FINDON HIGH SCHOOL
Drummond Avenue Findon South Australia 5023
P : 8445 7944 | F : 8345 5401
E : dl.0805_info@schools.sa.edu.au
www.findonhs.sa.edu.au

FINDON HIGH SCHOOL

BYOD Policy

March 2019

Start with a dream.
Finish with a future.

Government of South Australia
Department for Education

TABLE OF CONTENTS

What is Bring Your Own Device (BYOD)

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

Bring Your Own Device

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

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

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

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

To do this effectively, we have adopted a 'Bring Your Own Device' (BYOD) policy for all students since the beginning of the 2016 school year.

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

- BYOD Policy (this document)
- BYOD Fact Sheet
- Digital Citizenship
- Findon High School Network Access Guide

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

Please refer to FAQs section if you have any questions, if you require any additional information please contact Craig Palamoutain ICT Manager, or send an email to dl.0805.ictadmin@schools.sa.edu.au.

21st Century Learning

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

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

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

BYOD Policy

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

All users will be required to acknowledge receipt and understanding of the BYOD policy in this document and adhere to the Digital Citizenship Guidelines. Non-compliance may result in suspension or the removal of privileges for a period of time aligned to the Findon High School Behaviour Management Policy.

Only devices approved for connection by the Findon High School ICT Support Staff (FHS ICT) may be used.

All BYOD devices must only be connected to the schools wireless network. Direct connections using LAN or USB cables is prohibited unless a specific exemption is approved by the FHS ICT Staff.

BYOD - ICT Policy

The BYOD policy applies to any device is for personal learning (including appropriate use of all Wireless Network Capable Digital Devices brought from home for school or class use).

Purpose

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

Electronic and ICT Equipment and devices in this policy include, but are not limited to, **computers** (such as desktops, laptops, tablets & iPads), **storage devices** (such as USB flash memory devices, portable Hard Drives, SD cards, CDs, DVDs, iPads, iPods, MP3 players and Electronic Books), **cameras** (such as video, digital, webcams), all types of **mobile phones**, **video and audio players/receivers** (such as portable CD and DVD players), and any other technologies as they come into use.

Currently the school recommends the use of laptops and netbooks as the preferred devices due to their compatibility with the school wireless systems and their inbuilt protections against Malware. All other devices will have limited or no access to the schools ICT networks and services. Only devices that have been approved for use can connect to the schools wireless network.

Access to the school's ICT networks, infrastructure and data is a privilege and all staff, students and other persons seeking access to the school network must **consent to and sign this BYOD policy prior to connecting the device to the school network**. Users include all full and part time staff, relief teachers, students, and other agents who use a personally owned, or school owned device to access, share, store relocate or backup any school or student based data.

Non-sanctioned use of personal devices to back up, store and otherwise access any data owned by the school and stored on our network is strictly prohibited.

Rationale

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

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

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

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

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

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

Monitoring Of Devices Connected to the School Network

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

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

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

Connectivity of all staff and student owned devices will be centrally managed by the Findon High School ICT Support Staff, and configurations will be in accordance with the guidelines in place to protect and secure school data and information systems and storage. Configuration of devices will include password protection and encryption, and any other controls essential to isolating and protecting sensitive information accessed from or stored upon personal devices or the school's network. Staff and students will be expected to adhere to the same security protocols when connecting to non-school equipment to help protect any information from being lost or stolen from their devices.

Failure to comply will result in immediate suspension of all network access privileges so as to protect the school's infrastructure. No student, staff member or relief teacher is to divulge their password to a third party and all personal device users are responsible for bringing their devices to school fully charged and labelled for identification.

Student access of the internet independent of the school's proxy servers (i.e. by personal ISP mobile connection or hotspot) is prohibited.

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

ICT for Personal Learning and Acceptable Use Policy

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

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

- The school's IT Services Team reserves the right to refuse the connection of personal devices to the School network if such equipment is being used in any way that could potentially cause harm to the school's systems, data, users or resources.
- All users must employ reasonable security measures including, but not limited to, passwords, encryption, physical controls and safe storage of personal devices whenever they contain school data. Any attempt to contravene or bypass security or acceptable use procedures will be deemed a contravention of this ICT for Personal Learning and Acceptable Use Policy and will limit the ability of the user to access the school's ICT network and resources.
- Staff and students agree to only view, listen to, or access, school appropriate content on their personal devices while at school.
- Due to copyright, content such as music and games is not to be transferred to other devices or the school's computer network. Furthermore, students and staff may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from the Principal and those whom they are recording.

Mobile Phone Policy

Our school policies are built on the fundamental principle that students have a right to learn and teachers have the right to teach. We also believe in courtesy and respect and this policy aims to encompass these principles.
Although there is no ban on students bringing mobile phones to school we would urge students and parents to consider whether it is necessary for the following reasons:

- Disruption of staff who are teaching their classes
- Disruption to the learning of other students in the class
- The security of the phone and the possibility of damage or theft

In the event that students choose to bring phones to school the care and security of the phone would be the student's responsibility.

Students who bring a phone to school are required to abide by the following conditions:

- Phones can be used in class if the teacher deems it permissible for school related purposes
- If a student chooses to bring a mobile phone they may not use it in the corridors to make personal calls during lessons (see communication policy below)
- Unauthorised use of video or camera phones to capture persons without written consent will result in consequences policy being enacted without impunity
- Phones use as a calculator is restricted to only if the previous clauses are sanctioned. However, they may not be used under any circumstance during test conditions. Therefore, it is recommended that students should have an appropriate calculator for school
- Students undertaking SACE school assessments (this includes tests, assignments and examinations undertaken during lesson time) should not have in their possession any electronic device apart from an approved calculator. This rule includes mobile phones and electronic dictionaries and is not negotiable

Communication between students and parents

If a parent needs to contact a student we would recommend this to be done through the front office in the appropriate way and not by a student's mobile phone.

If a student is involved in an incident we would expect that they notify the school first to enable us to deal with the situation rather than contact the parent first. This would include situations involving illness, conflict with other students or other behaviour management issues.

Consequences for not following this policy:

- Warning to students
- Diary note requiring parent signature and loss of class phone privileges
- Referral to year level coordinator
- Withdrawal room
- Loss of all phone privileges during school hours
- After School Detention

If the problem persists this issue would be treated as deliberate disobedience.

All students should use their lockers to store phones or other valuables.

In special cases such as Physical Education lessons where students ask staff to look after valuables, if the staff member elects to take the valuables no responsibility for their security will be accepted. The responsibility for student valuables remains with the student and the secure lockers are provided for this purpose. All students are responsible for keeping their passwords secure.

Examples and Conditions

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

Such activities include but are not limited to:

- Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, and harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
- Criminal activities that can be punished under law.
- Selling or purchasing illegal items or substances.
- Obtaining and/or using anonymous email sites, spamming, spreading viruses.
- Causing harm to others or damage to their property.
- Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
- Deleting, copying, modifying, or forging other users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.

- Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.
- Using any computer/mobile devices to pursue “hacking,” internal or external to the school, or attempting to access information protected by privacy laws.
- Accessing, transmitting or downloading large files, including “chain letters” or any type of “pyramid schemes.”
- Intentionally accessing, creating, storing or transmitting material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
- Breaking copyright laws.
- Attempting to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities

BYOD Guidelines

Students may use a privately owned electronic “Internet ready” device on the school’s wireless network with teacher or administrator permission.
The use of a privately owned electronic device to support and enhance instructional activities is at the subject teacher’s discretion. All users of the school network are bound by expectable use agreement whereby individuals will not over use data allowance.

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

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

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

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

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

No student shall use any computer or device to illegally collect any electronic data or disrupt networking services.

Devices are brought to school at the students' and parents' own risk. In the event that a privately owned device is lost, stolen or damaged, the school is not responsible for any financial or data loss.

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

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

Student Agreement

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

Students may not use the school's Internet facilities and ICT resources in any circumstances unless the appropriate BYOD and Acceptable Use Agreement has been signed and returned to the School.

Online resources for parents and students are available at www.cybersmart.gov.au.

The specific conditions of the User Agreement are outlined below

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

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

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

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

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

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

I shall not maliciously destroy or steal ICT equipment from the school. Unacceptable or rough use of any equipment belonging to the school, myself or other students or staff will also not be tolerated. If I have damaged ICT equipment I understand that the costs for repair or replacement will be me and my parent/caregivers' responsibility.

I understand that I am never permitted to use the school network for private storage for non-educational, non-approved files, including games, videos, music, etc.

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

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

Consequences

The following are consequences for breaches of the BYOD and Acceptable Use Policy:
Warning from subject teacher and note in diary which needs to be signed by both the Home Group teacher and the parent. Offences may incur significant penalties including limited or no access to the school's ICT network and related sources.

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

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

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

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

Students who damage or misuse others' personally owned devices will be responsible for any replacement or repair costs associated with such damage or theft.

Cloud Computing Services User Agreement- Students

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

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

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

1. Privacy Consent

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

2. Acceptable Use

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

- give your account password to anyone else;
- access (or try to access) anyone else's account, or try to defeat any security controls;
- send or help to send unsolicited bulk email (spam);
- publish, send or knowingly access material that is pornographic, hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;
- knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or
- disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.

3. Monitoring

You agree that IT Support Staff responsible for IT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

If you notice a problem with the Cloud Computing Services, or if you think that someone is trying to access your account (or someone else's account), you agree that you will tell the school's IT Support Staff straight away.

4. Suspension Or Termination Of Use And Other Consequences

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

Acceptable Devices

Which should I bring?

There is a choice of purchasing a device or bringing your own device if you already have one and it meets the technical specifications to join the school network.

In conjunction with EduNet we have a Parent Online Purchasing Portal where devices can be purchased by credit card, PayPal or interest free finance (subject to approval).

The Purchasing Portal is located via the link on the FHS Website.

There is a choice of either a 3 different laptops and are available at Education discounted prices. The device will also be electrically tested and tagged.

When purchasing these devices you have the option to take out accidental damage insurance (highly recommended unless the device can be covered by your existing household contents insurance), other options will also be available to purchase at the same time (carry bag, mouse, external hard drive etc.).

The devices purchased through the portal will be preconfigured to join the FHS wireless network, have software installed to access printers. Microsoft Office Pro Plus is also available at no cost to students.

The devices warranty will be supported by the FHS ICT Support Staff, who will arrange repair etc. as required. Any repair costs that are not covered by the warranty will be passed onto the student or parent/caregiver who can then claim on their insurance.

Though laptops are slightly heavier to carry around than a tablet or iPad, they allow you to be more productive in situations where you will be creating documents, movies, or other digital media.

Minimum Specifications for BYOD

The Minimum requirements supported by Findon High School are:

- Windows 7 or higher, OSX Lion or higher,
- 2.0 GHz Processor, Core i3 processor or higher
- 4GB of RAM minimum
- 64GB of storage minimum
- Wireless 802.11g/n
- 6 hour battery life (no charging available at school)
- Current Antivirus Software

Students bringing their own devices may find they do not meet the standards to be able to join the FHS wireless network. They will also not be supported by the FHS ICT Support Staff.

Digital Citizenship Policy

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

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

Digital Citizenship Guidelines

This Agreement has five conditions of being a Digital Citizen:

- **Respect Yourself.** I will show respect for myself through my actions. I will select online names that are appropriate, I will consider the information and images that I post online. I will consider what personal information about my life, experiences, experimentation or relationships I post. I will not be obscene.
- **Protect Yourself.** I will ensure that the information, images and materials I post online will not put me at risk. I will not publish my personal details, contact details or a schedule of my activities. I will report any attacks or inappropriate behaviour directed at me and I will seek support from appropriate people or organizations. I will protect passwords, accounts and resources.
- **Respect Others.** I will show respect to others. I will not use electronic mediums to bully, harass or stalk other people. I will show respect for other people in my choice of websites, I will not visit sites that are degrading, pornographic, racist or inappropriate. I will not abuse my rights of access and I will not enter other people's private spaces or areas.
- **Protect Others.** I will protect others by reporting abuse, not forwarding inappropriate materials or communications; and not visiting sites that are degrading, pornographic, racist or inappropriate. I will moderate unacceptable materials and conversations, reporting conversations that are inappropriate or unacceptable.
- **Respect Intellectual property.** I will request permission to use resources. I will suitably cite any and all use of websites, books, media etc. I will acknowledge all primary and secondary sources. I will validate information. I will use and abide by the fair use rules.
- **Protect Intellectual Property.** I will request to use the software and media others produce. I will use free and open source alternatives rather than pirating software. I will purchase, license and register all software. I will purchase my music and media, and refrain from distributing these in a manner that violates their licenses. I will report vandalism and damage I will act with integrity.

Software

Required Software

DECD has negotiated with Microsoft to make available Office 365 services to students at no cost including:

- Office Pro Plus (for student owned Windows, Android and iOS devices)
- Office Online (Web based Microsoft Office)
- OneDrive (1 GB of Personal cloud storage)

This will be preinstalled on devices purchased through the portal and can be installed on other devices by the FHS ICT Support Staff (Media is not supplied).

Windows 10 Education Edition for students can be installed on a student owned device by FHS ICT Staff if requested and is also provided free of charge.

The minimum requirement is Office 2007 or above.

Recommended Web Browsers

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

- Internet Explorer (10+)
- Safari
- Google Chrome
- Firefox

Anti-Virus Software

A current and up to date anti-virus application MUST be installed and active on all devices connected to the FHS Network. Any device found not to have current antivirus software will be blocked from the network.
There a many effective free or low cost Anti-Virus products available – please see the ICT Support staff if you require further information.

Other Software

The following free applications should also be installed on all BYOD devices to ensure the best possible user experience and engagement. These applications can be installed by the FHS ICT Staff or via the FHS intranet site)

- Adobe Reader DC
- 7Zip
- VLC Player
- Google SketchUp Make
- Notepad++
- Proxy Switcher
- PaperCut Client
- Microsoft Movie Maker

Technical Support

Network Connection

Students need to connect to the school's wireless network by following the Accessing Findon High School Wireless Network document and using the username and password provided to each student at the start of the year. Only approved devices can be connected.

Students who are having technical issues connecting their technology tool can then visit the ICT Support Office Window (normal support is from 8:15am to 3:30pm during school terms – outside these time by arrangement)

An initial scheduled time will be made in Home Group to help support students to connect student's device during the first week of each term.

Charging

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

Printing

Printing will be supported for all devices via PaperCut. All prints are logged and charged to the student when printed. Printing of PDF files from USB devices is also available on the KonicaMinolta Copiers located in the resource centre and outside the ICT Support Office.

Insurance and Liability

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

Data Loss and Backup

Students should ensure that their files are backed up in at least 3 places (laptop hard drive, USB device and FHS server).

If a device purchased via the parent portal from Leader Education requires the operation system to be reinstalled the FHS ICT Support staff will not be responsible for the backing up of any data.

Flash based storage (USB Flash Drives and Solid State Drives) although very fast are not a reliable long term backup option. It is strongly recommended that and external Hard Disk Drive be purchased and regular backups performed.

FAQs

What is Bring Your Own Device (BYOD)

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

How do I connect to the Findon High Schools wireless network?

Please Refer to the following Document:

Accessing Findon High School Wireless Network

Is student internet monitored?

Internet access is filtered whilst they are using the school's network. Their complete web history is also logged and monitored accordingly.

Where do I go for support?

If students are not able to connect to the school's wireless network and have followed the steps of the **Accessing Findon High School Wireless Network documents**, students can visit the IT office between 8:15am-3:30pm (note the office is not always attended).

My laptop was damaged/stolen when I brought it to school. Who should I contact?

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

Can my child charge their device at school?

It is the responsibility of the student to bring their device to school charged. **Under no circumstances can a device be plugged into a power point at school.**

Can my child use the printer from this device?

Devices purchased through the Portal will be able to print. Other personal devices may not meet the technical specifications to access the Findon High School wireless network.

What happens to students work if the computer hard drive fails or the computer is stolen?

We recommend and encourage students to use additional backup measures to keep their documents safe such as: external hard drives, USB drives, cloud storage.

Accessing the Findon High School Wireless Network

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

Accessing the FHS Wireless Network:

- Connect to the FHS Wireless networks, using your devices wireless network adaptor.
- Once connected, open the web browser on your device and you will be automatically redirected to the Student WiFi Portal .
- Input your FHS **Username** and **Password** followed by the **Login** button to connect to the chosen network.
- If your login attempt is successful, you will be automatically redirected to the Findon High School Student Portal and ready to start searching the internet. This will also connect you to the network drives.

Please be aware that these connections have active web content filtering. Your browsing history will be logged and monitored.

Student Computer Use Agreement

Access to computers and the Internet is provided for the purposes of educational research and learning. The purpose of this policy is to provide rules for appropriate use of these facilities. Students and parents are asked to carefully read and then sign the following agreement.

Student Agreement:

I understand that the use of computers and access to the Internet from Findon High School must be in support of educational research and learning and I agree to the following:

- I will refrain from accessing any news groups, chat groups, web pages or other areas of cyberspace that would be considered offensive in the judgment of the Principal or his/her delegate because of pornographic, racist, violent, illegal or other content
- Accordingly, I am responsible for monitoring and appropriately rejecting materials, links, dialogue and information accessed/received by me
- I will not use valuable computer/Internet time using chat lines, chat rooms or playing games unless approved by the school
- I will not use or attempt to bypass the schools internet filtering or proxy servers, or disable any management or monitoring systems installed on any device, and I will not use or access hacking or anonymising websites or services
- I will be courteous and use appropriate language. Therefore I will refrain from using obscene, harassing or abusive language and will report any case of such usage against me to my teacher or the Student Network Coordinator or school administration
- I accept responsibility to keep copyrighted material from entering the school. Therefore, I will not download software, games, music, graphics, videos or text material that are copyrighted and I will not violate any copyright laws by posting or distributing copyrighted material
- Plagiarism is unacceptable. Therefore I will use any downloaded material in an appropriate manner in assignments, listing its sources in a bibliography and clearly specifying any directly quoted material
- I will not reveal personal information, including names, addresses, credit card details or telephone numbers of myself or others
- I will not damage computers, computer systems or networks. This includes unplugging/swapping mice, keyboards, etc. If I discover any methods of causing such damage I will report them to the school ICT coordinator or school administration and I will not demonstrate them to others
- I will respect equipment in all computer areas and will not take any equipment without a teacher's permission. I will report any theft I am aware of to the school administration.
- I will abide by the log-in process to access the computer network and Internet. I understand that passwords are confidential and must not be given to others, or displayed or written down.
- I understand that cyber bullying through text message/ image exchange or via any form of technology is inappropriate and even if this incident was off the school site and out of hours. These matters could also be referred to the police.
- I understand that use of any unapproved file sharing technology is not permitted.

If I violate any of the terms of this agreement, I will be denied all access to school computers and network for a time to be determined by the Principal and may face further disciplinary action as determined by the Principal. I am aware that each case will be considered individually.

Student's Name _____ Year Level _____

Student's Signature _____ Date _____

Parent Agreement:

As a parent/guardian of I hereby acknowledge that I have read the agreement on student use of computers and the Internet and discussed it with my child. I understand that this use is designed for educational purposes. I recognise that while every effort will be made to monitor student use of the Internet, it is impossible for Findon High School to continually monitor and restrict access to all controversial materials. I further acknowledge that, while questionable material exists on the Internet, the user must actively seek it and therefore is ultimately responsible for bringing such material into the school. I therefore do not hold the staff or Principal of Findon High School responsible for any material acquires from the Internet.

Parent Signature _____ Date _____