



CYOD / BYOD HANDBOOK AND STUDENT CHARTER

Kenmore State High School

School Contact:

Daniel Haines

Head of I.T.

p. 3327 1552

e. dhain12@eq.edu.au

kenmoreshs.eq.edu.au

Contents

Foreword	3
Technology Program Overview	4
What is the CYOD scheme?	4
Why does the school maintain ownership?.....	5
CYOD costs explained	5
Breakdown of CYOD Service Guarantee fee	5
What is the BYOD scheme?	6
Device selection	7
Breakdown of BYOD Service Guarantee fee	7
Laptop Program Inclusions	7
Software and Applications	8
Adobe Creative Cloud	8
Recommendation	9
Device care	10
Data security and back-ups	10
Acceptable device use	11
Passwords	11
Digital citizenship	12
Cybersafety	12
Web filtering	13
Privacy and confidentiality	14
Intellectual property and copyright	14
Monitoring and reporting	14
Misuse and breaches of acceptable usage	14
Responsible use of Technology Devices at Kenmore State High School	15
Responsible use agreement	18

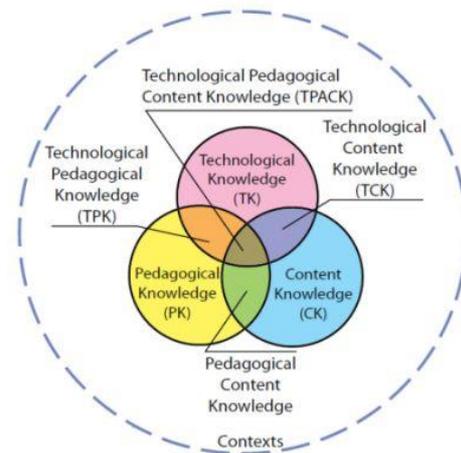
Foreword

This handbook has been developed as a guide for parents and students about matters relating to the Student 1-to-1 Technology Program at Kenmore State High School.

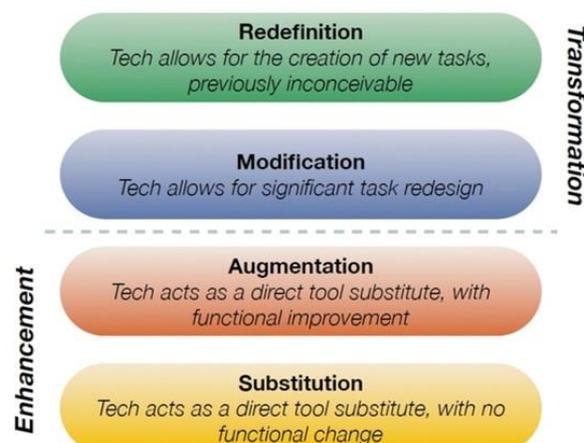
The Kenmore SHS Laptop Program has been very successful over the last six years and has delivered many benefits to the school community. 2015 brought a new direction for the program, building on the benefits to student learning achieved in previous years. The school implemented a variety of options for the school community in the aim of providing a cost effective device that supports student learning.

Unfortunately, schools no longer receive funding from the Federal Government for the procurement of technology devices. Kenmore State High School purchased 1043 laptops through the National Secondary School Computer Fund (NSSCF). The increased access to technology this program provided has allowed major redevelopments of curriculum for our Years 10 to 12 students; and provided learning opportunities for students that were not possible without 1:1 access to a technology device. Moving forward, the school has had to look at other ways to provide access to computers for students while remaining cost effective for parents.

At Kenmore State High School, technology is a tool that enhances pedagogy and allows differentiation in learning. Teachers as life-long learners, will continue to focus on developing their technological, pedagogical and content expertise; utilising ICT in an educationally purposeful way.



Technology facilitates the creation and sharing of knowledge. It provides the extensive ability to share information locally and globally. By utilising virtual classrooms and online learning environments, students can research, collaborate, present, create, refine and represent knowledge in contemporary and meaningful ways. 1:1 access to appropriate technology allows students to transition seamlessly, the learning from school to home and in between. It provides opportunities for students to be challenged by tasks that were once inconceivable: truly transforming learning; and preparing students to be the innovators, entrepreneurs and digital leaders of tomorrow.



Technology Program Overview

The goal when formulating a future direction for technology access at Kenmore State High School was to deliver options that are affordable as well as meeting the educational needs of our students.

From 2015, the school has implemented two models for student access to technology in the classroom and at home: A school-managed Choose Your Own Device (CYOD) program and a self-managed Bring Your Own Device (BYOD) program. Both programs see improved access to technology for students across all year levels and provide students (and parents) with some choice of the technology device that best suits their student's learning needs.

In 2015, we invited our Year 9 and 10 students to participate. In 2016, the program was extended to all year levels.

Our Technology Program works on a split Junior Secondary (Years 7 to 9) / Senior Secondary (Years 10 to 12) technology model. This split aligns with device warranties and expected usable life of a technology device. It also aligns with the curriculum and pedagogical demands and expected usage patterns of a technology device – how we see Year 7 to 9 students using devices, versus that of our Years 10 to 12s.

What is the CYOD scheme?

The 'Choose Your Own Device' (CYOD) scheme provides parents with a range of devices to choose from and elect to purchase. The parent initially contributes the cost of the device to the school via a Participation Agreement and an annual Service Guarantee fee of \$150 and the school will then purchase the device for their students' sole use. The School will retain ownership of the device which allows the school to:-

- install and maintain school owned software including Operating System,
- provide full student access to the school network and internet,
- provide full technical support through our school ICT Service Desk,
- provide access to Hot-Swap laptops when the student's device is in for repair,
- have Computrace anti-theft software installed as standard on all devices,
- have 'lemon clause' protections in place for all purchases,
- fully manage onsite, all Warranty and Accidental Damage Protection (ADP) claim issues.

At the end of the Participation Agreement the school will dispose of the device according to Department of Education and Training (DET) policy. Parents will have the opportunity to acquire the device at this time. As the device will be at the end of its expected life, the school will dispose of the asset to parents for a nominal fee of \$1. At this time, the laptop will get restored back to its factory state.

All devices will come with a 3-year warranty (including battery). Devices will all be purchased with ADP warranty, which, from our experience, has been invaluable in minimising the cost of damage that devices used in a school-context often receive.

Why does the school maintain ownership?

The school maintains ownership of the device until the end of the agreement so that we are legally allowed to install our school software (Inc. Operating System), as well as being able to manage the warranty and ADP claims. At the end of the three years, or if the student leaves the school, the opportunity to acquire the device will be provided as outlined above. At this point, ownership will be transferred and any remaining ADP coverage may be able to be transferred (depending on vendor terms) for a small fee.

CYOD costs explained

The cost of participating in the CYOD scheme is dependent on which device you choose. Due to the ever changing nature of personal devices and the fluctuation of the Australian Dollar, the release of available devices is made as close as possible to the opening of a purchasing window. An annual Service Guarantee fee of \$150 is charged on top of the device costs. Refer to the *Breakdown of CYOD Service Guarantee fee* for more information about Service Guarantee fee inclusions.

The following examples below outline how the costs are charged: -

Cost of device - \$1300 – 3 year program			
Year	Description	Amount	Total
1 st	Up-front Participation Agreement contribution	\$1300	
	Service Guarantee fee	\$150	\$1450
2 nd	Service Guarantee fee	\$150	\$150
3 rd	Service Guarantee fee	\$150	\$150
			\$1750

Breakdown of CYOD Service Guarantee fee

- All warranty and ADP #1 issues handled by the School,
- Full on-site Technical Support via ICT Service Desk (8am to 3:30pm) including software rebuilds, network/internet connectivity and printing problems, troubleshooting and fixing software and hardware issues,
- Access to Hot-Swap Devices when device repair is expected to exceed 24 hours,

- Adobe Creative Cloud Master Collection, Office 2013+, Symantec Endpoint Protection Anti-Virus pre-installed.
- Other school software (MYOB, ClickView, Sparkview, Inspiration, Autodesk Suite and more) for self-installation via School's Service Portal,
- Insurance against loss, fire and theft #2.

#1 excess may apply and there may be a limit to number of claims allowed. This information will be provided within the CYOD Selection Guide and is subject to the terms of the chosen vendor. 2016 and 2017 CYOD rounds have \$0 excess, one claim per calendar year.

#2 excess applies (1st claim = \$200, 2nd claim = \$400, 3rd claim = Full replacement cost).

What is the BYOD scheme?

The 'Bring Your Own Device' (BYOD) scheme allows parents to use an existing family owned device or purchase a new device of their choice that meets the minimum requirements of the school. The student will be required to have the appropriate software to meet the subject requirements that they intend to study (please see the *Software and Application* section for more information).

Although you may choose to use a BYOD device at school, this still requires the payment of an annual \$100 / \$120 fee to support the costs associated with the running of a BYOD program. Please see the *Breakdown of BYOD Service Guarantee fee* for more information about the Service Guarantee fee inclusions.

The BYOD device will be able to connect to the school wireless network and access the school's filtered Internet connection as well as access some of the school network drives. Printing from BYOD devices is supported. The school will install client software which will provide benefit to the student as well as a degree of visibility and management to the school while the device is connected to the school network. The client program will allow students to self-install software, access a flexible knowledge base for self-help and submit and view the status of their support tickets via the School's Service Portal. The software will provide the school with visibility to such things as device specifications, available hard drive space and when the device was last connected to the school network. This information is valuable when diagnosing connectivity and software installation issues.

Because of the potentially broad range of devices and configurations across all student-owned devices, only minimal assistance might be possible through the ICT Service Desk for issues beyond connection to the network, installation of software, basic triage and quick fixes.

Access to the department's ICT network is provided only if the device meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device [Advice for State Schools on Acceptable use of ICT Facilities and Devices](#).

Students and parents are responsible for the security, integrity, insurance and maintenance of privately-owned devices and their private network accounts.

Device selection

Before acquiring a device to use at school the parent or caregiver and student should be aware of the school's specification of appropriate device type, operating system requirements and software. These specifications relate to the suitability of the device to enabling class activities, meeting student needs and promoting safe and secure access to the department's network.

Breakdown of BYOD Service Guarantee fee

- BYOD – Concierge style Wi-Fi device connection subscription fees,
- Infrastructure requirements to support the BYOD scheme,
- Software license fees especially designed for BYOD devices (Inc. Adobe Creative Cloud),
- Technical support to connect to the school Wi-Fi and printers, and install Adobe software,
- Basic diagnosis of device software/hardware issues and recommendation of course of action (e.g. warranty claim, uninstallation of software, etc.).

Laptop Program Inclusions

The differences of the two schemes is outlined below:

	CYOD (Choose your own Device)	BYOD (Bring your own Device)
Device	Choice of approved and support devices.	Any device that meets minimum specifications.
Software and Operating System (Windows 8/10/+, Office 2013+, Anti-virus)	✓	✗
Adobe Creative Cloud Design and Web Suite	✓	✓ (not all platforms)
Adobe Creative Cloud Master Collection (Senior Secondary)	✓	✓ (requires an additional \$20 annual subscription)
School Software (MYOB, MixCraft, Inspiration, Sparkview, etc.)	✓	✗
Lemon Clause	✓	✗
Computrace anti-theft protection	✓	✗
Network Access	✓	✓*1
Internet Access	✓	✓*2

Internet Filtering		
• At School	✓	✓
• At Home	✓	✗
Onsite – Technical Support		
• On Site Warranty	✓ (3 years)	✗
• Battery Warranty	✓ (3 years)	✗
• On Site ADP ^{*3}	✓ (3 years)	✗
• Operating System rebuilds	✓	✗
• On Site fault diagnosis	✓	Provides advice only
• General Troubleshooting	✓	Provides advice only
• Access to Hot-Swap devices	✓	✗

*1 provided approved Anti-virus software installed.

*2 the use of personal 3G/4G Internet (including tethering to device) is not permitted at school. This includes BYOD devices. Non-filtered internet access is forbidden under Education Queensland policy as it poses a child protection issue. Only internet provided by the school is allowed to be used while the device is at school.

*3 excess may apply and there may be a limit to number of claims allowed. This information will be provided within the CYOD Selection Guide and is subject to the terms of the chosen vendor. 2016 and 2017 CYOD rounds have \$0 excess, one claim per calendar year.

Software and Applications

Students who participate in the CYOD scheme will have access to all necessary school software. As subject specific software demands change and new software versions are released, CYOD students will access to install school owned software as required.

With BYOD devices, the installation and maintenance of personal software is the responsibility of the family. Genuine versions of software need to be installed to ensure updates. Some subjects require the use of subject specific software. Historically at this school, subject specific software demands have changed from year to year. As the school has owned all student-use devices, this has not proved to be too challenging in the past, however with BYOD devices and the implications of software licencing, there may arise situations where students are required to acquire software on short notice. All reasonable measures will be made to ensure software choices have little or no financial implication on families choosing the BYOD option.

Adobe Creative Cloud

Adobe Creative Cloud Master Collection will be available to all Senior Secondary students in the CYOD scheme. For the BYOD scheme participants, the Adobe Creative Cloud Design & Web

K12 Apps is available to install. If the full Creative Cloud Master Collection is desired, a small annual fee of \$20 will be charged to install and run these applications. The device will need to be taken to the ICT Service Desk for installation. This fee is a cost imposed by Adobe for the upgraded licensing of the software.

Recommendation

It is recommended that, where possible, families join the Choose Your Own Device Program. It is the School's belief that the high quality devices, bulk-purchase pricing, 3-year warranty and accidental damage protection, access to Hot-Swap devices and full software and support offered; make the program a great value proposition for families over the life of the technology device. We see it as a convenient option for parents; with students being able to have any technology issues resolved themselves, via the School's ICT Helpdesk. Over the last two years of running the CYOD and BYOD programs, a far greater percentage of CYOD students are in their classes with a working device, than those who elect to bring their own device.

CYOD/BYOD Student Charter

This section of the CYOD/BYOD Handbook and Student Charter is relevant for all students, regardless of choosing the Choose Your Own Device (CYOD) or Bring Your Own Device (BYOD) program option.

Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a device at home, in transit or at school belongs to the student. CYOD participants are covered by Accidental Damage Protection (ADP)* warranties and the School's self-insurance against theft and loss*. Advice should be sought regarding inclusion in home and contents insurance policies for parents choosing the BYOD option.

*Excesses may apply and there may be a limit to number of claims allowed.

General precautions

- Food or drink should never be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don't place pressure on the lid of the device when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don't clean the screen with a household cleaning product.

Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is responsible for the backup of all data. While at school, students may be able to save data to the school's network, which is safeguarded by a scheduled backup solution. All files

must be scanned using appropriate anti-virus software before being uploaded to the department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive, SD card or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

Acceptable device use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within the [Acceptable Use of the Department's Information, Communication and Technology \(ICT\) Network and Systems](#)

This policy also forms part of this Student Charter. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

Communication through internet and online communication services must also comply with the department's [Code of School Behaviour](#) and the Responsible Behaviour Plan available on the school website.

While on the school network, students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems, school or government networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so as not to 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).

The password should be changed regularly, as well as when prompted by the department or when known by another user.

Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason.

Students should log off or lock the computer at the end of each session to ensure no one else can use their account or device.

Students should also set a password for access to their BYOD device and keep it private.

Parents/caregivers may also choose to maintain a password on a BYOD device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls with such use being the responsibility of the parent/caregiver.

Digital citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation. The school's Responsible Behaviour Plan also supports students by providing school related expectations, guidelines and consequences.

Cybersafety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver as soon as is possible.

Students must also seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Students are encouraged to explore and use the ['Cybersafety Help button'](#) to talk, report or learn about a range of cybersafety issues.



Students must never initiate or knowingly forward emails, or other online content, containing:

- a message sent to them in confidence
- a computer virus or attachment that is capable of damaging the recipients' computer
- chain letters or hoax emails

- spam (such as unsolicited advertising).

Students must never send, post or publish:

- inappropriate or unlawful content which is offensive, abusive or discriminatory
- threats, bullying or harassment of another person
- sexually explicit or sexually suggestive content or correspondence
- false or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to read the department's [Cybersafety and Cyberbullying guide for parents and caregivers](#).

Web filtering

The internet has become a powerful tool for teaching and learning; however students need to be careful and vigilant regarding some web content. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the [Code of School Behaviour](#) and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering applied.

The filtering system provides a layer of protection to staff and students against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

Students are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET network must also be reported to the school.

All CYOD devices are protected by web filtering when connected to the internet away from the school. Any parents choosing the BYOD option are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate internet use by students outside the school.

Parents, caregivers and students are also encouraged to visit the [Australian Communications and Media Authority's CyberSmart website](#) for resources and practical advice to help young people safely enjoy the online world.

Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's device, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

Monitoring and reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The school reserves the right to restrict/remove access of school owned and personally owned devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of school owned and personally owned devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible use of Technology Devices at Kenmore State High School

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

Student

- participation in CYOD/BYOD program induction
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, see [ACMA CyberSmart](#))
- security and password protection — password must be difficult enough so as not to 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)
- maintaining a current back-up of data
- charging of device
- abiding by intellectual property and copyright laws (including software/media piracy)
- ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason
- understanding and signing the CYOD/BYOD Student Charter Agreement.

Parents and caregivers

- acknowledgement that core purpose of device at school is for educational purposes
- internet filtering for BYOD devices when not connected to the school's network
- encourage and support appropriate digital citizenship and cybersafety with students (for more details, see [ACMA CyberSmart](#))
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the CYOD/BYOD Student Charter Agreement.

The following are examples of responsible use of devices by students:

- Use technology devices for:
 - engagement in class work and assignments set by teachers
 - developing appropriate 21st Century knowledge, skills and behaviours
 - authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
 - conducting general research for school activities and projects

- communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
 - accessing online references such as dictionaries, encyclopedias, etc.
 - researching and learning through the school's eLearning environment
 - ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate and respectful of others when using a technology device.
 - Switch off and place out of sight the technology device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
 - Use the technology device for private use before or after school, or during recess and lunch breaks.
 - Seek teacher's approval where they wish to use a technology device under special circumstances.

The following are examples of irresponsible use of devices by students:

- using the device in an unlawful manner
- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and internet resources
- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violating copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the device's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invading 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
- using the technology device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use technology devices at exams or during class assessment unless expressly permitted by school staff.

In addition to this:

Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission and without them present.
- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.
- Students must get permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.
- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.
- Parents and caregivers need to be aware that damage to mobile devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's Responsible Behaviour Plan.
- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

Kenmore State High School – CYOD / BYOD Student Charter

Responsible use agreement

The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER:

- I have read and understood the *CYOD/BYOD Handbook and Student Charter* and the school *Responsible Behaviour Plan*. (Both documents available via School website).
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behavior, as per the intent of the *Student Charter* and the *Responsible Behaviour Plan*, will result in consequences relative to the behaviour.

Student's name: **Year:** **ID No**
(Please print)

Student's signature: **Date:** / /

Parent's/caregiver's name:.....
(Please print)

Parent's/caregiver's signature: **Date:** / /

Please note: Participation in the Student Technology Program (CYOD or BYOD option) is conditional upon participation in the Student Resource Scheme.

Version 2.1a Updated 5th November 2016

THIS IS A WORKING DOCUMENT AND MAY BE UPDATED THROUGHOUT THE YEAR.

Latest version will be available from the School website.