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

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

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, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

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

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.

Standard school behaviour management procedures apply for misuse of any BYOx item. While at school, all material on the devices is subject to review by school staff. Students are to connect their device to the designated wireless network only. Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software mechanisms that are in place.

Bremer 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.

Responsible use of BYOx

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

Responsibilities of stakeholders involved in the BYOx program:

School

- BYOX program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cyber safety
- Network and printing connection at school (to print, students must be a current Student Resource Scheme member) and be up to date with payments of school fees
- Internet filtering (when connected via the school's computer network)
- Some technical support (please consult Technical Support section of this booklet)
- Some school-supplied software e.g. Microsoft Office 365
- Printing facilities (to print, students must up-to-date in the Student Resource Scheme)

Student

- Participation in BYOx program induction
- Acknowledgement that the core purpose of device at school is for educational purposes
- Ensure that personal use is kept to a minimum, internet and online communication services are generally used for genuine curriculum and educational actives. Use of unauthorized programs and intentionally downloading unauthorized software, graphics or music that is not associated with learning, is not permitted
- Care of device
- Appropriate digital citizenship and online safety
- Security and password protection — password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students)
- Technical support (please consult Technical Support section of this booklet)
- Maintaining a current back-up of data
- Charging of device at home
- Abiding by intellectual property and copyright laws (including software/media piracy)
- Internet filtering (when not connected to the school's network)
- 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 BYOx Charter Agreement

Parents and caregivers

- Acknowledgement that core purpose of device at school is for educational purposes
- Internet filtering (when not connected to the school's network)
- Encourage and support appropriate digital citizenship and cyber safety with students
- Technical support (please consult Technical Support section of this booklet)
- Required software, including sufficient anti-virus software
- Protective backpack or case for the device
- Adequate warranty and insurance of the device
- Understanding and signing the BYOx Student Charter

The following are examples of responsible use of 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 violating copyright laws
- Using 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
- Taking into or use mobile devices at exams or during class assessment unless expressly permitted by school staff

In addition to this:

Information sent from the Bremer State High 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 computer 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.
- 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 Responsible Behaviour Plan.
- 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.