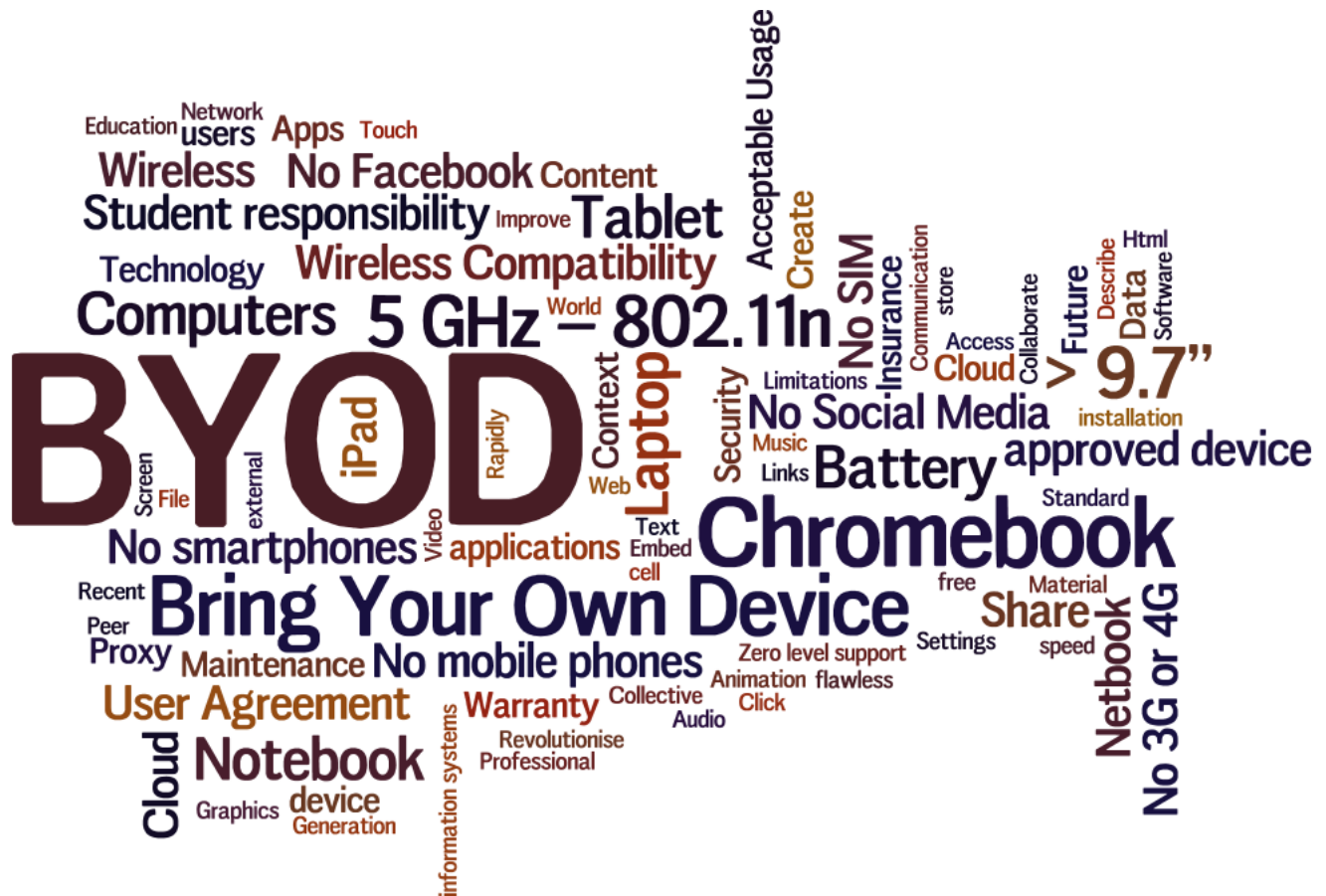
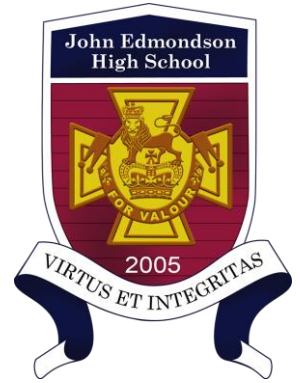


John Edmondson High School



BYOD Program Handbook

John Edmondson High School



'Bring Your Own Device' (BYOD) Policy

Rationale

John Edmondson High School recognises the importance of technology in connected learning and the positive effects it has on engagement and achieving learning outcomes. In order to prepare students for an ever-changing world beyond school, teachers at JEHS support the philosophy that technology can play a significant role in learning.

BYOD is a solution where students bring and use their own device be it a tablet, laptop or other approved device at school, in order to access the Internet using the school's wireless network for learning.

BYOD Objectives

Students are allowed to bring any device that meets our **BYOD Device Specifications**.

These devices can only be used at school with the knowledge and written approval of the parent/guardian & JEHS. Students and parents/guardians must read & agree to the '**JEHS Technology Policy**', '**JEHS BYOD Policy**' and the '**Digital Devices and Online Services for Students**'. The signing and returning of the '**BYOD User Agreement**' constitutes such knowledge and approval. All signed agreements will be kept on file on the school network.

A BYOD contact at school will be available to answer questions and to give assistance. However, the school does not manage, repair, support, own or warrant the device - it's your choice and your device. Our 'Technical Support Team' will be able to assist with questions about device specifications to ensure it can be connected to the school's Wi-Fi network.

It is the student's responsibility to save and backup their own work. Backup facilities are only carried out on the files that the student has uploaded to the school server. No backup of personal files will be provided. No printing services will be provided by the school from these devices. Any work requiring printing will be processed through school based desktop computers or at home.

Students can use their BYOD to access the school's cloud based 'Learning Management System' (LMS) called 'CANVAS' at school and can also take full advantage of it at home. CANVAS will allow students and teachers to engage with each other in an educational environment outside their classroom.

BYOD: Type of devices permitted

Various devices in a range of price categories will meet the Device Specification. Devices include a Chromebook, laptop, or a tablet. Chromebooks or Tablets may be half the price of larger sized Ultrabooks or Laptops.

Mobile phones and devices with a screen size less than 9.7 inches will not be allowed under the JEHS BYOD program as they do not provide an acceptable screen size for effective learning support.

The device must be able to connect to the 5 GHz - 802.11n standard wireless signal provided by the DEC Wireless infrastructure. Students are not permitted to use a SIM card in the device and are not permitted to use any 3G or 4G connections to connect to the Internet or any applications.

BYOD and Internet Connectivity

Internet is provided by the school's secured wireless network. The school's Internet is filtered and monitored and blocks unacceptable or banned internet sites including some social media sites such as Facebook. This filtering is only applied when the student is at school. Internet access on the device will be filtered through the school's and DoE's proxy filtering system. While students are at school, they are prohibited from connecting to other networks.

SIM CARDS in DEVICES ARE NOT ACCEPTABLE. All SIM cards should be removed and students must not use any 3G or 4G connections to connect to the Internet or any applications. Any student who connects or 'tethers' their device to their mobile phone in order to gain access to the Internet will be breaching the BYOD User Agreement and as such school discipline consequences for the breach will apply.

Device Software

Chromebooks, Laptops, Tablets are not all the same. They offer different types of software and have different functions.

The Department of Education (DoE) provides the Adobe Creative Cloud applications & Microsoft Applications at no cost to students.

Students can also access 'Google Apps for Education' for free through their Google Education account, which is linked to the student's DoE Portal account.

The Adobe applications are currently available for download by students through their portal. Microsoft Windows and Office products are also available from their student portal.

BYOD: Acceptable Use of Devices - Terms & Conditions

- Students and parents must sign and return the '**JEHS Bring Your Own Device User Agreement**' in order to bring and use an approved technology device to school.
- Students are to always use these devices responsibly at school and **must** follow '**JEHS Technology Policy**', '**JEHS BYOD Policy**' and the '**Digital Devices and Online Services for Students**' at all times. Devices must not be used in a way that disrupts or is likely to disrupt the learning environment or interfere with the operation of the school or Department of Education (DoE).
- Devices are to be on silent at all times during lessons unless teachers direct otherwise. Teachers may choose to insist all students place their devices face down, or closed, on their desks.
- Use of devices during class time is solely at teacher's discretion. Students must follow teacher's instructions and not interrupt their own or other students' learning.
- Misuse of a device may result in confiscation. Depending on the severity of the breach, the return collection of the device will be negotiated.
- Students are not permitted to use any electronic device to record audio or video media or take photographs of any student or staff member, including lessons, without the knowledge and permission of a teacher. Failing to adhere to this rule may result in suspension and in extreme cases; the matter may be referred to police. The distribution of any unauthorised media may result in disciplinary action including but not limited to suspension, criminal charges, and expulsion.
- Devices must not be used to bully, intimidate, harass others through SMS or text messaging or through photographic, video or other data transfer system/application available on the device. Failing to adhere to this rule may result in suspension and in extreme cases; the matter may be referred to police.
- Devices must not be used to download or otherwise access inappropriate material on the internet such as child abuse, pornographic or other offensive material
- Devices must not be used to film fights or other criminal behaviour involving students that occur at school, during school activities or while on the way to or from school
- Devices must not be used in a way that threatens or is likely to threaten the safety or wellbeing of any person or for any use that is in breach of any law.
- Students who bring devices to school must take responsibility for them. Staff members take no responsibility for such devices and it is not possible for them to carry out lengthy investigations if a device goes missing or if a device gets damaged.
- No backup or printing services will be provided by the school.
- Students who persistently misuse a device may face suspension and may have their privilege of bringing it to school removed.
- Devices must not be attached to any school-owned equipment without the permission of a teacher.
- Devices must not be used to hack or bypass any hardware and software security or filters implemented by the Department of Education or the school.
- Students should not use any device to search for, link to, access or send anything that is offensive, pornographic, threatening, abusive, defamatory or considered to be bullying.

- Students must be aware of appropriateness of communications when using school or personally owned devices. Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students.
- Students may not utilise any technology to harass, threaten, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. This unacceptable student behaviour is known as cyber bullying and will not be tolerated. Any cyber bullying that is determined to disrupt the safety and/or well-being of the school is subject to disciplinary action.
- Students are not permitted to use unacceptable devices under the school's BYOD program. These include, but are not limited to, mobile phones or any device with a screen size less than 9.7 inches.
- JEHS attempts to provide a safe Internet experience for students by deploying the department's filtering technology. To utilise the school's wireless network, students are required to log in through their DEC Student Portal. While we are aware that students have access to the internet through mobile phones, **the use of mobile phones as a BYOD solution is prohibited.**
- Students are prohibited from connecting to other networks at school. All SIM cards must be removed and students must not use any 3G or 4G connections to connect to the Internet or any applications. Any student who connects or 'tethers' their device to their mobile phone in order to gain access to the Internet will be breaching the BYOD User Agreement and as such school discipline consequences for the breach will apply.
- When at school, students will use their wireless connection exclusively for educational purposes. Activities such as downloading files not related to schoolwork, playing computer games or watching movies is not permitted and breaches acceptable use of the school wireless network. Students using the wireless network for anything other than educational purposes could result in disciplinary action.
- Students should use strong passwords and have suitable privacy controls. They should neither let other students use their device nor should they reveal their passwords to another individual.
- Students who are also enrolled with TAFE or have a TAFE account are not permitted to use TAFE logins at school. Use of TAFE account at school will be considered as breach of the User Agreement and may result in disciplinary action.
- This device is owned by you or the student. However, a student must remember that their teachers will be given full access to the device under the user agreement. If a student would not want a teacher to see something, then it should not be on the device. The space on the device should be reserved for applications to support learning.
- JEHS reserves the right to access & inspect a student's personal device if there is reason to believe that the student has violated any Department of Education policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device. Violations of any school policies, administrative procedures or school rules involving a student's personally owned device will result in confiscation of the device, loss of privileges to use the device in school and/or school's disciplinary action.

John Edmondson High School

BYOD - Device Specifications Checklist



Hardware Specifications

Wireless Compatibility

This is the most important specification as there will be no Internet access if your device does not comply

Device must have **5GHz - 802.11n** standard to connect to school's Wi-Fi network

*Devices must be dual band to connect to both 2.4GHz and 5GHz, however **5GHz – 802.11n** is a must.*

3G or 4G connections; All SIM cards must be removed and students must not use any 3G or 4G connections to connect to the Internet or any applications.

Form Factor

Chromebook, Laptop or Tablet

The device **MUST** have a minimum of 9.7" diagonal screen size. A larger screen size is recommended for creative or technical work

It is recommended that the device have a physical keyboard and a wireless mouse to make it easier for typing and navigation.

A mobile phone is NOT an acceptable device.

Storage Space

Most new machines will meet the needs of students. We are encouraging students to utilise cloud based storage for their work so that they can access it from all locations and devices.

Therefore storage space is not too critical. Below is just a guide;

- Minimum 16 GB storage on a Chromebook or a Tablet.
- Minimum 64 GB storage on a Windows device.

A minimum of 2GB RAM (memory) is recommended for tablets and Chromebooks and a minimum of 8GB RAM for Laptops.

Battery Life

Advertised battery life of at least **six hours** without charge

Note: There are no facilities to charge laptops at school.

Note: Students can manage this by ensuring the power save option is enabled on the computer and that the computer is fully charged over night for use at school each day.

Operating System

The device must have the most up to date operating system for its type. For example;

- Latest Google Chrome OS
- Microsoft Windows 10, or newer
- Apple MacOS X 10.6 or newer

Note: Chrome is the operating system on the Chromebooks. This OS does NOT run any of the Windows products. Instead, it provides a range of applications that work in an internet browser, eg Google Apps. This software can open and edit Microsoft and Adobe documents.

Up to date Operating system, Antivirus software and application updates are student's responsibility

Additional Considerations

The following are not *requirements* of the BYOD program, but are recommended for your consideration.

Protective cover/case

Students usually carry their devices in their school bag. It is important that the device is buffered from damage. A hard cover or a case containing memory foam for added protection is essential.

Insurance; Accidental loss & breakage	It is recommended to purchase devices with insurance to include loss and accidental damage; however it is your choice.
Warranty; Length and type of warranty	<p>Devices can be purchased with different warranties. The things to consider here are. The length and type of warranty.</p> <p>Length of Warranty: We are expecting the student to have the device for at least a few years. The cost of extended warranty versus replacing the device needs to be considered.</p> <p>Types of Warranty: There are two options for types of warranty;</p> <p>Back-to-base is the cheapest but would mostly require the device to be packaged and posted back to the supplier for repair.</p> <p>Onsite warranty is more expensive and would usually mean that a repairer would come to your home and fix the device.</p> <p>You will need to weigh up the cost of replacing the device against the cost of insurance or extending the warranty. This is a decision parents will need to make at the point of purchase.</p>

Software Specifications

Students will need to perform various tasks on the device and therefore will need to have relevant software for each task. Rather than look at software in terms of brands, the BYOD approach we are taking means that students will utilise a number of different devices within the classroom with different brands of software. For example a student may use Google Apps, Microsoft Office, Apple Pages or Open Office Text Document to create a word processed document. The software specification is, therefore, about what students will need to do.

There is a growing move towards applications being delivered through the Internet in what has been termed '**the cloud**'. Before purchasing expensive software, please read the following;

Cloud based software

- **Google Apps** allow the user to log into Google and create documents, presentations, spreadsheets, drawings and forms or simple databases. It provides the ability to work collaboratively and share documents across a variety of devices and operating systems. Google Apps is **free** to students.
- **Microsoft Office 365** offers a similar service to Google Apps and is also **free** to students.

*Students have access to both Microsoft 365 and Google Apps through their DEC portal at **no cost**.*

Other software not in the cloud that is available free but not essential

- **Adobe Enterprise Agreement:** Adobe software is used for developing online application, graphics, music, web design etc. Adobe has offered a **free** student version of their software that can be downloaded onto student's BYOD. Due to the processing power and memory needed to run Adobe software, a low end BYOD will not be suitable. This will not work on a Chromebook. If students need access to this level of software they will utilise the specialist technology spaces within the school.

Access the internet to research create, communicate and collaborate	Any modern & up to date web browser. Chromebooks run only on Google Chrome. On Windows and Apple based computers you can run Internet Explorer, Google Chrome or Mozilla Firefox. These are free to download.
Create documents	Any word processor. Examples include Microsoft Word, Apple Pages, Google documents (free in the cloud)
Create presentations	Any presentation tool. Examples include Microsoft PowerPoint, Apple Keynote, Google presentations (free in the cloud)
Create spread sheets	Any spreadsheet tool. Examples include Microsoft Excel, Apple Numbers, Google spread sheets (free in the cloud)
Take notes	Students can use their device to take notes either through a word processor, or Apps like OneNote, Notability or Evernote

For more information and answers to FAQ's visit the school's website:

<http://www.jedmondson-h.schools.nsw.edu.au>

John Edmondson High School

Technology Acceptable Use Policy



As technology is used more and more in schools it is important that policies and contracts are put in place to govern its use – and to protect the school and students. **John Edmondson High School's Technology Acceptable Use Policy** applies to the use of school owned devices or BYOD devices & any related technology.

The purpose of this policy is to;

- ensure that the computers are kept in good working order to ensure maximum access to students
- ensure that the school's computers are used only for educational purposes and
- provide a safe learning environment for all students

Assignments and Homework

Assignments and homework completed on computer should be:

- the students' own work.
- formatted in such a manner that is easy to find and read information.
- set out with a heading or title page, body and bibliography.
- edited so that information directly downloaded from electronic sources has been synthesised by the student and put into the context of the assignment. Any work directly downloaded and handed in will not be accepted.
- set out in a way that all sources of information are acknowledged either in the bibliography or by direct mention in the assignment.
- handed in for marking as a hard copy unless otherwise stated by the teacher.

Plagiarism and Copyright

- Users will not plagiarise works that they find on the Internet or the school Intranet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.
- Under no circumstances will illegal copies of copyrighted software be made available or allowed on the Department of Education or the school equipment.

Student Personal Safety & Respect for Privacy

- Users will not re-post a message that was sent to them privately without permission of the person who sent them the message.
- Students will not post personal contact information about themselves. Personal contact information includes telephone number, home address, work address, etc. An e-mail address may be used where it is necessary to receive information.
- Students will not post personal contact information or any other information about other people without their permission. This includes their telephone number, home address, work address and other details. In addition, users will not include any reference to Department of Education or the school personnel or users, including their names and pictures, without their permission.

Illegal or Destructive Activities

- Users will not attempt to gain unauthorised access to the Department of Education network, the school computer network or any other computer network. Users must not go beyond their authorised access. This includes attempting to log in through another user's account or access another user's files.
- Users will not make deliberate attempts to disrupt any computer system performance or destroy data.
- Users will not use the Department of Education network, the school computer network or any other computer network to engage in any illegal act.
- Users will not attempt to harm or destroy hardware and/or data of another user. This includes, but is not limited to, the uploading or creation of computer viruses. Report all faults and malfunctions to your teacher.
- Any of these actions will result in disciplinary action.

System Security

- Users are responsible for the use of their individual account (and password) and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person.
- Users are not permitted to connect USB drives for use on any school computers.

Inappropriate Conduct

- Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.
- Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Users will not post information that, if acted upon, could cause damage or a danger of disruption.

- Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Users will not harass another person. Harassment is acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, the user must stop.
- Users will not post false or defamatory information about a person or an organisation.

Inappropriate Access to Material

- Users will not use Department of Education or the school computer network to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). Exceptions may be made if the purpose of such access is to conduct research, and if such access has been approved by the teacher.
- If a user inadvertently accesses such information, they should immediately exit the site and disclose the inadvertent access to their teacher. Repeated access to such sites will result in disciplinary action.

John Edmondson High School



'Bring Your Own Device' (BYOD) Policy

Rationale

John Edmondson High School recognises the importance of technology in connected learning and the positive effects it has on engagement and achieving learning outcomes. In order to prepare students for an ever-changing world beyond school, teachers at JEHS support the philosophy that technology can play a significant role in learning.

BYOD is a solution where students bring and use their own device be it a tablet, laptop or other approved device at school, in order to access the Internet using the school's wireless network for learning.

BYOD Objectives

Students are allowed to bring any device that meets our **BYOD Device Specifications**.

These devices can only be used at school with the knowledge and written approval of the parent/guardian & JEHS. Students and parents/guardians must read & agree to the '**JEHS Technology Policy**', '**JEHS BYOD Policy**' and the '**Digital Devices and Online Services for Students**'. The signing and returning of the '**BYOD User Agreement**' constitutes such knowledge and approval. All signed agreements will be kept on file on the school network.

A BYOD contact at school will be available to answer questions and to give assistance. However, the school does not manage, repair, support, own or warrant the device - it's your choice and your device. Our 'Technical Support Team' will be able to assist with questions about device specifications to ensure it can be connected to the school's Wi-Fi network.

It is the student's responsibility to save and backup their own work. Backup facilities are only carried out on the files that the student has uploaded to the school server. No backup of personal files will be provided. No printing services will be provided by the school from these devices. Any work requiring printing will be processed through school based desktop computers or at home.

Students can use their BYOD to access the school's cloud based 'Learning Management System' (LMS) called 'CANVAS' at school and can also take full advantage of it at home. CANVAS will allow students and teachers to engage with each other in an educational environment outside their classroom.

BYOD: Type of devices permitted

Various devices in a range of price categories will meet the Device Specification. Devices include a Chromebook, laptop, or a tablet. Chromebooks or Tablets may be half the price of larger sized Ultrabooks or Laptops.

Mobile phones and devices with a screen size less than 9.7 inches will not be allowed under the JEHS BYOD program as they do not provide an acceptable screen size for effective learning support.

The device must be able to connect to the 5 GHz - 802.11n standard wireless signal provided by the DEC Wireless infrastructure. Students are not permitted to use a SIM card in the device and are not permitted to use any 3G or 4G connections to connect to the Internet or any applications.

BYOD and Internet Connectivity

Internet is provided by the school's secured wireless network. The school's Internet is filtered and monitored and blocks unacceptable or banned internet sites including some social media sites such as Facebook. This filtering is only applied when the student is at school. Internet access on the device will be filtered through the school's and DoE's proxy filtering system. While students are at school, they are prohibited from connecting to other networks.

SIM CARDS in DEVICES ARE NOT ACCEPTABLE. All SIM cards should be removed and students must not use any 3G or 4G connections to connect to the Internet or any applications. Any student who connects or 'tethers' their device to their mobile phone in order to gain access to the Internet will be breaching the BYOD User Agreement and as such school discipline consequences for the breach will apply.

Device Software

Chromebooks, Laptops, Tablets are not all the same. They offer different types of software and have different functions.

The Department of Education (DoE) provides the Adobe Creative Cloud applications & Microsoft Applications at no cost to students.

Students can also access 'Google Apps for Education' for free through their Google Education account, which is linked to the student's DoE Portal account.

The Adobe applications are currently available for download by students through their portal. Microsoft Windows and Office products are also available from their student portal.

BYOD: Acceptable Use of Devices - Terms & Conditions

- Students and parents must sign and return the '**JEHS Bring Your Own Device User Agreement**' in order to bring and use an approved technology device to school.
- Students are to always use these devices responsibly at school and **must** follow '**JEHS Technology Policy**', '**JEHS BYOD Policy**' and the '**Digital Devices and Online Services for Students**' at all times. Devices must not be used in a way that disrupts or is likely to disrupt the learning environment or interfere with the operation of the school or Department of Education (DoE).
- Devices are to be on silent at all times during lessons unless teachers direct otherwise. Teachers may choose to insist all students place their devices face down, or closed, on their desks.
- Use of devices during class time is solely at teacher's discretion. Students must follow teacher's instructions and not interrupt their own or other students' learning.
- Misuse of a device may result in confiscation. Depending on the severity of the breach, the return collection of the device will be negotiated.
- Students are not permitted to use any electronic device to record audio or video media or take photographs of any student or staff member, including lessons, without the knowledge and permission of a teacher. Failing to adhere to this rule may result in suspension and in extreme cases; the matter may be referred to police. The distribution of any unauthorised media may result in disciplinary action including but not limited to suspension, criminal charges, and expulsion.
- Devices must not be used to bully, intimidate, harass others through SMS or text messaging or through photographic, video or other data transfer system/application available on the device. Failing to adhere to this rule may result in suspension and in extreme cases; the matter may be referred to police.
- Devices must not be used to download or otherwise access inappropriate material on the internet such as child abuse, pornographic or other offensive material
- Devices must not be used to film fights or other criminal behaviour involving students that occur at school, during school activities or while on the way to or from school
- Devices must not be used in a way that threatens or is likely to threaten the safety or wellbeing of any person or for any use that is in breach of any law.
- Students who bring devices to school must take responsibility for them. Staff members take no responsibility for such devices and it is not possible for them to carry out lengthy investigations if a device goes missing or if a device gets damaged.
- No backup or printing services will be provided by the school.
- Students who persistently misuse a device may face suspension and may have their privilege of bringing it to school removed.
- Devices must not be attached to any school-owned equipment without the permission of a teacher.
- Devices must not be used to hack or bypass any hardware and software security or filters implemented by the Department of Education or the school.
- Students should not use any device to search for, link to, access or send anything that is offensive, pornographic, threatening, abusive, defamatory or considered to be bullying.

- Students must be aware of appropriateness of communications when using school or personally owned devices. Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students.
- Students may not utilise any technology to harass, threaten, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. This unacceptable student behaviour is known as cyber bullying and will not be tolerated. Any cyber bullying that is determined to disrupt the safety and/or well-being of the school is subject to disciplinary action.
- Students are not permitted to use unacceptable devices under the school's BYOD program. These include, but are not limited to, mobile phones or any device with a screen size less than 9.7 inches.
- JEHS attempts to provide a safe Internet experience for students by deploying the department's filtering technology. To utilise the school's wireless network, students are required to log in through their DEC Student Portal. While we are aware that students have access to the internet through mobile phones, **the use of mobile phones as a BYOD solution is prohibited.**
- Students are prohibited from connecting to other networks at school. All SIM cards must be removed and students must not use any 3G or 4G connections to connect to the Internet or any applications. Any student who connects or 'tethers' their device to their mobile phone in order to gain access to the Internet will be breaching the BYOD User Agreement and as such school discipline consequences for the breach will apply.
- When at school, students will use their wireless connection exclusively for educational purposes. Activities such as downloading files not related to schoolwork, playing computer games or watching movies is not permitted and breaches acceptable use of the school wireless network. Students using the wireless network for anything other than educational purposes could result in disciplinary action.
- Students should use strong passwords and have suitable privacy controls. They should neither let other students use their device nor should they reveal their passwords to another individual.
- Students who are also enrolled with TAFE or have a TAFE account are not permitted to use TAFE logins at school. Use of TAFE account at school will be considered as breach of the User Agreement and may result in disciplinary action.
- This device is owned by you or the student. However, a student must remember that their teachers will be given full access to the device under the user agreement. If a student would not want a teacher to see something, then it should not be on the device. The space on the device should be reserved for applications to support learning.
- JEHS reserves the right to access & inspect a student's personal device if there is reason to believe that the student has violated any Department of Education policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device. Violations of any school policies, administrative procedures or school rules involving a student's personally owned device will result in confiscation of the device, loss of privileges to use the device in school and/or school's disciplinary action.

John Edmondson High School BYOD - FAQ's



What is BYOD?

BYOD stands for Bring Your Own Device. BYOD is a program where students will be able to bring and use their own device; be it a chromebook, tablet, laptop or other approved device at school, in order to access the school's filtered Internet service for learning.

What types of devices can my child bring to school?

Students may bring devices such as chromebooks, laptops, netbooks, and tablets. The exact specifications can be found in the 'JEHS BYOD – Device Specifications Checklist'. Please be aware devices such as gaming devices are not part of the BYOD program.

Will any device do?

BYOD is just that. It is your device. Students can use a device brand and operating system of their choice as long as they meet the JEHS BYOD Device Specifications.

Can my child use their Smartphone or iPod touch as a BYOD device?

No. Smartphones or iPod touch devices do not provide an acceptable screen size for effective learning support. These devices are also generally equipped with SIM cards. These devices are unacceptable devices under the BYOD program.

When can my child bring and use their own device at school?

Before students can use the device within the school, parents and students will need to sign and return to school the BYOD User Agreement, after reading and accepting the terms of the JEHS BYOD Policy, JEHS Technology Acceptable Use Policy and the Digital Devices and Online Services for Students. The program starts in 2016.

Who maintains and pays for these devices brought to school?

These devices will be purchased by and remain the property of the student/family. Any maintenance and warranty of devices are also the student's responsibility. The Internet service provided by the school is free for students to use on their devices.

How do I acquire a new device?

New devices can be purchased from any reputable retailer, just take along the 'JEHS BYOD – Device Specifications Checklist'.

Can my child customise or individualise their device?

The device is owned by the family. As such, students are allowed to install whatever they wish on their devices. However, students must remember that their teachers will be given full access to the device for learning support purposes under the user agreement. If a student would not want a teacher to see something, then it should not be on the device.

Can the device be charged at school?

There are no charging facilities provided at school. It is the student's responsibility to ensure the device has enough charge to last the whole school day. Under the user agreement, students are responsible to bring their device fully charged for use every day. Generally, a fully charged chromebook will last for up to 9 hours without charging.

What services for backup and printing will be provided by the school?

It is the student's responsibility to save and backup their own work. Backup facilities are only carried out on the files that the student has uploaded to the school server. No backup of personal files will be provided. No printing services will be provided by the school from these devices. Any work requiring printing will be processed through school based desktop computers or at home.

How will my child access the school wireless network/Internet? Can they use their own Internet?

Internet is provided by the school's 5 GHz secure wireless network. DEVICES WITH SIM CARDS ARE NOT ACCEPTABLE. All sim cards should be removed. Any student who connects or 'tethers' their device to their mobile phone in order to gain access to the Internet will be breaching the BYOD User Agreement and as such school discipline consequences for the breach will apply. The school's internet is filtered and monitored and blocks unacceptable or banned internet sites including some social media sites such as Facebook. This filtering is only applied when the student is at school.

Can my child access blocked or inappropriate sites at school?

The school's wireless Internet access available to students will be filtered in the same way that access is managed at present. However, if students connect using their 3G or 4G connections, then this will bypass the filtered Internet access, allowing them to access blocked, unacceptable or banned Internet sites including some social media sites such as Facebook. This will be in breach of the BYOD Policy.

Will there be technical support provided at school?

Yes, support will be limited to connecting to the school's wireless network as well as minor standard application support. There will be no support provided for repairs of any kind.

How should I protect the device from damage?

A range of protective covers are available online or in stores. It is recommended that students protect all devices while in use or stored in their school bags.

What happens if the device is stolen, lost or damaged?

The device is the sole responsibility of the student. The guidelines for the BYOD program specifically address the risk of students bringing their own devices to school. We recommend taking out warranty and insurance to cover these eventualities. Most manufacturers will not cover theft, loss or deliberate damage under their warranty. It is recommended that parents discuss options with their home & contents insurance provider for details and cover. The school will not be responsible for loss, damage or theft.

How will the school deal with students who use their devices for non-educational purposes (such as games) during school times?

Students have always found ways to be off task in a classroom environment. We understand that having a device creates distraction from in-class tasks much more tempting. JEHS expects students to stay on task while in class. Students failing to do so will be dealt with in accordance with the school's discipline policy in conjunction with the BYOD and Technology policies.

Can students use another student's device?

Because of the inherent nature of personally owned devices, devices should only be used by the owner of the device. It is the student's responsibility to take care of their device. Usually, having physical access to someone's personal device also provides the ability to email or text message from their accounts.