What is Bring Your Own Device (BYOD)

*Bring your own device (BYOD) refers to technology models where students bring a personally owned device to school for the purpose of learning.*

Bring Your Own Device

Murray Bridge High School is committed to aiding students and staff in creating a 21st Century learning environment. Students and staff are able to access our wireless network with their personal devices (laptops, netbooks, tablets, etc) during the school day. With classroom teacher approval, students may use their own devices to access the internet and collaborate with other students.

Many schools are implementing Bring Your Own Device policies for their students and staff. By allowing students to use their own technology at Murray Bridge High School we are hoping to increase the access all students have to the technology they need to succeed.

We also recognise the importance, and indeed, the pervasion of technology in our everyday lives.

As we prepare students for life in the 21st Century we must equip them with the skills to utilise technology responsibly and empower them for lifelong learning.

To do this effectively, we are adopting a ‘Bring Your Own Device’ (BYOD) policy for students in Years 8 to 12 from the beginning of the 2014 school year.

A successful technology programme is supported by clear standards, policy documents and guidelines. We have prepared the following documents:

- BYOD Policy
- BYOD Fact Sheet
- Digital Citizenship

Information sessions are also planned to assist parents. These sessions are designed to provide further information and an opportunity to ask questions.

2014, Parent Information Evening (6.00pm to 7.00pm in the Drama Workshop)
Wednesday 12 February 2014.

Please refer to FAQs section if you have any questions

Additional questions may be directed to Brian Davis, IT Manager, or send an email to dl.0785.ictadmin@schools.sa.edu.au
21st Century Learning

Murray Bridge High School is committed to moving students forward in a 21st Century learning environment. Murray Bridge High School’s ICT leadership team has implemented a BYOD initiative because we believe that it is a sustainable way for the school to have every child to have access to a device. A device in the hands of every student could extend and enrich learning by:

- Shifting instruction towards more student centred learning, where inquiry and authentic learning are emphasized.
- Focusing on 21st Century Learning, including critical and creative thinking, collaboration, communication, self direction, global awareness and cultural awareness.
- Using online learning tools and digital content
- Increasing student engagement through ICTs

If the devices the students use beyond the school day are the same ones they use for school, the student can seamlessly switch from personal use to learning anytime, anywhere. The learning activities on the device are accessible to the students 24/7, enabling them to pursue personal interests associated with such learning. The students are literally carrying around accessibility to academic learning that can be called up at a moment’s notice.

BYOD Policy

All students and staff have access to the Murray Bridge High School wireless network, including the access to the Internet for teaching and learning.

Access to the Murray Bridge High School IT system is a privilege, not a right. All users will be required to acknowledge receipt and understanding of the BYOD policy in this document and adhere to the Digital Citizenship Guidelines.

Noncompliance may result in suspension or the removal of privileges for a period of time aligned to the Murray Bridge High School Behaviour Management Policy.
BYOD - ICT Policy for personal learning (includes appropriate use of all Wireless Network Capable Digital Devices brought from home for school or class use).

PURPOSE

This policy defines the standards, procedures and expectations for all users who are connecting a personally owned device to Murray Bridge High School’s ICT network or who are using the school’s ICT services data and networks. The policy also applies to software and hardware that is not owned or supplied by the school, especially those that staff and students have acquired for personal use but are not licensed or formally approved by the school.

Electronic and ICT Equipment and devices in this policy include, but are not limited to, computers (such as desktops, laptops & iPads), storage devices (such as USB and flash memory devices, CDs, DVDs, iPads, iPods, MP3 players and Electronic Books), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other technologies as they come into use. Currently school recommended laptops and netbooks are preferred devices due to their compatibility with the school wireless systems and their inbuilt protections against Malware. Devices from other manufacturers may be allowed by the school’s ICT Staff, after assessment for compatibility and, where required, assessment of up to date anti-virus protection. All other devices will have limited or no access to the school’s ICT networks and services.

Access to the school’s ICT networks, infrastructure and data is a privilege and all staff, students and other persons seeking access to the school network must consent to and sign this BYOD policy prior to connecting the device to the school network. Users include all full and part time staff, relief teachers, students, and other agents who use a personally owned, or school owned device to access, share, store relocate or backup any school or student based data. Non sanctioned use of personal devices to back up, store and otherwise access any data owned by the school and stored on our network is strictly prohibited.

RATIONALE

Technology provides students and staff with unique and powerful ways to enhance their learning. Murray Bridge High School supports a learning environment where personalised learning and achievement is enhanced through appropriate and effective access to the tools and resources essential to achieving academic excellence. The school will continue to develop and evaluate cyber safety and e-learning practices.

New technologies play a particularly important role in enabling learning to occur beyond the boundaries of the school. Young people’s familiarity with modern technology, and their engagement in e-learning, enhances curriculum-based learning and networking that extends around the world.

Mobile technologies, chat, blogs, wikis, webcams, reality television and interactive games are intrinsic to their worlds. Current technologies shape their expectations and their abilities to access, acquire, manipulate, construct, create and communicate information.

ICT capabilities and digital literacy are essential skills. The use of ICT will make
significant gains for learners across all ages and curriculum areas.

Whilst acknowledging the role of ICT tools and services it is essential that we protect the integrity, confidentiality and security of all school data and that all employees and students act in accordance with our school policies to ensure that we minimise the risks of the following potential threats:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Potential risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device loss</td>
<td>Devices need to be password protected to minimise the loss or theft of work files</td>
</tr>
<tr>
<td>Data theft</td>
<td>Users need to ensure that sensitive data is not uploaded onto devices and stolen or sold by an employee or unsanctioned third party</td>
</tr>
<tr>
<td>Malware</td>
<td>Viruses, trojans, worms, spyware and other threats are increasingly a risk to our network where personal devices are not adequately protected from malware</td>
</tr>
<tr>
<td>Compliance</td>
<td>Loss or theft of personal or confidential data could expose the school to risk of non-compliance with various child protection, identity theft and privacy laws, so employees and students need to maintain compliance with this and related policies at all times</td>
</tr>
</tbody>
</table>
MONITORING OF DEVICES CONNECTED TO THE SCHOOL NETWORK

The Principal of Murray Bridge High School retains the right to be the final arbitrator of what is, and is not, appropriate content and has overall responsibility for the appropriate access to and use of the school's ICT infrastructure, network and data management, including the right to monitor, access and review all use of school resources and infrastructure. This includes all personal web browsing, and emails sent and received on the school’s ICT facilities.

As part of its quality assurance, data integrity and security processes, the school will establish audit trails capable of tracking the attachment of an external device to the school network in cases of suspected breaches of this policy or misuse of the school’s ICT resources. Such tracking will be able to monitor dates, times and duration of access to ensure that school data and security has not been compromised by external parties.

Consequences for breach of this policy will be determined by the Principal and may include prohibiting an individual from bringing their mobile device to school. The Principal also reserves the right to audit at any time any material on equipment that is owned or leased by the school, and to audit privately owned ICT electronic devices and equipment (including USBs) used at School or at any school related activity.

Connectivity of all staff and student owned devices will be centrally managed by the Murray Bridge High School IT Department, and configurations will be in accordance with the guidelines in place to protect and secure school data and information systems and storage. Configuration of devices will include password protection and encryption, and any other controls essential to isolating and protecting sensitive information accessed from or stored upon personal devices or the school’s network. Staff and students will be expected to adhere to the same security protocols when connected to non-school equipment to help protect any information from being lost or stolen from their devices.
Failure to comply will result in immediate suspension of all network access privileges so as to protect the school’s infrastructure. No student, staff member or relief teacher is to divulge their password to a third party and all personal device users are responsible for bringing their devices to school fully charged and labelled for identification.

Any phone internet connection, such as 3G, or NextG, must be switched off if possible and the device priority pointed to the school’s wireless network. Accessing the internet independently of the school’s proxy servers (i.e. by personal ISP) is not allowed in order to ensure cyber safety.

At the conclusion of a user’s employment or enrolment at the school, all school data, access and email communication will be wiped from the device.

**ICT for Personal Learning and Acceptable Use Policy**

It is the responsibility of every student and employee of Murray Bridge High School to ensure that our ICT resources are never used to abuse, vilify, defame, harass, degrade or discriminate against others. Thus all personal devices must be utilised responsibly, ethically and securely to safeguard the rights of others and the security of all school data, ICT systems and infrastructure.

Thus, the following access controls must be observed at all times:

1. The school’s IT Services Team reserves the right to refuse the connection of personal devices to the School network if such equipment is being used in any way that could potentially cause harm to the school’s systems, data, users or resources.

2. Only appropriately managed and registered devices will be permitted to access the school network and be connected to school data and resources. Such devices must adhere to the school’s authentication requirements at all times.

3. All users must employ reasonable security measures including, but not limited to, passwords, encryption, physical controls and safe storage of personal devices whenever they contain school data. Any attempt to contravene or bypass security or acceptable use procedures will be deemed a contravention of this ICT for Personal Learning and Acceptable Use Policy and will limit the ability of the user to access the school’s ICT network and resources.

4. Staff and students agree to only view, listen to, or access, school appropriate content on their personal devices while at school.

5. Due to copyright, content such as music and games is not to be transferred to other devices or the school’s computer network. Furthermore, students and staff may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from the Principal and those whom they are recording.

*Mobile phone photos, voice and text use by students during the school day are prohibited by this policy.*
TERMS AND CONDITIONS

Examples of inappropriate use that will result in termination of a user’s access and privileges include any activities that create security and/or safety issues for the School network, users, school or computer resources; that expend School resources on content it determines lacks legitimate educational content/purpose; or other activities as determined by the Principal as inappropriate.

Such activities include but are not limited to:

1. Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, and harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.

2. Criminal activities that can be punished under law.

3. Selling or purchasing illegal items or substances.

4. Obtaining and/or using anonymous email sites, spamming, spreading viruses.

5. Causing harm to others or damage to their property.

6. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.

7. Deleting, copying, modifying, or forging other users’ names, emails, files or data, disguising one’s identity, impersonating other users, or sending anonymous email.

8. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.

9. Using any computer/mobile devices to pursue “hacking,” internal or external to the school, or attempting to access information protected by privacy laws.

10. Accessing, transmitting or downloading large files, including “chain letters” or any type of “pyramid schemes.”
11. Intentionally accessing, creating, storing or transmitting material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.


13. Attempting to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities

BYOD Guidelines
Students may use a privately owned electronic “Internet ready” device on the school’s wireless network with teacher or administrator permission.

The use of a privately owned electronic device to support and enhance instructional activities is at the subject teachers discretion. All users of the school network are bound by expectable use agreement whereby individuals will not over use data allowance.

The school wireless network is a monitored service accessed by unique username and password. Inappropriate sites are filtered and blocked when necessary to ensure student use of the internet is for educational purposes.

Students are prohibited from accessing the Internet using any external Internet service e.g 3g devices or other alternatives. A BYOD device is only to be connected via Wi-Fi access only using the students unique username and password. No student shall establish a wireless ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds.

Voice, video, and image capture applications may only be used with teacher permission and relevant to the learning environment whilst being respectful of the rights of others.

The privately owned electronic device owner is the only person allowed to use the device and their unique username and password associated with the device. In the event that a student believes that his/her password has been compromised, he/she should immediately see IT staff to have the password changed.

No school software can be installed on personal devices due to the terms of the licenses unless stated otherwise.

No student shall use any computer or device to illegally collect any electronic data or disrupt networking services.
Devices are brought to school at the students’ and parents’ own risk. In the event that a privately owned device is lost, stolen or damaged, the school is not responsible for any financial or data loss.

The Principal reserves the right to examine the privately owned electronic device and search its contents if there is reason to believe that the student’s device may have inappropriate material. If this is the case this will result in appropriate disciplinary action as specified in the Behaviour Management Policy and may result in removal of privileges and or suspension.

Violation of the school’s BYOD Policy, while using a personal electronic device on the school’s wireless network will result in appropriate disciplinary action as specified in the Behaviour Management Policy and may result in removal of privileges and or suspension.
STUDENT AGREEMENT

The safety of the students at Murray Bridge High School is of paramount concern. Any apparent breach of cyber safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school’s Personal Responsibility Policy in regard to cyber safety practices. In serious incidents, advice will be sought from appropriate external sources, such as the police and/or a lawyer with specialist knowledge in this area. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Students may not use the school’s Internet facilities and ICT resources in any circumstances unless the appropriate BYOD and Acceptable Use Agreement has been signed and returned to the School. Online resources for parents and students are available at www.cybersmart.gov.au

The specific conditions of the User Agreement are outlined below.

I understand that the use of ICT equipment and access to the Internet at Murray Bridge High School must be in support of educational research and learning. I take sole responsibility for use of my accounts and passwords and personally owned devices and will not share my password with others.

I will refrain from accessing any websites, images, computer files, newsgroups, chat groups or other electronic material from any sources that would be considered offensive in the judgement of the school.

I will be courteous and use appropriate language in communication via the Internet. I will refrain from using obscene, harassing or abusive language and will report any occurrences of such usage against me to a member of staff. I will ensure that I do not use ICT resources to abuse, vilify, defame, harass, degrade or discriminate others.

I accept responsibility in regard to copyright protected material. Therefore, I will not download and redistribute software, games, music, graphics, videos or text unless authorised to do so by the copyright owner and/or the school.

I understand that plagiarism (presenting someone else’s work as my own) is unacceptable. Therefore, I will list any downloaded material used in the preparation of assignments in a bibliography and clearly indicate where material has been directly quoted from another source.

I will not reveal personal details of myself or others via ICT resources unless instructed to do so by the school.

I shall not maliciously destroy or steal ICT equipment from the school. Unacceptable or rough use of any equipment belonging to the school, myself or other students or staff will also not be tolerated. If I have damaged ICT equipment I understand that the costs for repair or replacement will be me and my parent/caregivers’ responsibility.
I understand that I am never permitted to use the school network for private storage for non-educational, non-approved files, including games, videos, music, etc.

Students are forbidden to plug any device into the school’s wired network. Any student caught with a device plugged in to the wired network will receive immediate consequences including suspension. The school’s network security system scans and reports on any non school devices plugged in to the school’s wired network.

If I violate any of the terms of this agreement, I will be subject to the consequences outlined below.

**CONSEQUENCES**

The following are consequences for breaches of the BYOD and Acceptable Use Policy:

1. Warning from subject teacher and note in diary which needs to be signed by both the Pastoral Care teacher and the parent. Offences may incur significant penalties including limited or no access to the school’s ICT network and related sources.

2. Student blocked from computer use for a total of 5 school days (excluding days where students are not in the classroom). Year Level Leader to send letter home informing parents of this serious consequence. (Students are still expected to complete all school work on time.)

3. In circumstances, which involve harassment, accessing inappropriate material or materials that compromise or attempt to compromise the school’s network, students will be automatically blocked for a 5 day period or until ethical and legal compliance issues have been resolved.

4. When a student is found to have maliciously damaged equipment, they will be blocked from computer use for a 10-day period; unacceptable or rough use of the equipment will also not be tolerated. Any damaged equipment may have costs recovered for repair or replacement by the student/parent/caregiver who are responsible for the damaged equipment.

5. Students, who fail to comply with the policy guidelines and procedures for personally owned devices, will have their access and connectivity privileges suspended until compliance is guaranteed by the student and family.

6. Students who damage or misuse others’ personally owned devices will be responsible for any replacement or repair costs associated with such damage or theft.
CLOUD COMPUTING SERVICES
USER AGREEMENT- STUDENTS

This User Agreement sets out the terms on which you may access cloud computing services provided by the school, including Google Apps and Edublogs (Cloud Computing Services). Cloud computing involves the use of web-based services (rather than a PC or school server) for functions such as email, blogs and data storage.

You will need to sign and return this User Agreement before you will be allowed to access the Cloud Computing Services.

By signing this User Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this User Agreement, including the consequences of any breach of the terms.

1. Privacy Consent

Information that you transfer or store using the school’s Cloud Computing Services (including email, blogs and data storage) may be stored by Google, Edublogs or other Cloud Computing Service providers (Cloud Providers) in the United States of America, or such other country as the Cloud Providers may decide. By using the school’s Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

2. Acceptable Use

You agree that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

(a) give your account password to anyone else;

(b) access (or try to access) anyone else’s account, or try to defeat any security controls;

(c) send or help to send unsolicited bulk email (spam);

(d) publish, send or knowingly access material that is pornographic, hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;

(e) knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or

(f) disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.

3. Monitoring
You agree that IT Support Staff responsible for IT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately. If you notice a problem with the Cloud Computing Services, or if you think that someone is trying to access your account (or someone else’s account), you agree that you will tell the school’s IT Support Staff straight away.

4. Suspension or termination of use and other consequences

If there is an emergency security issue, or if you are suspected of making inappropriate use of the Cloud Computing Services, your access to the Cloud Computing Services may be suspended or terminated. This means that you might not be able to access your school’s ICT services, including your school email account. If you are found to have made inappropriate use of the Cloud Computing Services, the school may also apply other disciplinary consequences.

Acceptable Devices

Which should I bring?

There is a choice of purchasing a device or bringing your own device if you already have one and it meets the technical specifications to join the school network. In conjunction with Learning With Technologies and Acer we have a Parent Online Purchasing Portal where devices can be purchased by credit card, PayPal or interest free finance (subject to approval). The Purchasing Portal is located at www.lwt.com.au/orders/murraybridgehs. There is a choice of either a laptop or netbook and are available at DER (Digital Education Revolution) prices. These devices will have accidental damage insurance, a carry bag and have preloaded the Murray Bridge High School operating system. They will be preconfigured to join the Murray Bridge High School wireless network and warranty will be supported by the Murray Bridge High School IT Support Staff.

Though laptops and netbooks are heavier to carry around, they allow you to be more productive in situations where you will be creating documents, movies, or other digital media.

Minimum requirements are Windows 7 or higher, OSX Lion or higher, Wireless 802.11n 2.4 or 5Ghz, 2GB of RAM, Core i3 processor or higher, 6 cell battery (9 cell preferred).

Students bringing their own devices may find they do not meet the standards to be able to join the Murray Bridge High School network. They will also not be supported by the MBHS IT Support Staff.
**Digital Citizenship Policy**

Digital Citizenship is a concept which helps teachers and parents to understand what young people should know to use technology appropriately. Digital Citizenship is more than just a teaching tool; it is a way to prepare all users of technology for a society full of technology.

The Murray Bridge High School IT Committee has a digital citizenship policy to focus on student learning and student needs with an emphasis on how to teach students to work, live and share in digital environments. This is founded on the belief that students will be using online technologies as part of learning to prepare for life in a globalized connected society.

**Digital Citizenship Guidelines**

This Agreement has five conditions of being a Digital Citizen.

- **Respect Yourself.** I will show respect for myself through my actions. I will select online names that are appropriate, I will consider the information and images that I post online. I will consider what personal information about my life, experiences, experimentation or relationships I post. I will not be obscene.

- **Protect Yourself.** I will ensure that the information, images and materials I post online will not put me at risk. I will not publish my personal details, contact details or a schedule of my activities. I will report any attacks or inappropriate behavior directed at me and I will seek support from appropriate people or organizations. I will protect passwords, accounts and resources.

- **Respect Others.** I will show respect to others. I will not use electronic mediums to bully, harass or stalk other people. I will show respect for other people in my choice of websites, I will not visit sites that are degrading, pornographic, racist or inappropriate. I will not abuse my rights of access and I will not enter other people’s private spaces or areas.

- **Protect Others.** I will protect others by reporting abuse, not forwarding inappropriate materials or communications; and not visiting sites that are degrading, pornographic, racist or inappropriate. I will moderate unacceptable materials and conversations, reporting conversations that are inappropriate or unacceptable.

- **Respect Intellectual property.** I will request permission to use resources. I will suitably cite any and all use of websites, books, media etc. I will acknowledge all primary and secondary sources. I will validate information. I will use and abide by the fair use rules.

- **Protect Intellectual Property.** I will request to use the software and media others produce. I will use free and open source alternatives rather than pirating software. I will purchase, license and register all software. I will purchase my music and media,
and refrain from distributing these in a manner that violates their licenses. I will report vandalism and damage I will act with integrity.
Software

Required Software

The Department has negotiated with Microsoft to make Microsoft Office available to students at a cost of $25.00 per year. This will be available and installed on portable devices by the IT Staff (Media is not supplied). When students finish Year 12 they will be able to keep the Office program which will assist them in their tertiary studies.

The minimum requirement is Office 2007 or above.

Recommended Web Browsers

We recommend having at least two updated web browsers on your device. We have found the following browsers to be the most stable and reliable:

Internet Explorer
Safari
Google Chrome
Firefox
**Tech Support**

**Network Connection**
Students need to connect to the school’s wireless network by following the Accessing Murray Bridge High School Wireless Network document and using the username and password provided to each student at the start of the year.

Students who are having technical issues connecting their technology tool can then visit the IT help desk.

An initial scheduled time will be made in Pastoral Care groups to help support students to connect students device.

**Charging**
It is the responsibility of the student to bring their device to school charged. Devices cannot be charged at school due to the Work Health and Safety regulations.

**Printing**
Currently there is no printing option from a personally owned device. This will change in the future as we update the way the school’s printers are configured and dispersed throughout the school. Until then students have the option of accessing their document from a school computer to print or if they have a USB.

A printing program will be installed to facilitate web based printing. This program will also monitor and track print jobs. Year 8, 9 and 10 students will be issued a print credit of $3.00 per term. Year 11 and 12 students will be issued a print credit of $5.00 per term. This is covered by the Materials and Services component of school fees.

Printing will be charged at 5c per page for black and white and 20c for colour. A print kiosk will be located in the Resource Centre where students will be able to purchase additional credit by using coins.

**Insurance and Liability**
Murray Bridge High School does not accept liability for any loss, damage or theft of any device that is brought to school under the program. The responsibility for the storage, safe-keeping and care of the device is the responsibility of the device owner. The school’s insurance policy does not apply to these devices; instead these are covered by the user’s insurance policy. As such it is strongly recommended that families ensure that the details such as serial numbers and receipts of purchase for these devices are stored securely at home for insurance purposes.
FAQS

What is Bring Your Own Device (BYOD)
Bring Your Own Device (BYOD) refers to technology models where students bring a personally owned device to school for the purpose of learning.

How do I connect to the Murray Bridge High Schools wireless network?
Please Refer to the following Document:

Accessing Murray Bridge High School Wireless Network

Is student internet monitored?
Students internet access is filtered whilst they are using the school’s network. Their complete web history is also logged and monitored accordingly.

Where do I go for support?
If students are not able to connect to the school’s wireless network and have followed the steps of the *Accessing Murray Bridge High School Wireless Network* documents, students can visit the IT office located in A Block between 9am-3pm.

My laptop was damaged/stolen when I brought it to school. Who should I contact?
Bringing your own device to school can be useful; however some risks are involved as well. It is always a good idea to record the device’s serial number in case of theft and have your own insurance. The school is not responsible for the theft of a device, nor is the school responsible for any damage done to the device while at school. Any time a theft occurs, you should speak with your Year Level Leader to make them aware of the issue. Devices purchased through the Parent Online Purchasing Portal are only covered by accidental damage insurance. Parent/Caregivers will need to ensure that their devices are covered for other situations under their own insurance policies.

Can my child charge their device at school?
It is the responsibility of the student to bring their device to school charged. **Under no circumstances can a device be plugged into a powerpoint at school.**

Can my child use the printer from this device?
Devices purchased through the Portal will be able to print. Other personal devices may not meet the technical specifications to access the Murray Bridge High School wireless network.

What happens to students work if the computer hard drive fails or the computer is stolen?
We recommend and encourage students to use additional backup measures to keep their documents safe such as: external hard drives, USB drives, cloud storage.
Accessing the Murray Bridge High School Wireless Network

The following is a quick reference guide outlining the process for connecting to the MBHS student wireless network for BYOD. For more information regarding connecting to a wireless network on different devices, please refer to the FAQ tab of the Technology page on the Murray Bridge High School Website.

**Accessing the MBHS Wireless Network**
1. Connect to the MBHS Wireless networks, using your device’s wireless network adaptor.

2. Once connected, open the web browser on your device and you will be automatically redirected to the Student WiFi Portal.

3. Input your MBHS Username and Password followed by the Login button to connect to the chosen network.

4. If your login attempt is successful, you will be automatically redirected to the Murray Bridge High School Student Portal and ready to start searching the internet.

*Please be aware that these connections have active web content filtering. Your browsing history will be logged and monitored.*
**Student and Parent/caregiver**

**BYOD Use Agreement**

I understand and agree to Murray Bridge High School’s BYOD and Digital Citizenship Policy.

I am aware that by failing to comply with requirements of the BYOD policy I may have my privileges removed in line with the MBHS Behavior Management Policy.

Name of Student........................................Pastoral Care Group .........................

Signature of student........................................Date........................................

Parent Caregiver........................................Date........................................

Please note: This agreement will remain as long as your child is enrolled at this Murray Bridge High School. If it necessary to amend any information, you will be advised.

PLEASE RETURN A SIGNED COPY TO YOUR CHILD’S PASTORAL CARE TEACHER ASAP. PLEASE KEEP A COPY FOR YOUR OWN REFERENCE.