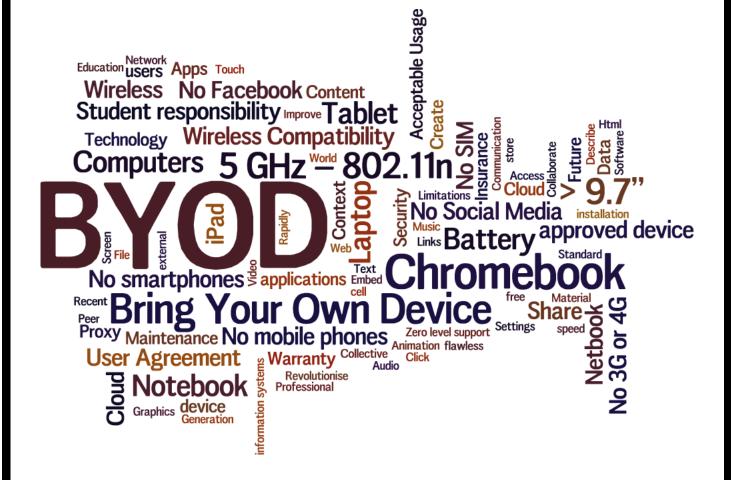# John Edmondson High School

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

In 2016, and beyond, students are encouraged to bring their own fully charged technology device to school every day. This device will be required at school every day and the student's name should be clearly visible on the back of the device and should not be able to be easily removed. Teachers will be preparing activities which require use of this device in many lessons. 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 *'DEC Online Communication Services: Acceptable Usage for School 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 will use their BYOD to access the school's new 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. You should carefully consider all your options for purchase or lease. John Edmondson High School's preferred device is a Chromebook because of its quick start-up, ease of use and lower cost.

Mobile phones or 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.

The device's battery must last for at least six hours as there are no facilities to charge devices at school. It is also highly recommended to have a physical keyboard and a wireless mouse to make it easier for typing and navigation.

A good quality device should last for a few years. Parents should consider the versatility and the weight of the device they select for their child. Please check the 'BYOD - Device Specifications Checklist' document to ensure the device you purchase will meet the requirements of our network. We have negotiated with a company called **'Learning with Technologies'** who has setup a BYOD parent portal to assist you in choosing a device. However, you are under no obligation to purchase the device using this service.

Cost Concerns

The purchase of a device is a major decision and a significant expense. A quality device should last from Year 7 to Year 12. Therefore, if viewed over six years the expense is significantly less.

Internet access through the Department's network will be provided at no cost to students. Access to Office 365 and Google Apps for Education will also be available at no cost to students. This means that there is no need to purchase Microsoft Office as software for devices. The Adobe suite will also be offered free through the Department of Education.

We are committed to delivery of the same learning outcomes for all our students whatever their family's financial circumstances. We have developed an Equity Policy that outlines a number of strategies the school may take, in consultation with you, to support access to technology.

Device Security

There is no secure storage available at school and the school and the Department of Education does not accept any liability for loss, damage or theft of student devices. You are advised to consider insuring the device against loss or damage, particularly if it is of significant value. It is also worth checking with your "Home and Contents" insurer, as some insurers will cover portable devices up to certain values.

The best security measures are the student's own vigilance and responsibility towards their own device. However, you might also consider using a device locator service or an application to track your lost device. These services/applications include the "Find my iPad" service built in to Apple iOS devices, "Prey" for Windows or "LoJack for Laptops" and many more. You can also track your device's IP address with Gmail or Dropbox or other apps like 'Plan B'. There are many helpful websites that explain the setup of these apps and services.

The school does not own, support or warrant the device. Experience from the *'Digital Education Revolution'* scheme indicates that students who took good care of their device and considered themselves the device's owner rarely had device security issues. A range of protective covers are available online or in stores. It is highly recommended that students protect all devices while in use or stored in their school bags.

BYOD and Internet Connectivity

Internet is provided by the school's 802.11n - 5 GHz 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. All can be used for:

- note making, calculation, working with images audio and video

- accessing the Cloud and Cloud based applications available through Google Drive, Google Apps For Education and Microsoft Office 365
- accessing cloud based teaching & learning tools such as Canvas, Edmodo & Microsoft OneNote

The Department of Education (DoE) provides copies of the Adobe Creative Cloud applications & Microsoft Applications at no cost to students. With these applications available on a 'Free of Cost' basis, BYOD's become far more economical than they would be if the applications had to be purchased at retail prices. Refer to the 'BYOD - Available Software' in the Appendix section of the 'JEHS BYOD Handbook'.

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.

It will make no difference whether students are working with a Chromebook, Laptop or Tablet as the teaching will be device neutral. Refer to 'NSWDEC BYOD Device Neutral Activity Guide' in the Appendix section of 'JEHS BYOD Handbook' Students will be encouraged to collaborate with others. Teamwork, communication and sharing will be features of a BYOD setting.

BYOD Equity Policy

BYOD programs in an educational setting inherently impose a financial cost on students and their families in supplying a device. The JEHS BYOD Program can only function effectively if all students have access to a device that meets the Device Specifications. There will be available a small quantity of "pool" devices maintained by the school for short term loan only.

To ensure access and equity for all students, under the BYOD program, the school has established procedures for families to apply for assistance in obtaining access to a device that meets the Device Specification. If you believe you are unable to provide a device that meets the specification you may make an application in writing to the Principal, or make an appointment to speak with the Principal, so that your particular case can be outlined.

While the school won't purchase devices for students in the BYOD program there are several options available to provide assistance to students.

These include:

- Loan of a laptop or other device for a particular day at a cost
- Recurrent daily loan of a laptop or other device at a cost

You will be asked to make an agreement with the school that confirms the alternate arrangements made for your child's access to a device. Any damage or loss of the loan device will have to be paid for by the student or their family.

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 use these devices responsibly at all times at school and **must** follow *'JEHS Technology Policy', 'JEHS BYOD Policy'* and the *'DEC Online Communication Services: Acceptable Usage for School 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 can also have 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 4GB 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 7, Windows **8.1** 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	Devices can be purchased with different warranties. The things to consider here are. The length and type of warranty. **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. **Types of Warranty**: There are two options for types of warranty; **Back-to-base** is the cheapest but would mostly require the device to be packaged and posted back to the supplier for repair. **Onsite warranty** is more expensive and would usually mean that a repairer would come to your home and fix the device. 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.

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 thought 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.

Online Communication Services: Acceptable Usage for School Students

✔ **This document defines the policy for school students of the NSW Department of Education and Communities for the appropriate and acceptable use of internet and online communication services provided by the Department.**

IMPLEMENTATION DOCUMENTS

No implementation documents.

RELATED INFORMATION

- Anti-Bullying Plan for Schools (2005)
- Use by Staff of Employer Communication Devices (2004)
- Web Publishing Guidelines
- Copyright: Podcasting in Schools Policy
- Cybercrime Act 2001

1. Objectives - Policy statement

1.1 The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Today's students are exposed to online communication tools and the internet in their community. They have the right to expect secure access to these services as part of their learning experiences with the NSW Department of Education and Communities.

1.2 Use of the internet and online communication services provided by the NSW Department of Education and Communitiesis intended for research and learning and communication between students and staff. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

1.3 Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

1.4 Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to their supervisors.

1.5 Students who use the internet and online communication services provided by the NSW Department of Education and Communities must abide by the Department's conditions of acceptable usage. They should be made aware of the acceptable usage policy each time they log on.

1.6 Students should be aware that a breach of this policy may result in disciplinary action in line with their school's discipline policy.

2. Audience and applicability

2.1 This policy applies to all school students located at NSW public schools who access internet and online communication services within the NSW Department of Education and Communities network and from any external location.

3. Context

3.1 This policy document takes account of the Memorandum *Student Access to the Internet* of 18 July 1997 and the Memorandum DN/04/00215 – *Review by Schools of their Student Access to the Internet Policies.*

3.2 This policy document should be read as consistent with school discipline, child protection, anti-discrimination and anti-racism policies.

3.3 Document history and details

4. Responsibilities and delegations

4.1 Access and Security

4.1.1 Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- ensure that communication through internet and online communication services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their personal e-learning account.
- log off at the end of each session to ensure that nobody else can use their e-learning account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.

- never knowingly initiate or forward emails or other messages containing:
  - a message that was sent to them in confidence.
  - a computer virus or attachment that is capable of damaging recipients' computers.
  - chain letters and hoax emails.
  - spam, e.g. unsolicited advertising material.
- never send or publish:
  - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
  - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
  - sexually explicit or sexually suggestive material or correspondence.
  - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and internet and online communication services is generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks of the NSW Department of Education and Communities.
- ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

4.2.1 Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.3 Intellectual Property and Copyright

4.3.1 Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

4.4 Misuse and Breaches of Acceptable Usage

4.4.1 Students will be aware that:

- they are held responsible for their actions while using internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.
- the misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, evaluation and reporting requirements

5.1 Students will report:

- any internet site accessed that is considered inappropriate.
- any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education and Communities.

5.2 Students should be aware that:

- their emails are archived and their web browsing is logged. The records are kept for two years.
- the email archive and web browsing logs are considered official documents.
- they need to be careful about putting their personal or sensitive information in emails or on websites.
- these records may be used in investigations, court proceedings or for other legal reasons.

6. Contact
Director, Learning Systems, (02) 9266 8951.

Document history and details

Approval date

29/05/2006

Approving officer

Deputy Director General Schools

Implementation date

03/06/2006

Web publication date

16/01/2015

Superseded documents

This document supersedes the Memorandum to Principals 97/011 (S.010) *Student Access to the Internet*. This document updates and, where possible, supersedes existing school policy for student Internet and email use. Existing student access to the Internet policy that is specific to a school and is not covered by this policy should be retained.

It is the responsibility of the user to verify that this is the current and complete version of this document, located at: https:/ / www.det.nsw.edu.au/ policies/ general_man/ general/ accep_use/ PD20020046.shtml

EXPLORE OUR DEPARTMENT

- **ABOUT US**
- **ABORIGINAL AFFAIRS**
- **CENTRE FOR EDUCATION STATISTICS & EVALUATION**
- **EARLY CHILDHOOD EDUCATION AND CARE**
- **PUBLIC SCHOOLS NSW**
- **TEACH NSW**

- **STUDENTS**
- **PARENTS**
- **JOB SEEKERS**
- **NEWS CENTRE**
- **POLICIES**

CONTACT US
35 Bridge Street
Sydney NSW 2000
1300 679 332

SOCIAL PROFILE
Twitter
Linkedin
Facebook
RSS
YouTube
Download our apps

NSW GOVERNMENT Education

- DoE home
- Contact us
- Customer service
- Privacy
- Copyright
- Accessibility
- Information access
- NSW Government
- Jobs NSW
- Terms and conditions
- NEALS

John Edmondson High School
BYOD User Agreement

JEHS provides access to technology in the form of desktop computers connected to a school network. The Bring Your Own Device (BYOD) program aims to enhance these learning opportunities and experiences for students.

Any student who wishes to use a computer device at school must carefully read, agree to, sign and return this **BYOD User Agreement** in conjunction with the *JEHS BYOD Policy, JEHS Technology Policy* and the *DEC Online Communication Services: Acceptable Usage for School Students* in the company of a parent or caregiver unless otherwise directed by the principal. Any questions should be addressed to the school and clarification obtained before the User Agreement is signed.

If a student connects a device without signing and submitting a user agreement they are in breach of the school rules and subsequent discipline action may be taken. JEHS reserves the right to confiscate any unauthorised device. The school adopts this policy in order to maintain a safe and secure environment for students and its staff.

User Agreement

Student:

- I have read and agree to use my device in accordance with *JEHS BYOD Policy, JEHS Technology Policy* and the *DEC Online Communication Services: Acceptable Usage for School Students*.
- I have reviewed the *JEHS BYOD Device Specifications Checklist* document and have ensured my device meets the outlined specifications.
- I agree that my use of the Department's internet will be primarily for learning.
- I agree that use of my device during school activities is at the direction of the teacher.
- I will not attach any school-owned equipment to my device without the permission of a teacher.
- I agree to only ever use my own portal/internet log-in details and never share them with others.
- I agree to not hack or bypass any hardware and software security implemented by the Department or the school.
- I agree to not use BYOD to knowingly search for, link to, access or send anything that is;
    - offensive
    - abusive
    - pornographic
    - defamatory
    - threatening
    - considered to be bullying
- I agree to report inappropriate behaviour and material to my teacher.
- I agree to stay safe by not giving out my personal information to others.
- I understand that my activity on the internet is recorded and these records may be used in investigations, court proceedings or for other legal reasons.
- I acknowledge that the school cannot be held responsible for any damage to or theft of my device.

- I understand that I must bring the device to school fully charged each day and that there are no facilities for charging my device at school.
- I understand that technical support at school is limited to helping me access the school's wireless network only.
- I understand that inappropriate use of my device will result in confiscation of my device and disciplinary action.
- I understand that any teacher has the right to inspect and confiscate a device if there are suspected violations of the *JEHS BYOD Policy, JEHS Technology Policy* or the *DEC Online Communication Services: Acceptable Usage for School Students* and any breaches of these policies may result in the loss of network and/or device privileges, as well as other school disciplinary action.

    In addition, I understand that:
- I must treat all school and other users' devices with care. I understand that I will be required to pay for the costs of repair/replacement for any damage caused by my actions.

Parent/Caregiver:

- We have read and agree that our child will abide by the ***JEHS BYOD Policy, JEHS Technology Policy*** and the ***DEC Online Communication Services: Acceptable Usage for School Students.***
- We have reviewed the ***JEHS BYOD Device Specifications Checklist*** document and have ensured our child's device meets the outlined specifications.
- We understand our child's responsibilities regarding the use of the device and the Internet.
- We understand that the school cannot be held responsible for any damage to or theft of my child's device.
- We understand that failure to comply with the policies and the BYOD User Agreement will result in confiscation of the device, loss of privileges to use the device in school and/or school's disciplinary action.
- In signing below, we understand and agree to the JEHS BYOD User Agreement, JEHS BYOD Policy, JEHS Technology Policy and the DEC Online Communication Services: Acceptable Usage for School Students.

Name of student: ....   **Roll Class:** ....

Signature of student: ....   **Date:** .... / ..... / ....

(signed in the presence of)

Name of parent/carer: ....

Signature of parent/carer: ....   **Date:** .... / ..... / ....

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL OFFICE

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 DEC Online Communication: Acceptable Usage for School Students. The program starts in 2016.

Do students have to bring the device to school every day?

Yes. This device will be required at school every day. Teachers will be preparing activities which may require use of this device. Students must ensure that their device is fully charged.

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'. The school has negotiated with a company called **'Learning with Technologies'**

who has setup up a BYOD parent portal to assist you in choosing a device. However, you are under no obligation to purchase the device using this service.

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.

I don't have or can't afford a device that my child can bring to school.

There will be available a small quantity of "pool" devices maintained by the school for short term loan only. To ensure access and equity for all students, the school has established procedures for families to apply for assistance in obtaining access to a device. If you are unable to provide a device that meets the specification you may make an application in writing to the Principal, or make an appointment to speak with the Principal, to outline your case.

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.

What do I, as a parent, need to do to accommodate the device at home?

You need to ensure that the device is fully charged for the next day and is updated with the latest operating software, antivirus programs and apps. It is also important that the student's work is backed up in case of accidental loss of data.

Will students be completing homework using the device?

Yes. Teachers may set homework where the device will need to be used to complete it. It is advised that parents employ normal monitoring methods when using the device.

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 I need to have Internet access at home?

It would be helpful to have some form of Internet access (wired or wireless) in order for a child to make full use of school resources from home, as well as the multitude of resources available on the Internet. But, as such it is not a requirement. In addition, there are many providers of free Wi-Fi in the community that students could use to access the internet outside of school hours. Please be aware that these connections do not provide access to filtered internet as experienced on the school's network.

Will there be technical support provided at school?

Yes. However, considering that there will be hundreds of devices that could be brought to school as part of the BYOD program, the extent of technical support will be limited to support 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.

As a parent, am I required to add additional software (virus protection, filter, tracking device etc.) to my child's technology device?

Yes. All applicable devices that connect to the internet will need to have antivirus software installed. *However, no antivirus software is needed for the **Chromebooks**. They come with built-in malware and virus protection, with multiple layers of security. It automatically updates the system and the Virus protection, so you are always running the latest and most secure version. Chrome manages your updates silently in the background.* Installing latest updates for software, tracking software and apps is your responsibility.

Will parents need to purchase apps or applications to support learning?

There may be a small cost associated for downloading required applications. There are many applications and apps that are available for free. Students will also have access to Adobe Creative Cloud applications, Microsoft applications and Google Apps for Education at no cost.

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. However, you might also consider using a device locator service or an application to track your lost

device. These services/applications include the "Find my iPad" service built in to Apple iOS devices, "Prey" for Windows or "LoJack for Laptops" and many more.

What suggestions does the school have for dealing with damage?

No matter how much care is taken with devices, there is always the chance of accidental or unintended damage. For this reason we strongly recommend that families investigate warranty and insurance options at the time of purchase or with their current insurance provider. Many insurance providers will provide options for ensuring these types of devices against theft and accidental or intentional breakage/damage. The school is unable to provide any reimbursements for the damage to the device.

What if my own device is broken or being repaired, can I borrow a device?

If you purchase your device from a retailer, you must consider the warranty options. You must check if the retailer will provide you with a loan device until your device gets repaired or replaced? However, if you purchase your device from the parent portal setup by **'Learning with Technologies'**, they will provide you with a pool device that can be used at school while the device is being repaired or replaced.

Can I store my device at school?

No. There are no facilities to store devices securely at JEHS. Students are advised to place a lock code or security measure on the device to disallow access and be vigilant at all times.

Some classes will have very specific requirements that may not be met by the vast majority of BYOD devices – classes like technology, photography, arts etc. How will those classes work?

JEHS will continue to maintain computing labs for higher order tasks and specialised software. Students will have access to these specialised software and computers at school.

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.

Where can I find out more about BYOD?

Our school website has a link to BYOD program that will provide more specific information regarding the program. Please visit our website http://web1.jedmondson-h.schools.nsw.edu.au/internet/jehs/ to find more information regarding BYOD.

John Edmondson High School
Connecting to the Wi-Fi

We are aware that under the BYOD program, students can bring in devices from different platforms including;

Chromebook

Windows 7 laptop

Windows 8.1 laptop

Android tablet

IPad

MacBook ….. and so on

The school's Wi-Fi has the capability to connect to all these devices, provided they meet the 'Wireless Compatibility' requirement as listed in the 'BYOD – Device Specifications Checklist' section.

Basically, a **5 GHz - 802.11n** connection

However, the Wi-Fi connection settings vary for these devices from different platforms. For example; a Windows 8.1 device will have different settings to Windows 7 device. An iPad will have different setup for connecting to the Wi-Fi compared to a MacBook. Yet again and an Android device will connect differently to a Chromebook.

The following pages give instructions for connecting various devices or platforms to the school's Wi-Fi.

Please remember that no matter which device, or which platform, successful connection is a two-step process.

Step 1 - Connect to the Wi-Fi

Step 2 - Turn the 'Proxy' on

Google Chromebook

Step 1 – Connect to the Wi-Fi

1. Before you begin, on another computer, you need to download and save a certificate file to a USB.

   a. Go to: https://mad-directories.det.nsw.edu.au/certificaterequest/

   b. Click on **PROD Internal** from the right-hand menu

   c. When prompted, download and save the file to a USB drive

2. Turn on your Chromebook and sign in as usual. Depending on your Chromebook settings, you **may** need to do this while connected to a non-DEC wireless network.

3. Import the certificate you have saved.

   To do this:
   a) Go to Settings
   b) Select **Advanced settings...**
   c) Select **Manage certificates...**
   d) Go to **Authorities** tab
   e) Select **Import...**
   f) Browse and select the certificate. You may need to select **All Files** to locate it.

4. Select the **detnsw** (or nswdet) wireless network.
   Preferred connection is **'detnsw'

5. Complete the next screen with the following details:
   - **SSID:** detnsw
   - **EAP method:** PEAP
   - **Phase 2 Authentication:** Automatic
   - **Server CA certificate:** PROD-DEC-ROOT-CA[PROD-DEC-ROOT-CA]
   - **User certificate:** None installed
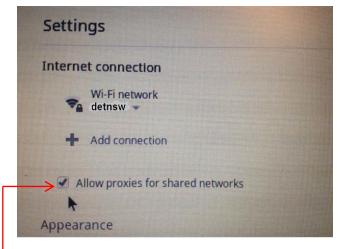   - **Identity:** Your portal username@detnsw (e.g. john.citizen4@detnsw)
   - **Password:** Your portal password
   - **Anonymous identity:** *leave blank*

6. On the bottom right corner, click on the Wi-Fi symbol. Then click on **No network** and **detnsw (or nswdet)**
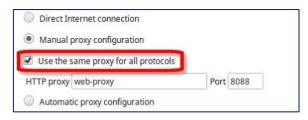
Step 2 – Turn on the Proxy**

1. Click on **Settings**

2. Tick next to **Allow Proxies for shared networks**

3. Click on the Wi-Fi symbol again and click on **Connected to detnsw** (or nswdet)

4. Click on **detnsw** or nswdet.

   This will open up a window with **Connection and Proxy tabs**. Go to the proxy tab and enter the details as below:

   Select **Manual proxy configuration**
   Tick **Use the same proxy for all protocols**
   HTTP proxy: proxy.det.nsw.edu.au
   Port: 8080

5. The proxy settings are saved automatically. Click **Close**

The first time you go to a website, you will be prompted to enter your portal username and password.
   Do not use @detnsw after your username.

Step 1 – Connect to the Wi-Fi

1. Click on the **Wi-Fi** symbol on the desktop taskbar.

2. From the Wireless menu, select the **detnsw** or **nswdet** connection and **Connect**.

   **Preferred connection is 'detnsw'

3. Enter your Student Portal login details. Put **@detnsw** after your username. Password is your portal password. Press '**OK'**

4. You should now be connected to the Internet.

Step 2 – Enter the Proxy Details**

5. Enter proxy details in the browser connection settings of your Internet browser.
   Enter proxy details as follows
   Address: proxy.det.nsw.edu.au
   Port: 8080

Troubleshooting for Windows 7

If it fails to connect, don't worry. Click **Cancel**.

6. Click **Open Network and Sharing Centre**.

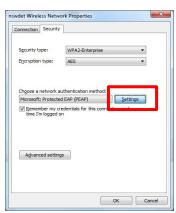7. Click on **Manage wireless networks**.

8. Click **Add**

9. Enter the details as per the picture below and click **Next**.

10. Click **Change Connection Settings**.

11. Go to the **Security** tab and make the details are as follows and then click **Settings**.
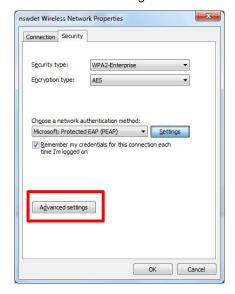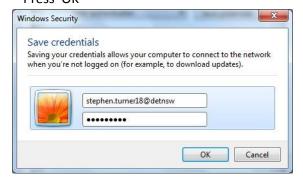
12. Untick this option.

EAP MSCHAPv2 Properties

When connecting:

☐ Automatically use my Windows logon name and password (and domain if any).

OK   Cancel

13. Click on **Advanced** settings.

nswdet Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)   Settings

☑ Remember my credentials for this connection each time I'm logged on

Advanced settings

OK   Cancel

14. Change the settings as per the picture below and click **'Save credentials'**.

Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User authentication   Save credentials

☐ Delete credentials for all users

☐ Enable single sign on for this network

15. Now enter in your portal username & password

    Put **@detnsw** after your username.
    Press 'OK'

Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

stephen.turner18@detnsw

••••••••

OK   Cancel

16. You should now be connected.
    Reselect the **detnsw** connection and connect automatically.

Not connected

Connections are available

Wireless Network Connection

detnsw

☑ Connect automatically   Connect

coonahs

Open Network and Sharing Center

17. Open your internet browser. You will be prompted to fill in your portal username and password.

    Do not use @detnsw after your username.

Windows 8

Step 1 – Connect to the Wi-Fi

1. Click on the **Wi-Fi** symbol on the desktop taskbar.

2. From the Wireless menu, select the **detnsw** or **nswdet** connection and **Connect**.

    **Preferred connection is *'detnsw'*

3. Enter your Student Portal login details. Put **@detnsw** after your username. Password is your portal password. Press '**OK'**

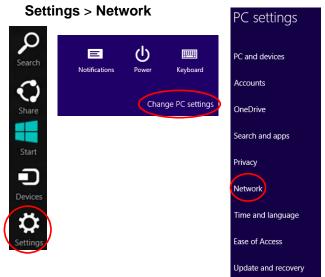4. When prompted to 'continue connecting?', choose '**Connect'**.

Step 2 – Enter the Proxy Details**

5. Choose Charm Bar > **Settings** > **Change PC Settings** > **Network**

6. Choose **Proxy** > **Manual Proxy Setup** > **On**
    Enter proxy details as follows
    Address: proxy.det.nsw.edu.au
    Port: 8080
    Click **Save**

Now when you open the Internet browser you will be prompted to fill in your portal username and password.

   Do not use @detnsw after your username.
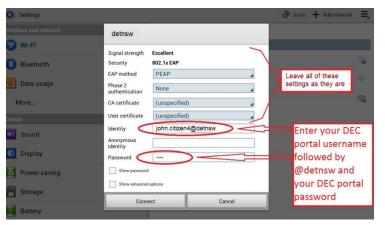
Android Tablet

Step 1 – Connect to the Wi-Fi

1. Make sure the wireless is turned on. Go to the top toolbar and turn Wi-Fi on.

2. From the Wireless menu, select the **detnsw** or **nswdet** connection and **Connect**.

   **Preferred connection is 'detnsw'

3. Enter your Student Portal login details. Put @detnsw after your username e.g. **john.citizen4@detnsw**
   Choose **Connect**.

4. The **detnsw** or **nswdet** will now be ticked and your tablet is connected to the Wi-Fi. Internet will still not work though.

   Internet will still not work though. Go to Step 2

Step 2 – Enter the Manual Proxy***

5. Click on the **detnsw** or **nswdet** connection and choose **'Show Advanced options'**.

6. Fill in the Proxy Settings:
   a. **Proxy Settings:** Manual
   b. **Proxy hostname:** proxy.det.nsw.edu.au
   c. **Proxy Port:** 8080

   Now choose '**Connect**'.

7. Open the Internet browser. You will be prompted to fill in your portal username and password.

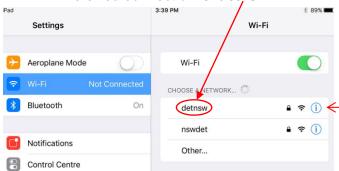   *Do not use @detnsw after your username.*

iPad

Step 1 – Connect to the Wi-Fi

1. Make sure the wireless is turned on. Both 'detnsw' and 'nswdet' may appear on your Wi-Fi choices.
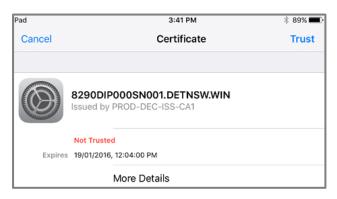
   Preferred connection is **'detnsw'

2. From the Wireless menu, select 'detnsw'. Enter your Student Portal login details. Put @detnsw after your username e.g. john.citizen4@detnsw
   Click Join.

3. Accept / Trust the Certificate

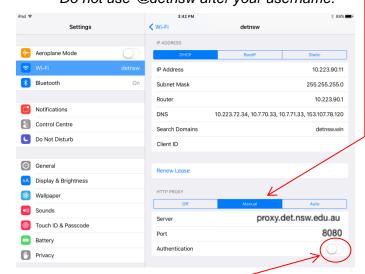4. The 'detnsw' will now be ticked and your iPad is connected to the Wi-Fi.
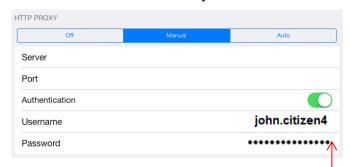   *Internet will still not work though. Go to Step 2*

Step 2 – Enter the Manual Proxy***

5. Now, go back to settings > Wi-Fi > click on the blue (i) symbol on the 'detnsw' that you are connected to.

6. Choose 'Manual' in the HTTP Proxy down the bottom and enter Proxy details
   Server: **proxy.det.nsw.edu.au**
   Port: **8080**
   Do not use @detnsw after your username.

7. Next turn Authentication on and add your username and password**.
   Do not use @detnsw after your username.

8. Now when you open the Internet browser you will be prompted to fill in your portal username and password.
   Do not use @detnsw after your username.
   Just username and password

** 1) If it is a shared device, leave the username & password blank in the proxies. You will be prompted for it later.

*** 2) iPads store your details so there is no need to turn off the Manual Proxy to connect to your home Wi-Fi.

Created - Nov 2015

MacBook, MacBook Air and MacBook Pro

Step 1 – Connect to the Wi-Fi

1. Make sure the wireless is turned on. Go to the top toolbar and turn Wi-Fi on.

2. From the Wireless menu, select the 'detnsw' or 'nswdet' connection.

   **Preferred connection is 'detnsw'

3. Enter your Student Portal login details. Put **@detnsw** after your username e.g. john.citizen4@detnsw

4. Accept or Trust certificate, if prompted

5. The 'detnsw' will now be ticked and your mac device is connected to the Wi-Fi.
   Internet will still not work though. Go to Step 2

Step 2 – Enter the Manual Proxy***
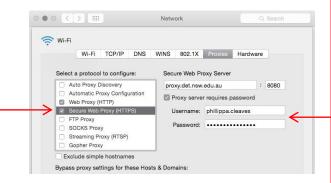
6. Choose 'Open Network preferences' > Proxies

7. Tick Web Proxy (HTTP), enter **proxy.det.nsw.edu.au** and **8080**. Now tick 'Proxy Server requires password' and fill in your username and password**.

   Do not use @detnsw after your username.

8. Tick Secure Web Proxy (HTTPS), enter **proxy.det.nsw.edu.au** and **8080**. Now tick 'Proxy Server requires password' and fill in your username and password**.
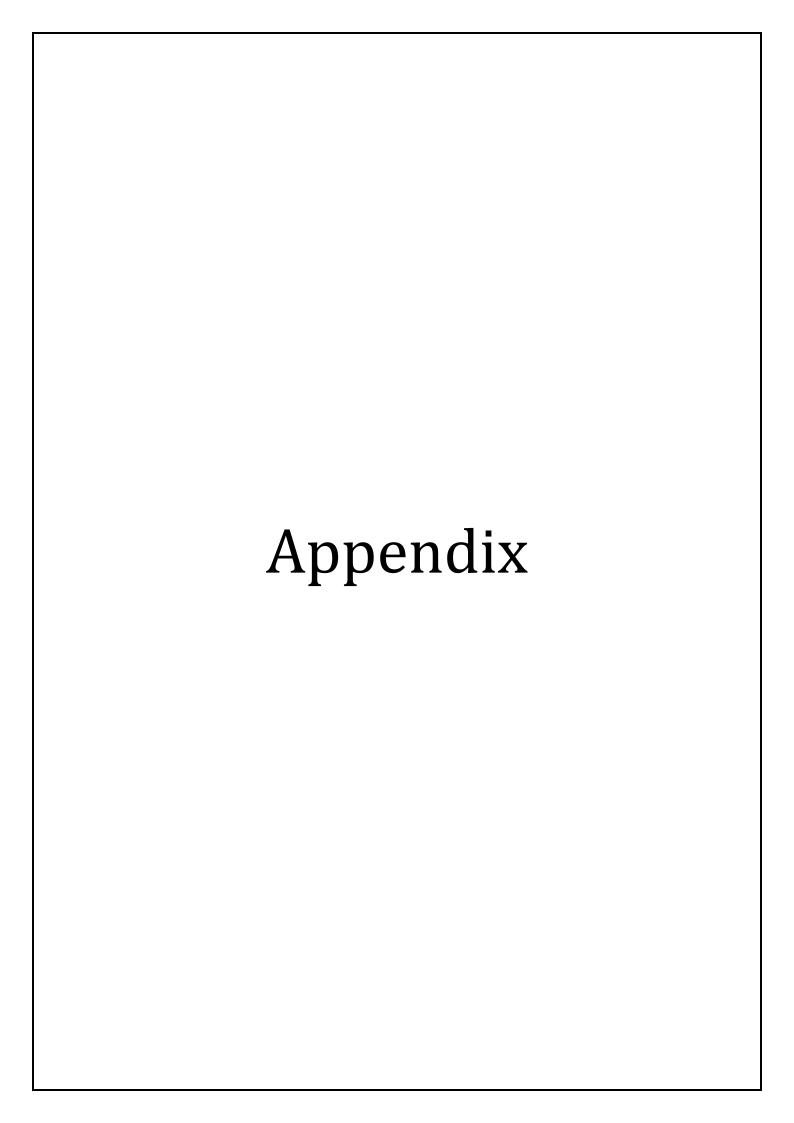
   Do not use @detnsw after your username.

9. Save this page then click 'Apply' on the 'Network Preferences' panel.

10. Now when you open the Internet browser you will be prompted to fill in your portal username and password.
    Do not use @detnsw after your username.

** 1) If it is a shared device, leave the username & password blank in the proxies. You will be prompted for it later.

*** 2) Undo the 2 ticks for the Proxies when you have to connect to your home Wi-Fi.   Created - Nov 2015
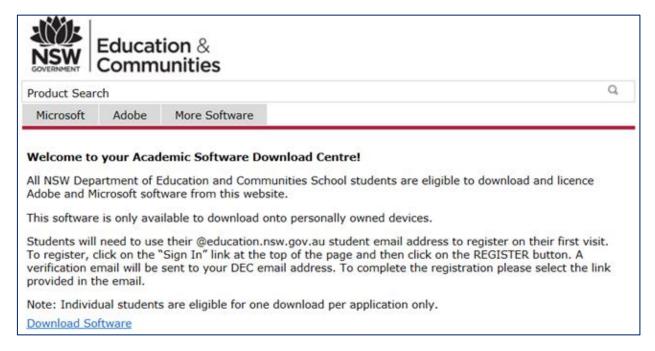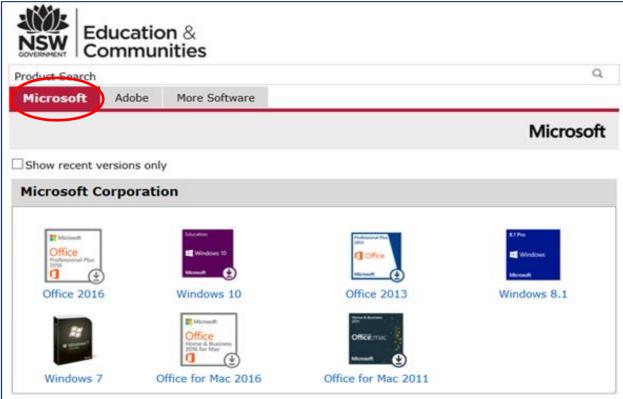
Appendix

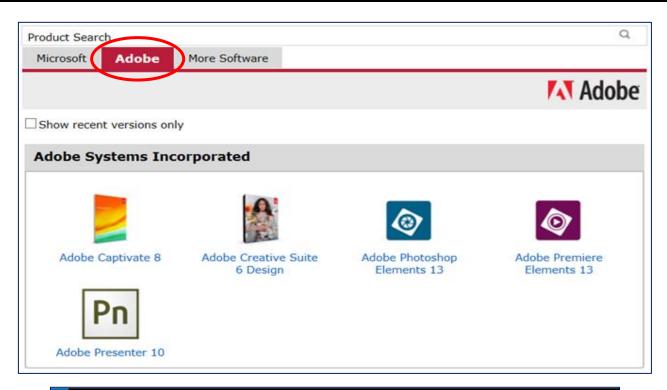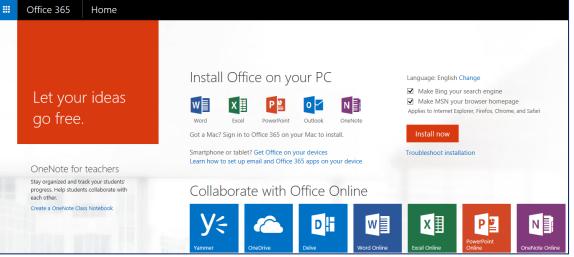# John Edmondson High School BYOD – Available Software

The Department of Education (DoE) provides copies of 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.
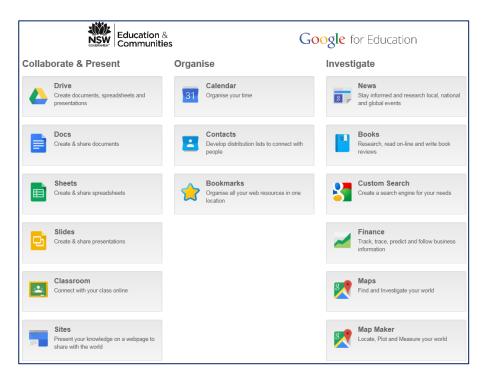
These software are currently available for download by students through their portal. Refer to the school's website to view the 'NSW DEC Software Download Instructions' video.

NSWDEC BYOD Device Neutral Activity Guide

- This guide will give teachers and student options to choose software, tools and apps according to the learning activity students are working through.
- Why not let students choose the tool that best fits the learning activity at hand?
- Remember, the Web Tool column will generally suit all platforms as the tools work from a browser, not from a piece of installed software
- Due to filtering and unexpected installation issues, it is recommended that students install software / apps / create accounts at home
- Inside the DEC internet environment, mobile apps may not have full functionality.
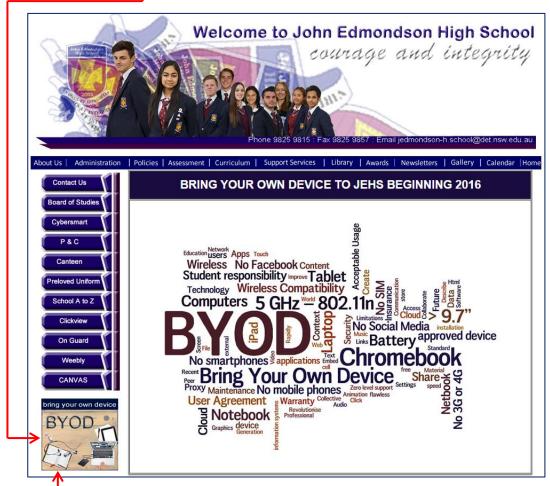- For more information on BYOD in NSW Department of Education and Communities visit http://nswdecbyod.weebly.com

	Windows	Mac / Apple	Web Tool	iPad	Android	Chrome OS
Notetaking / Word Processing	Word Evernote OneNote	Pages Evernote Office Word	Google Docs Google Keep Evernote	Google Docs Evernote Notability	Google Keep Evernote Papyrus	Google Docs Google Keep Evernote
Timelines	Powerpoint Publisher Paint	KeyNote Pages Skitch	Timetoast Dipity Xtimeline	Timeline Maker Timeline 3D Timestream		Tiki Toki Time and Line Concept Board
Quizzware	Polleverywhere SRN - Student Response Network Socrative	Infuselearning.com SRN - Student Response Network Socrative	Polleverywhere Socrative SRN - Student Response Network	Stu's quizboxes SRN - Student Response Network Socrative	SRN - Student Response Network Socrative	Quizzlet Revision Quizzes Quiz Center
Presentations / Photo Slideshow	Powerpoint Photo gallery Windows Movie Maker	Keynote Powerpoint iMovie	Prezi Google Presentations Slide Rocket	Prezi, ($) Keynote Haiku Deck	($) QuickOffice Google Presentation Animoto	Google Presentations/Slides Prezi

	Windows	Mac / Apple	Web Tool	iPad	Android	Chrome OS
Research	Internet Explorer Firefox (freeware) OneNote	Safari Firefox Evernote Instagrok	Google Custom Search Boolify Evernote Instagrok Gooru	Some apps for researching (click to open)	Google Chrome DolphinHD OneNote	Google Browser Dolohin HD Instagrok
Bookmarking	Internet Explorer Firefox Google Chrome	Safari Firefox Google Chrome Opera	Diigo Google Bookmarks Delicious Symbaloo Pinboard	Diigo Delicious app Safari Chrome Browser	Diigo Google Bookmarks Delicious Pinboard	Google Bookmarks Pocket Dolphin HD
Data Gathering and Processing	Excel Access	Numbers	Google Forms/Sheets	Google Sheets ($) Numbers	Google Sheets ($) QuickOffice	Google Form/Sheets
voice recording	Sound Recorder Audacity	Audacity Garage Band	Twistedwave Podbean croak.it Songify	Audio Recording Apps for the ipad Educreations	Google Keep tape-a-talk recorder	VoicePad spring pad TwistedWave
Blogging	Shared OneNote Mysite Edublog	Evernote Mysite Edublog	Mysite Edublogs Weebly Jux Google site	Google Blogger Mysite Weebly Jux Google site	Mysite Blogger Wordpress Weebly Shared OneNote	Google Sites BlogEd Mysite Blogger
Digital Publishing / Posters	Publisher Adobe InDesign / Adobe Photoshop Powerpoint	Pages Adobe InDesign / Adobe Photoshop	Google Docs Smore Glogster Popplet Mural.ly Thinglink	($) Phoster ($) Quark Design Pad Pages Phoster	Skitch Mural.ly	Google Docs Glogster Mural.ly

Website Creation	Adobe Dreamweaver Adobe Muse	Adobe Dreamweaver Adobe Muse	Google Sites Weebly Yola Jux	Simpl Gusto Weebly	Google Sites Weebly	Google Sites Weebly Yola Jux
Comic Creation	Comic Life Adobe Photoshop Adobe Fireworks	Comic Life Adobe Photoshop Adobe Fireworks	Comic Life ToonDo Comic Creator	($) Strip Design Comic Life	Create a Comic Comic-Strip-It (lite) Comic Puppets (lite)	Pixton (edu version) Comics Head Bit Strip
Animation	Adobe Edge Animate Xtranormal pivotstick	Adobe Edge Animate ($) Anime Studio Debut	GoAnimate XtraNormal ToonDoo	Toontastic Puppet Pals Animation HD	Stickdraw Drawing Cartoons Powtoon	GoAnimate WeVideo SketchToy
Portfolios	Adobe Acrobat MySite	MySite	Google Sites MySite	MySite	Google Sites MySite	Google Sites MySite
Music	Finale	Garageband	GarageBand	Video Star GarageBand		beatlab AudioSauna audiotools
Graphical Modelling	google sketchup	123D Design	3D Tin TinkerCad	123D Sculpt	Autodesk Force Effect Autodesk 123D Design	Lucidcharts Autodesk 123D Design
Game Building	Kodu, Scratch Cube 2	Game Maker	Zondle Futaba Classroom Games GameStarMechanic	Hopscotch HD	Autodesk Force Effect	Math Tab AutoDesk Force Effect
Infographics	Adobe Fireworks Paint Adobe Photoshop	Adobe Fireworks Adobe Paint Skitch	Picktochart Visual.ly ease.ly infogr.am	Visual.ly Piktochart	Adobe Ideas ($)	Piktochart Infogr.am
Digital Study Skills	Office OneNote Office Powerpoint Evernote	Pages Evernote Flashbox	Quizlet StudyBlue Brianflips	StudyBlue Evernote Peek FlashCards Deluxe	Study Blue	Study Blue My Homework
Curation and Aggregation	OneNote Word Google Bookmarks	Reeder FlipBoard	Scoop.it Diigo Symbaloo Pearltrees	FlipBoard Scoop.it Pinterest	OneNote Evernote FlipBoard	mural.ly Evernote
Mindmapping	FreeMind PowerPoint Paint		bubbl.us Mural.ly MindMeister	Corkulous iThoughtsHD MindMeister Popplet	Mindmeister Mindomo SimpleMind	Lucidcharts mural.ly MindMeister
Collaborative documents	Google Drive Skydrive SharePoint	Google Drive Skydrive SharePoint	Google Drive SharePoint Confluence Wiki Wikispaces	Google Drive Book Creator SharePoint	Google Drive O365	Google Drive SharePoint Confluence Wiki Wikispaces
Image editing	Adobe Photoshop Elements Adobe Photoshop Pro Adobe Fireworks	Adobe Photoshop Elements Adobe Photoshop Pro Adobe Fireworks	Aviary PicMonkey Pixlr	Photoshop Touch PS Express PhotoFunia	Photoshop Touch Autodesk Sketchbook snapseed	Google Drawing PicMonkey Pixlr Editor Camera360
Mathematical Graphing	Geogebra Google SketchUp	Desmos	Desmos	Graphing Calculator	Desmos	Geogebra Desmos
Movie Making and Storytelling	Windows Movie Maker Adobe Premiere Elements Adobe Premiere Pro	iMovie Adobe Premiere Elements Adobe Premiere Pro	Animoto Powtoon ToonDo ($) GoAnimate	($) iMovie Animoto Puppet Pals	Animoto Magisto Powtoon WeVideo	Powtoon Pixorial Video WeVideo GoAnimate
Class Communication	Edmodo Schoology Lore Haiku	Edmodo Schoology Lore Haiku	Edmodo Schoology Lore Haiku	Edmodo Transfer Lore Haiku	Edmodo Schoology Lore Haiku	Edmodo Schoology Lore Haiku

Our Website………

To find more information regarding the Bring Your Own Device (BYOD) program, please visit our school's website. It hosts a **link** to our BYOD program and has many resources to support our BYOD program.

Click on the BYOD link to access the following BYOD pages.