BYOD

2024 BYOD

Parent Handbook

Year 3, 4, 5 and 6

IPADS ARE FOR *learning*

Follow these steps to get ready for BYOD

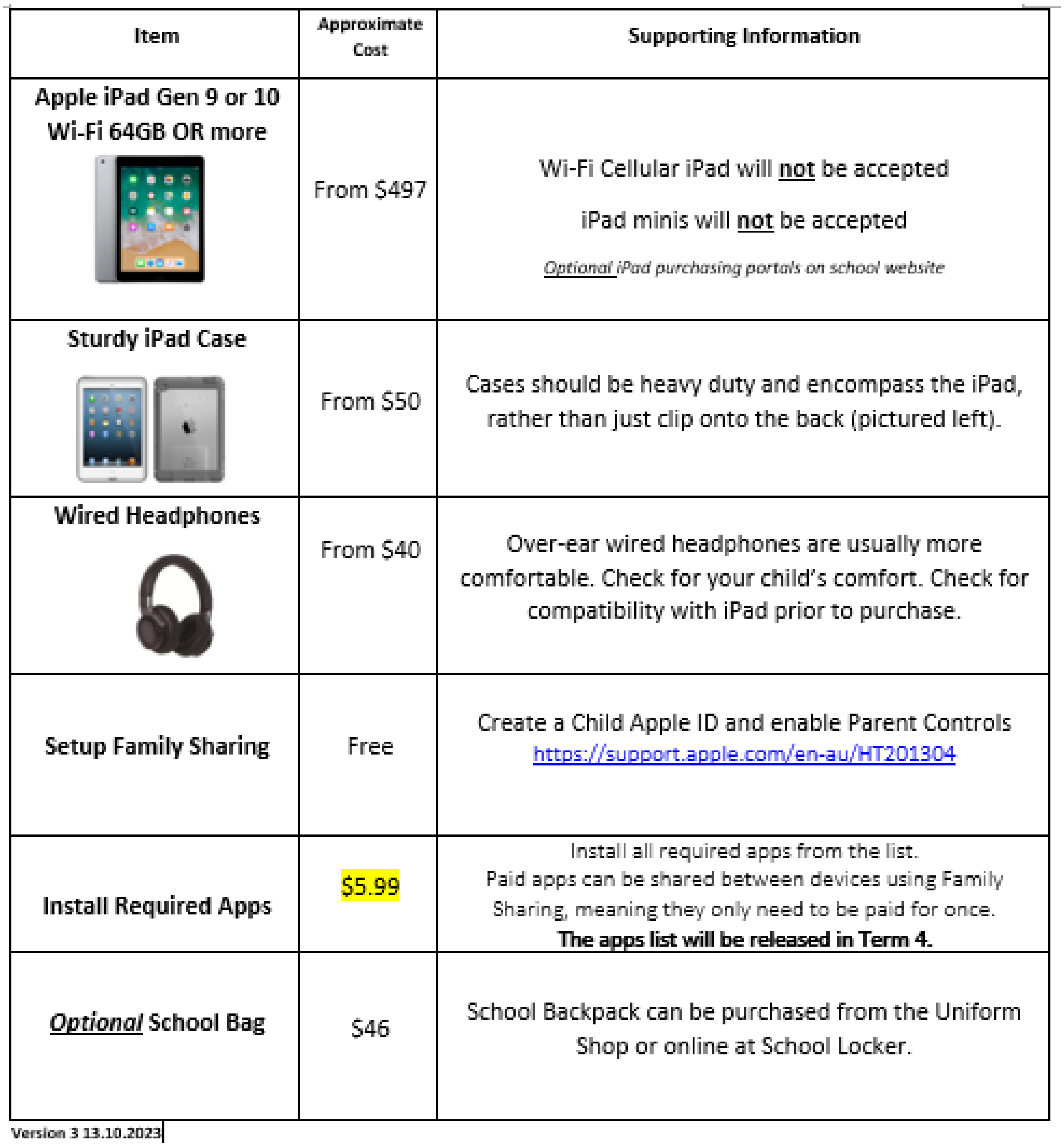
Step 1 Follow the Purchase List (**p.3)** to get items ready

Step 2 Label the iPad, case and headphones with your child's name (**p.4)**

Step 4 Use our BYOD 2024 Page on our school website to set up iPad for learning(**p.5)**

Step 4 Download Apps (list available on our website from Term 4)

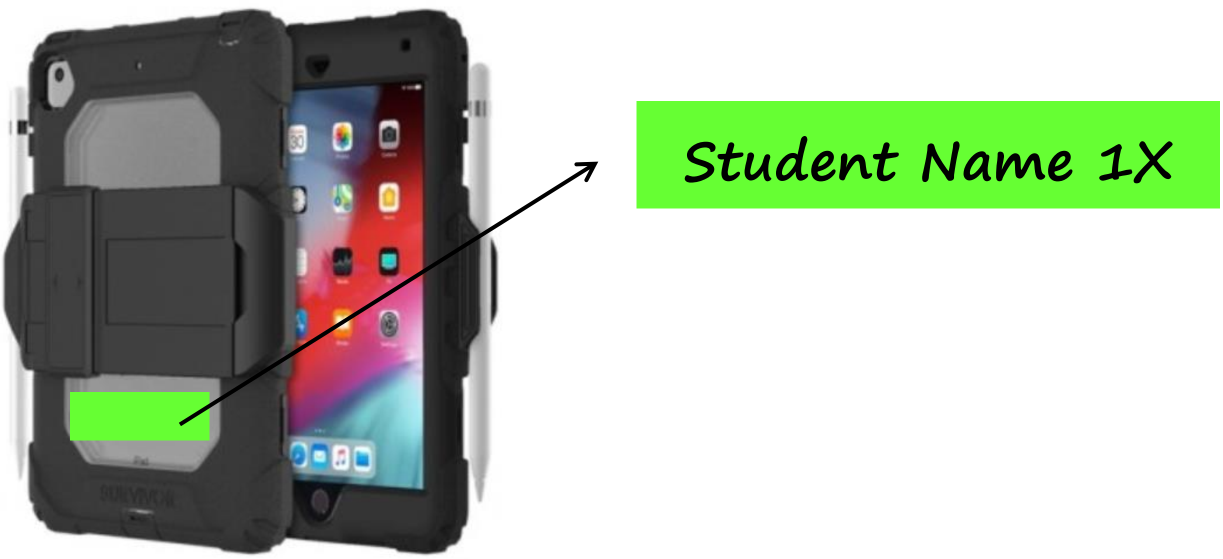
Step 1 Purchase the following items ready for the first day of school.



Item	Approximate Cost	Supporting Information
Apple iPad Gen 9 or 10 Wi-Fi 64GB OR more	From $497	Wi-Fi Cellular iPad will **not** be accepted iPad minis will **not** be accepted *Optional iPad purchasing portals on school website*
Sturdy iPad Case	From $50	Cases should be heavy duty and encompass the iPad, rather than just clip onto the back (pictured left).
Wired Headphones	From $40	Over-ear wired headphones are usually more comfortable. Check for your child's comfort. Check for compatibility with iPad prior to purchase.
Setup Family Sharing	Free	Create a Child Apple ID and enable Parent Controls https://support.apple.com/en-au/HT201304
Install Required Apps	$5.99	Install all required apps from the list. Paid apps can be shared between devices using Family Sharing, meaning they only need to be paid for once. **The apps list will be released in Term 4.**
***Optional* School Bag**	$46	School Backpack can be purchased from the Uniform Shop or online at School Locker.

Version 3 13.10.2023

Step 1 ✓	Follow the Purchase List to get items ready
Step 2	Clearly label the iPad, case and headphones with your child's name and 2024 class
Step 3	Use our BYOD 2024 Page on our school website to set up iPad for learning
Step 4	Download Apps (list available on our website from Term 4)



Step 1 ✓ Follow the Purchase List

Step 2 ✓ Label the iPad, case and headphones with your child's name

Step 3 Use our BYOD 2024 Page on our school website to set up iPad for learning

Step 4 Download Apps (list available from Term 4, via link below)

Follow this link to Setup iPad for Learning and download apps

https://norfolkvillagess.eq.edu.au/curriculum/bring-your-own-device

BYOD Program FAQs

SETTING UP and MANAGING iPAD

Setting up iPads for Learning

Follow these instructions to setup iPad for Learning

Family Sharing to setup a Child Apple ID

All students **must have their own Child Apple ID**, this is setup through Family Sharing. Family Sharing makes it easy for up to six people in your family to share Apps and Books, including purchased apps and books. Parents have control over content that is on their child's iPad. Parents are prompted with app requests from their children. Family sharing supports parents with managing iPad at home.

Using a device signed in with **parent** name:

Settings > tap your name > Family > Create Child Account

If you are an existing **Apple User** visit for further support to setup https://support.apple.com/en-au/HT201088

If you use other platforms such as Google or Samsung please use this document to help you setup Family Sharing. You will create the parent Apple ID and then follow instructions to setup a Family using your child's device. When this has been created sign out of your Apple ID on the iPad and sign in with the Child's Apple ID.

Screen Time

After Family Sharing is setup Screen Time and Parental Controls can be applied to your child's iPad.

With Screen Time, you can access real-time reports about how much time your child is spending on their iPad, and set time limits for before and after school use.

Use Apple device signed in **parent** name

Settings > Screen Time > Child's Name > Downtime, App Limits, Communication Limits, Communication Safety, Always Allowed and Content & Privacy Restrictions

Use each of these settings to make **parental decisions about what works best for your family**. Limits can be applied to games and social media apps. It is strongly recommended that all the apps your child has access to are age-appropriate. This information is available in the App Store.

It is strongly recommended that Content & Privacy Restrictions are applied to your child’s iPad. Using Screen Time, you can block or limit specific apps and features on your child's device, and restrict the settings their iPad for explicit content, purchases and downloads, and privacy.

Visit https://support.apple.com/en-au/HT208982 for further support to setup Screen Time.

Turning off iMessage

iMessage must be OFF while at school.

Whilst we understand that communication between home and school is important, iMessage for parent/child communication is not allowed. iMessage is not needed as a learning tool and as such, the use of this during learning time would constitute a breach of our BYOD Code of Conduct.

Settings > Messages > iMessage off

Accessibility Features

Accessibility features help all students to learn. Please turn on the following functions on your child's iPad.

Enable Spoken Content feature:

Settings > Accessibility > Spoken Content > Turn on Speak Selection

Enable Dictation:

Settings > General > Keyboard > Enable Dictation

Connecting to School Wi-Fi

Our school network is a managed online environment controlled by The Education Department. This means that all web searching and online access is carefully controlled and monitored to ensure that students are working in a safe online environment. You do not need to do anything to connect your child’s iPad to the school network, this will happen during school time when the iPad comes to school.

Why BYOD at NVSS?

- ICT Capabilities are woven throughout The Australian Curriculum and as such your child's creativity and capability can be furthered with our BYOD Program, preparing them for a positive employment future.
- 1:1 iPad environment enables learning to be personalised for your child and provides them with access to a wider range of tools to support and enhance learning.
- A personally owned iPad allows your child to share their learning with you, and to access a wider range of digital tools for homework, strengthening the link between home and school. Communication between your child, parent and teacher will be positively influenced using an iPad.
- An iPad will support your child to demonstrate what they know and can do in much broader ways, supporting further opportunities for high order thinking and critical and creative thinking, better preparing your child for their future.

Do I need to set up Family Sharing on my child's device?

Yes. At NVSS we value Family Sharing as an important way for parents to influence their child's device use. Family Sharing is a feature of Apple products. Family Sharing enables children under the age of 13 to have their own Apple ID which is linked to your parent account with the appropriate restrictions. It also allows families to share apps across 6 devices, which means you only need to purchase a paid app once and it can be used across many devices. Family Sharing also offers Parental Controls which support your child to manage their screen time and access to the device. http://www.apple.com/au/family-sharing

Who is responsible for managing the iPad?

Parents and students are responsible for managing and maintaining iPads for school use. This means that updates and app downloads will need to be completed at home. Students may be asked to remove any apps which are not necessary for learning if they are interrupting learning or taking up storage space on the iPad which is necessary for learning tasks.

Apple have a range of personal storage options. Please note that iCloud cannot be accessed on the school network.

For further information: support.apple.com/en-au/ht203977

All iOS updates need to be completed at home as the school MOE internet does not allow this to happen at school. It is important to keep your child's iPad updated with the latest operating software.

Who is responsible for damages to BYOD iPads?

Students will move from class to class with their iPads e.g. for a science lesson with a specialist teacher, and class teachers sometimes use outdoor spaces for learning, so this means that a sturdy case is required to protect the iPad. Rules are in place to prevent foreseeable problems and damage, however, from time to time accidents may occur. If damage is caused by deliberate or careless actions of a student (owner or others), the costs of repair will be passed on to those involved and behaviour consequences may apply. The decision around the responsibility for repair costs is at the discretion of the Principal. iPads can be added to home and contents insurance policies. For further information on this contact your insurance provider.

Do I still need to pay the Levy and purchase books?

Yes. In order to provide a balanced education, students will still need pencils, workbooks and other stationery so this means families need to pay Levy fee and purchase materials on the Booklist.

What apps will my child need on their iPad?

Our BYOD Apps List will be sent to all Year 3, 4, 5 and 6 families with the Levy and Booklist information in Term 4. The apps will be updated on our School Website

Why is an iPad the only device my child can bring?

At Norfolk Village we believe having a consistent device in the hands of all our students and teachers, enables our community to be confident, comfortable and productive with teaching and learning in the 1:1 environment.

What happens if my child forgets the passcode on their iPad?

You will need to connect the iPad to the computer it is synced with and restore it to a previous backup. It is important that you adhere to password procedures as outlined in the Privacy and Confidentiality section on page 9.

Can my child have access to iMessage at school?

No. While at school iMessage must be OFF.
Whilst we understand that communication between home and school is important, iMessage for parent/child communication is not allowed. iMessage and Facetime are not needed as a learning tools and as such, the use of this during learning time would constitute a breach of our BYOD User Agreement.

To communicate with your child during the school day please phone the school office or email their teacher.

Can we install social media apps?

No. Most social media apps are NOT age appropriate, for example a 9 year old should have apps that are recommended for 9 year-olds and under. All Social Media Apps including, but not limited to Facebook, Instagram, Tik Tok, Fortnite and Snapchat are not to be installed.

The Carly Ryan Foundation offers app guides for parents:
https://www.carlyryanfoundation.com/resources/fact-sheets and the Apple App Store provides recommended age limits.

Can we install apps that are not on the Apps List?

Yes. Students can have ‘extra’ apps installed on their iPad for personal use, provided they do not interfere with storage space for school requested apps. You may choose to place extra apps in a home screen folder called ‘Home’, to minimise distractions during learning time.

Are other web-enabled devices like smart watches allowed?

Phones must be signed into the office each morning (placed into silent mode) and then signed out at the end of each day. To wear a Smart Watch to school, students and parents must read, agree and sign our school Smart Watch Policy on page 19 of this handbook. This can also be found on our school website. Classroom teachers will hand out the agreements as necessary. Please return signed agreements to the office ASAP.

LEARNING WITH iPADS

Will my child still be using pencil and paper for learning?

Yes. iPads do not replace all aspects of learning. For example, handwriting features in the Australian Curriculum, so this will be taught. At Norfolk Village, iPads are a tool for learning, just as pencil and paper are, so teachers will select the best tool to suit the needs of students and the learning intention in all learning situations.

How will teachers monitor what my child is doing on their iPad?

At NVSS we believe in supporting student learning to get best outcomes for all students. Teachers use the Classroom App to help monitor and support student learning. This app connects with each iPad in a classroom and allows the teacher to see what students are doing on their screen while connected to the same wi-fi point at school. It tracks which apps are opened by each student, and how long they have been used. The Classroom App also supports teachers to quickly, with one action, share information and links with all students in the class. Students can also send evidence of their learning back to their teacher. For further information: www.apple.com/au/education/teaching-tools.

You can use this app at home to support your child's iPad use.

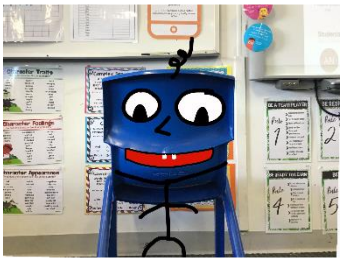
Education Queensland provides all State Schools with a Managed Operating Environment (MOE). This means that web searching is filtered and traceable for both students and staff.

How often will my child use their iPad in class?

iPads are an incredible learning tool and teachers will select the most appropriate learning tool to suit the learning intentions and needs of students. This means that iPad use will vary from day to day.

What will students do with their iPads?

The Australian Curriculum provides a huge range of opportunities for students to demonstrate their learning with digital products. The power of the iPad is in creating. Throughout our BYOD journey we have supported students to create: videos of maths concepts, advertising products such as posters, alternative endings for known stories, digital artworks, stop motion animations and appreciation videos. The options are limitless and teachers facilitate these opportunities for students.



Year 4 object personification

"YOU STILL HAVE THAT ON ANIKA " DOMINIQUE EXCLAIMS LOOKING SHOCKED
YYOU STILL HAVE THAT THING ON ANIKA!?
'OF COURSE I DO!' I REPLY WITH JOY IN MY VOICE
OF COURSE I DO!
THE BUSHES RUSTLED VICIOUSLY. WHOOSH! THE DOOR SLAMMED CLOSED! FELT A COLD CHILL GO UP MY SPINE. I LOOKED AROUND. NOTHING.
TAKE THE STUPID GAUNTLET OFF ANIKA
Supreme
'TAKE THE STUPID GAUNTLET OFF ANIKA' DOMINIQUE EXCLAIMS

Year 6 story telling

How can parents learn more about how to use an iPad?

Get involved with your child's learning and ask them to show you different activities they have completed and products they have created with their iPads. The Everyone Can Create series is a great resource if you would like to experiment and learn https://www.apple.com/au/education/k12/everyone-can-create/

Caring for iPads at School

Charging Batteries

iPads brought to school will need to be charged to a minimum of 90%. **The power supply will not be required to be brought to school.** BYOD classrooms will have a number of iPad power supplies to charge iPads in the event of a battery being depleted. Leaving power supplies at home reduces the weight of the equipment students transport to and from school and reduces likelihood of damage and/or loss.

Screen Care

Screens can be very costly to repair as such we recommend that iPads are not leaned on for any reason. iPads should not be stacked with other iPads or heavy objects, either in or out of a case. Heavy tapping and poking the screen may cause damage also. A good quality school bag will help to protect the screen on the way to and from school.

Storage at School

Classrooms are locked when not in use. Students do not take their iPads into the playground at lunch time.

Internet use with iPads

Internet Use at School

At school, students must agree to follow the Appropriate Use/Behaviour of School Network guidelines in relation to Internet Use. Internet access is provided by Education Queensland’s Managed Internet Service (MIS) and provides students with:

- Content-filtered Internet access
- Virus-filtered email
- School website hosting

MIS provides the means to filter students’ access to web pages from a global level; controlled by Education Queensland and from a school level when appropriate.

Internet Use at Home

iPads used in the BYOD program will continue to access home networks when at home.

Education Queensland Policy

Advice for state schools on acceptable use of ICT services, facilities and devices

This document supports the Use of ICT systems procedure and Use of mobile devices procedure by providing advice to state schools on the acceptable use of information and communication technology (ICT) services, facilities and access by departmental or personally-owned devices.
This advice provides the following information:

- ICT and the curriculum – an overview of the importance of ICT within schools
- Personal mobile device access – implementation of controls for school employees' personal mobile devices and students' personal mobile devices
- Student access to the department's ICT services, facilities and devices – controls that need to be considered when allowing students to access the Department of Education's (DoE) (department's) network
- School-specific ICT responsible use procedure – a template to assist schools in creating an ICT responsible use procedure
- Community access to state school ICT facilities and devices – ICT considerations when managing community activities within a school environments.

ICT and the curriculum

Students use ICT as an integral part of their learning and to equip them to live and work successfully in the digital world. In the Prep to Year 10 Australian Curriculum in all learning areas, students develop capability in using ICT for tasks associated with information access and management, information creation and presentation, problem-solving, decision-making, communication, creative expression and empirical reasoning. This includes conducting research, creating multimedia information products, analysing data, designing solutions to problems, controlling processes and devices, and supporting computation while working independently and in collaboration with others.
Students develop knowledge, skills and dispositions around ICT and its use, and the ability to transfer these across environments and applications. They learn to use ICT with confidence, care and consideration, understanding its possibilities, limitations and impact on individuals, groups and communities.

Personal mobile device access

The department is aware that limited personally-owned mobile device access is essential for the effective running of schools. The department reserves the right to restrict access of personally-owned mobile devices to ensure the integrity of the network and a safe working and learning environment for all network users. These mobile devices include but are not limited to mobile phones, laptops, tablet devices, voice recording devices (whether or not integrated with a mobile phone or MP4 player), handheld gaming devices (e.g. Nintendo Switch, Sega Genesis), smart watches, SD cards or USBs.

If in doubt when implementing technical requirements around the management of personally-owned mobile devices and access to the department's ICT facilities and devices, **advice can be sought from** the IT Service Centre on 1800 680 445. **Policy advice** can be sought directly from Manager, Information and Governance Management on 3034 5093. Additionally, information is available via the Services Catalogue Online (DoE employees only).

School employees personal mobile device access

Principals are to ensure that school employees follow the requirements under the Use of mobile devices procedure.

Student personal mobile device access

Widespread access to the network by student personally-owned mobile devices could compromise the integrity of the department's ICT network. Principals, however, can determine that for educational purposes a student can have access to the department's ICT network. This connection is provided only if the personally-owned mobile device meets the department's security requirements at a minimum by enabling the locking of the personal mobile device, such as a passcode/password, face recognition and/or fingerprint, and where possible installing and managing their own anti-virus software.

Schools wanting students to connect to the department's ICT network are required to develop procedures to ensure that such provisions are assessed against the department's security requirements (where necessary undertaking a risk assessment) and that students and their parents/guardians are provided with the necessary education and assistance to be able to meet these departmental requirements.

The procedures must include:

- providing advice to all students and their parents/guardians on appropriate security requirements (see iSecurity (DoE employees only) website for details)
- advising teachers/supervisors as soon as any breach of security is suspected
- the right to restrict/remove student access to the intranet, internet, email or other network facilities if they do not adhere to the school's network usage and access policy, guideline or statement
- ensuring that students are aware of occupational health and safety issues when using computers and other learning devices.

Schools that are implementing or have implemented the Bring Your Own 'x' (BYOx) (DoE employees only) process also need to ensure steps have been taken to provide a safe and effective learning environment for students while meeting the department's security requirements. This includes advising parents/guardians that the devices provided allow access to their home and other out of school internet services and that such services may not include any internet filtering.

Student access to the department's ICT services, facilities and devices

The department's *Digital Strategy 2019-2023* supports the investment in new foundations for contemporary learning, with near-seamless access to information and digital technologies at any time, any place and on any device. Essential tools for providing these innovative educational programs include the intranet, internet, email and network services (such as printers, display units and interactive whiteboards) that are available through the department's ICT network. These technologies are vital for the contemporary educational program provided in schools.

At all times students, while using these ICT services, facilities and devices, will be required to act in line with the requirements of the Student Code of Conduct and any specific rules of their school. In addition, students and their parents should:

- understand the responsibility and behaviour requirements (as outlined by the school) that come with accessing the department's ICT services and network facilities
- ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email
- be aware that:
  - access to ICT services, facilities and devices provides valuable learning experiences for students and supports the school's teaching and learning programs
  - ICT services, facilities and devices should be used appropriately as outlined in the Student Code of Conduct
  - the school is not responsible for safeguarding information saved/stored by students on departmentally-owned student computers or mobile devices
  - schools may remotely access departmentally-owned student computers or mobile devices for management purposes
  - students who use a school's ICT services, facilities and devices in a manner that is not appropriate may be subject to disciplinary action by the school, which could include restricting network access

  - illegal, dangerous or offensive information may be accessed or accidentally displayed despite internal departmental controls to manage content on the internet
  - teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student
- any inappropriate images/footage posted by individuals on website/s is managed according to the Online incident management guideline for school leaders (DoE employees only).

School-specific ICT responsible use procedure

The Use of ICT systems procedure provides direction to school principals around formulating a school procedure on access to the department's/school's ICT services, facilities and devices for parents and/or students to understand and acknowledge. This may take the form of a procedure, policy, statement or guideline and may require consultation with the school community. Acknowledging through signing seeks to support an understanding of what is lawful, ethical and safe behaviour when using or accessing the department's network and facilities by students and their parents. Principals may seek sign-off either on enrolment of students or alternatively at the start of each school year. Students should be reminded of their responsibilities at the beginning of each school year.

The following dot points are to assist schools to formulate their own procedure. Further guidance on drafting this section can be sought from the Use of ICT facilities and devices guideline.

Purpose statement

- Information and communication technology (ICT), including access to and use of the internet and email, are essential tools for schools in the provision of innovative educational programs.
- Schools are constantly exploring new and innovative ways to incorporate safe and secure ICT use into the educational program.
- School students, only with the approval of the principal, may be permitted limited connection of personally-owned mobile devices to the department's network, where this benefits the student's educational program.

Authorisation and controls

The principal reserves the right to restrict student access to the school's ICT services, facilities and devices if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program. For example, a student with restricted school network access may be allocated a stand-alone computer to continue their educational program activities.

The Department of Education monitors access to and use of its network. For example, email and internet monitoring occurs to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.

The department may conduct security audits and scans, and restrict or deny access to the department's network by any personal mobile device if there is any suspicion that the integrity of the network might be at risk.

Responsibilities for using the school's ICT facilities and devices

- Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the Student Code of Conduct.
- Students are to be aware of occupational health and safety issues when using computers and other learning devices.
- Parents/guardians are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
- Parents/guardians are responsible for appropriate internet use by students outside the school environment when using a school-owned or school-provided mobile device.
- The school will educate students (DoE employees only) regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices. Students have a responsibility to adopt these safe practices.
- Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so that it cannot be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

- Students cannot use another student’s or staff member's username or password to access the school network. This includes not browsing or accessing another person's files, home or local drive, email or accessing unauthorised network drives or systems. Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that copying software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from enforcement agencies.

Responsibilities for using a personal mobile device on the department’s network

- Prior to using any personally-owned mobile device, students must seek approval from the school principal to ensure it reflects the department's security requirements.
- Students are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.
- Where possible, appropriate anti-virus software has been installed and is being managed.
- Students must follow any advice provided on best security requirements e.g. password protection (see iSecurity (DoE employees only) website for details).
- Students and parents are to employ caution with the use of personal mobile devices particularly as these devices can store significant numbers of files some of which may be unacceptable at school e.g. games and 'exe' files. An 'exe' file ends with the extension '.exe' otherwise known as an executable file. These files can install undesirable, inappropriate or malicious software or programs.
- Any inappropriate material or unlicensed software must be removed from personal mobile devices before bringing the devices to school and such material is not to be shared with other students.
- Unacceptable use will lead to the mobile device being confiscated by school employees, with its collection/return to occur at the end of the school day where the mobile device is not required for further investigation.

Acceptable/appropriate use/behaviour by a student

It is acceptable for students while at school to:

- use mobile devices for:
  - assigned class work and assignments set by teachers
  - developing appropriate literacy, communication and information skills
  - authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, their parents or experts in relation to school work
  - accessing online references such as dictionaries, encyclopaedias, etc.
  - researching and learning through the department's eLearning environment
- be courteous, considerate and respectful of others when using a mobile device
- switch off and place out of sight the mobile device during classes, when these devices are not being used in a teacher-directed activity to enhance learning
- use their personal mobile device for private use before or after school, or during recess and lunch breaks, in accordance with Student Code of Conduct
- seek teacher's approval where they wish to use a mobile device under special circumstances.

Unacceptable/inappropriate use/behaviour by a student

It is unacceptable for students while at school to:

- use a mobile device in an unlawful manner
- download, distribute or publish offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment, or stalking
- insult, harass or attack others or use obscene or abusive language

- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions regarding the use of social media, online email and internet chat
- send chain letters or spam email (junk mail)
- share their own or others' personal information and/or images which could result in risk to themselves or another person's safety
- knowingly download viruses or any other programs capable of breaching the department's network security
- use in-phone cameras inappropriately, such as in change rooms or toilets
- invade someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- use the mobile phone (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school employees.

Sign-off

The sign-off process for school students and their parents/guardians should occur on enrolment and annually. The following is a suggested format, with the signature block to be placed at the end of the agreement.

Please note: Children from Prep to Year 3 inclusively are exempt from signing the student section below.

Student:

I understand that the school's information and communication technology (ICT) services, facilities and devices provide me with access to a range of essential learning tools, including access to the internet. I understand that the internet can connect me to useful information around the world.

While I have access to the school's ICT services, facilities and devices: I will use it only for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.

Specifically in relation to internet usage, should any offensive information appear on my screen I will close the window and immediately inform my teacher quietly, or tell my parents/guardians if I am at home.

If I receive any inappropriate emails at school I will tell my teacher. If I receive any at home I will tell my parents/guardians.

When using email or the internet I will not:

- reveal names, home addresses or phone numbers – mine or that of any other person
- use the school's ICT service, facilities and devices (including the internet) to annoy or offend anyone else.

I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT services, facilities and devices inside or outside of school hours.

I understand that if the school decides I have broken the rules for using its ICT services, facilities and devices, appropriate action may be taken as per the school's Student Code of Conduct, which may include loss of access to the network (including the internet) for a period of time.

I have read and understood this procedure/policy/statement/guideline and the Student Code of Conduct.

I agree to abide by the above rules/the procedure/policy/statement/guideline.

____________________________________ (Student's name)

____________________________ (Student's signature) ______________ (Date)

Parent or Guardian:

I understand that the school provides my child with access to the school's information and communication technology (ICT) services, facilities and devices (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information from around the world; that the school cannot control what is available online; and that a small part of that information can be illegal, dangerous or offensive.

I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend upon responsible use by my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT services, facilities and devices. Furthermore I will advise the school if any inappropriate material is received by my child that may have come from the school or from other students.

I understand that the school is not responsible for safeguarding information stored by my child on a departmentally-owned student computer or mobile device.

I understand that the school may remotely access the departmentally-owned student computer or mobile device for management purposes.

I understand that the school does not accept liability for any loss or damage suffered to personal mobile devices as a result of using the department's services, facilities and devices. Further, no liability will be accepted by the school in the event of loss, theft or damage to any mobile device unless it can be established that the loss, theft or damage resulted from the school's/department's negligence.

I believe ______________________ (name of student) understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT services, facilities and devices (including the internet) under the school rules. I understand where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the Student Code of Conduct. This may include loss of access and usage of the school's ICT services, facilities and devices for some time.

I have read and understood this procedure/policy/statement/guideline and the Student Code of Conduct.

I agree to abide by the above rules / the procedure/policy/statement/guideline.

____________________________________ (Parent/Guardian's name)

____________________________ (Parent/Guardian's signature) _____________ (Date)

The Department of Education through its Information privacy and right to information procedure is collecting your personal information in accordance with the *Education (General Provisions) Act 2006* (Qld) in order to ensure:

- appropriate usage of the school network
- appropriate usage of personal mobile devices within the school network.

The information will only be accessed by authorised school employees to ensure compliance with its Information privacy and right to information procedure. Personal information collected on this form may also be disclosed to third parties where authorised or required by law. Your information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact your child's school. If you have a concern or complaint about the way your personal information has been collected, used, stored or disclosed, please also contact your child's school.

Note: The Australian Mobile Telecommunications Association has published materials which may be of use to schools.

Community access to state school ICT facilities and devices

This section provides guidance for schools and their communities undertaking commercial or cost neutral community activities at the school or other educational facility, which require access to departmental ICT resources. This advice should be used in conjunction with Community use of schools facilities procedure.

The Department of Education encourages schools to provide their communities with access to government funded information and communication technologies (ICT) resources, where such access does not interfere with the normal operation of the school. By providing access to the school's ICT resources, the department, through its schools, is building partnerships that will support the continuing/lifelong learning needs of communities, and improve their ability to participate in future economic, social and educational opportunities.

Educational service delivery is the primary reason for providing ICT in schools. Access to school ICT will be granted only to community organisations that agree to adhere to the policies, procedures, practices and values of the department, and are of good standing. Access is formalised through written agreement between the school and the user or group, and, will be undertaken only if:

- the school has the capacity to extend the use of their ICT resources to community members
- there is a genuine community need for the types of services to be provided under the activity
- the activity does not impact negatively on the school's core business and responsibilities
- the activity does not contravene the *Competition and Consumer Act 2010* (Cwlth) and/or other relevant legislation, and
- the activity complies with contractual and/or licensing agreements held by the department.

This section provides guidance when:

- assessing the initial set-up of the community's access to ICT program and the on-going operation of such a program
- extending their ICT resources for community use.

It does not cover remote access and hand held ICT devices or elements related to schools operating as Registered Training Organisations.

Responsibilities

Principals:

- assess the need and school's capability prior to agreement for the conduct of a community program where access to government funded schools' ICT facilities is requested
- are accountable for:
  - preparation and administration of required documentation
  - management of assets, physical and environmental security and safety issues
  - management of access to ICT equipment and network/internet security
- regularly monitor the community access program to determine impacts on the schools and future continuity.

Regional Technology Managers:

- provide advice to principals when assessing the need and school's capability prior to establishing a community access agreement.

Executive Director, Legal and Administrative Law Branch:

- advise on the development and implementation of legal contracts to formalise agreements for community access to ICT.

Director, Education Workforce Relations:

- advise on appropriate allocation of staff member's involvement in community access to school ICT, particularly with respect to support outside working hours or industrial agreements.

Regional Facilities Manager:

- advise schools on the appropriate use of school facilities, including community access to ICT, in consultation with regional technology managers
- assist with the licensing of premises, including licensing cost calculation.

ICT Service Support:

- assist in establishing on-going ICT operations within schools, including terms of existing ICT licensing arrangements for provision of community access to ICT.

Assistant Director-General, Information and Technologies:

- approves this procedure and any subsequent reviews, amendments, related documents or associated departmental guidelines developed.

Process

Steps to be taken by Principals and/or their delegate:

Preparation and administration of required documentation

- follow the Community use of school facilities procedure and prepare a hire agreement
- if activity is being managed by the School's Parent & Citizen's Association, ensure they have:
  - liaised with the Queensland Council of Parents and Citizens Association (QCPCA) to discuss issues such as insurance requirements and completion of the activity declaration form
  - a current insurance policy that extends to volunteers involved with these activities
- approve community access to ICT for the school, ensuring the formal hire agreement, is prepared and signed and appropriate rules for the use of the school's ICT are established, adhered to and maintained by all parties
- arrange for participants to sign a hire agreement
- ensure all volunteers sign the School Volunteers Register and sign a Volunteer Agreement
- conduct Criminal History Checks and Working with Children Checks where required for employees and volunteers in accordance with Working With Children Check - Blue Cards procedure.

Management of assets, physical and environmental security and safety issues

- consider the security issues associated with community access to ICT resources and other equipment and ensure appropriate safeguards are put in place to protect these assets (refer to School security procedure)
- ensure that everyone involved in the community access activity is:
  - familiar with use of the school's security system and relevant security procedures
  - aware of their Workplace Health and Safety responsibilities
  - instructed in the use of the school's emergency procedures
  - covered through WorkCover or Public Liability Insurance
- make additional safety arrangements for community access activities conducted at night, for example:
  - adequate lighting to enable staff and community members to enter and exit the school in safety
  - participants are accompanied when walking to their vehicles or leaving school grounds
  - provision of a telephone to allow community members to arrange transport
  - inform P&C members of their need to comply with the confidentiality provisions of the *Education (General Provisions) Act 2006 (Qld)*
  - take appropriate steps to protect the physical/overall security and privacy of students and to ensure that inappropriate contact between participants and any students that may be on school grounds after hours is avoided (refer to the department's Student protection procedure)

- ensure that:
  - at least one individual responsible for leading emergency procedures is present whenever the community access activity is being conducted
  - an attendance roll is maintained
  - a telephone or intercom is available to allow staff and community members to communicate if an emergency arises
  - a first aid kit is available as described in Managing first aid in the workplace procedure
- ensure collection, storage and transfer of all monies collected are conducted in accordance with school accounting manual (DoE employees only) and/or the P&C Accounting Manual
- if the school enters into an agreement with another organisation, e.g. the P&C, to jointly provide a community access activity for which external funding has been received, ensure that the monies are not used against the intent of the funding organisation. For example, the P&C might receive a grant from a foundation to run Internet Safety Awareness courses for parents. The intent of the original grant is for such classes and should not be used for another purpose
- determine and agree to future ownership of any assets which may be purchased for the community access program.

Management of access to ICT equipment and network/internet security

- ensure adherence to Use of ICT systems procedure
- ensure all contractual and/or licensing agreements are adhered to, and that providing community access to school ICT does not contravene any ICT provider's licence arrangements
- establish processes to ensure that:
  - any information (physical and electronic) that identifies individual children is removed from the area in which the community access activity is to be held
  - traces of any inappropriate information that community members may have accessed on school computers are removed
  - individuals should be given an individual account registered in their own name, where access to the Managed Internet Service is provided on an on-going basis
- negotiate agreed level of service with technical support staff in accordance with relevant industrial instruments, if technical support is necessary. This may include negotiating on-call arrangements or extended hours of work
- ensure that community members do not have access to areas of the network, in accordance with the Use of ICT systems procedure containing information that could be used to identify:
  - individual students and student records
  - staff personnel records
  - financial information
  - other sensitive information. This may be achieved by password protection, firewalls or establishing a separate isolated drive/Local Area Network

- ensure, in accordance with the Information security procedure that:
  - the latest version of antivirus software is installed on all computers and that virus definition files are up-to-date introduction of viruses is limited by scanning all files and information contained on portable media and storage devices prior to it being used
  - close supervision of participants occurs so that viruses / spyware are not introduced
  - a virus scan is run on new disks and files
- ensure that participants:
  - access the school internet responsibly and in accordance with intent of this document
  - do not corrupt, damage or alter the settings, restrictions or content of the school's computers, either deliberately or inadvertently
  - do not disable or interfere with the operation of antivirus software installed on computers
  - do not introduce viruses or malicious code into the school's systems
  - do not create, knowingly access, download, distribute, store or display any form of offensive, defamatory, discriminatory, malicious or pornographic material
- establish a process to limit the amount of information downloaded by participants, as the network usage may significantly increase as a result of community use.

Last updated: 13 May 2020. Please email ICT policy on any questions or suggested changes required to this advice.

2024 NVSS BYOD User Agreement

Families are in partnership with the school to ensure that iPads are for learning. In order to support the successful integration of iPads as learning tools both students and parents have responsibilities. Please read and sign the following agreement:

IPADS ARE FOR *learning*

Students will:

- Use iPad for learning at school so I will only use SCHOOL APPS while at school
- bring my iPad with 100% battery every day
- Turn iMessage off and NOT access it during the school day
- not take photos/videos/recordings unless directed by a teacher
- not upload or share any school work unless directed by a teacher
- choose "Always Allow" in the Classroom App, and I will not change these settings
- keep my case on my iPad
- leave iPad inside during break times
- keep iPad in my bag before and after school
- use the Cyber High-5
- leave phones at the office
- not alter the QWERTY keyboard or fonts by downloading external apps

If I do not follow these rules I understand that:

- My parents may be notified.
- I may lose the privilege of using my iPad at school for a period of time and I will still need to complete my school work in other ways.
- The NVSS Behaviour Code will be used to inform any necessary consequences.

Student Name:	Class:	Date:

Parents will:

- set up my child's iPad using the information provided on School Website (QR Code Below)
- supply suitable headphones and a case for my child's iPad
- setup Family Sharing on my child's iPad
- use Child Apple ID to sign into my child's iPad
- install the required apps on my child's iPad
- turn iMessage and Facetime off during school hours using Communication Limits in Screen Time settings
- use Content and Privacy Restrictions in Screen Time to monitor the content which my child can access
- not install social media, games or entertainment apps which are not suitable for the age of my child. E.g. if my child is 9 years old I will not install apps intended for 12+
- not supply my child with a SIM card for their iPad
- support their child to leave any phones or smartwatches (connecting to outside networks) at the school office during school hours

Parent Name:	Parent Signature:	Date:

NVSS Smart Watch User Agreement

Families are in partnership to ensure that iPads and other devices are for learning. Please read and sign the following agreement to inform the use of smart watches at school:

If parents/carers choose to supply their child/children with smart watches, they must:

- **Understand that any smart watches that are worn to school must include parental controls/school mode.**
- Use parental controls to set school mode. This means that the watch will not have access to outside networks/camera/messaging/phone.
  - *In the event that smart watches can access outside networks the device will be removed in line with the NVSS Student Code of Conduct.*
- Understand that smart watches are worn at your own risk and any damages occurring during school hours (including before and after school) are the parent's /carer's responsibility. Parents and students are responsible for the security, insurance and maintenance of personal devices.
- Understand that if the device has a negative impact on student learning, the school will ask that the device does not come to school.

Parent Name:	Parent Signature:	Date:

Students will:

- Wear smart watches to tell the time, date and track steps.
- Leave their watch on and not remove or share this with anyone else.
- Follow the NVSS Student Code of Conduct.
  - *If the smart watch is connecting to an outside network it will need to be stored at the office during school hours.*
- Alert the teacher to any notifications that appear on their smart watch.

If I do not follow these rules I understand that:

- My parents may be notified.
- I may lose the privilege of having my smart watch at school.
- The NVSS Student Code of Conduct will be used to inform any necessary consequences.

Student Name:	Class:	Date: