POLICY FOR

Responsible Digital Citizenship

Author		Approved
Name	David Carter & Karina Rowe	Executive
Position	For ICT CAG	

Document No.	Effective Date	Version Date	Version No.	Cancels Version
Po002	1/11/2017	1/11/2017	001	New

1.0 Purpose

This policy identifies processes undertaken at Norwood Morialta High School to ensure the use of Digital Technology is aligned to the Department for Education and Government legislative requirements.

This policy is also design to support students in Cyber Safety and transparent use of all technologies whilst as a student at Norwood Morialta High School and beyond.

2.0 Version Control

Version Date	Version Number	Reference sections	Description of the change
1/11/2017	001	Not Applicable	New document introduced

3.0 Scope and Responsibilities

3.1 Scope:

The computer network, internet access facilities, computers and other ICT equipment/ devices bring great benefits to the teaching and learning programs at Norwood Morialta High school. The ICT equipment is for educational purposes appropriate to this environment and in keeping with our core values.

3.2 Responsibilities:

This school is committed to providing its students with a quality, internationally recognised education that prepares them for their future life. A BYOD Program means students have a range of ways to complete any set task allowing each student to be able to connect globally, learn collaboratively and use their laptop as a creative ideas device.

Students at Norwood Morialta High School are expected to have a laptop with them at each of their lessons and are supported by the school to ensure ethical and safe use of Technology is undertaken.

4.0 Policy Principles

4.1 Use of Technologies

4.1.1 Students must ensure they bring a full charged device to all lessons unless the teacher has otherwise requested. Teaching and learning programs will make use of devices to benefit students' learning through challenged based and collaborative learning activities and new ways to expose students to real world context.

4.1.2 Off-task behaviour will be subject to consequences in line with NMHS Promoting Responsible Behaviour Policy.

4.1.3 Any pornographic material, illegal movies / TV series / game downloads etc found on a device will result in suspension and/or exclusion from school. Any unlawful activity will be referred to SAPOL.

4.1.4 The use of the device is on the understanding that students will follow teacher instructions and access applications and files in safe and ethical ways. Students must not disrupt the smooth running of any school ICT systems nor attempt to hack or gain unauthorised access to any system. The school's wellbeing and responsible behaviour processes extend outside of school hours or off site.

4.1.5 NMHS reserves the right to monitor the content of student device(s) and may conduct live monitoring of activity on any device connected to our school network. Students must permit school staff and parents/caregivers to perform checks when requested and may have 'Parental Control' enabled by the school at the school's discretion.

4.1.6 Teachers and parents/caregivers may recommend students for 'Parental Control' where a student will have limited privileges and be unable to install software. These limited privileges may include websites, times of day, software, mail and chat.

4.1.7 Consequences for inappropriate use will be in accordance with the school's

Promoting Responsible Behaviour Policy and may include confiscation of the device for a period of time or managed privileges.

4.1.8 At the discretion of the school, a student's device screen may be displayed at any time to visitors in the school. Students' screens may be shared on any of the large display screens in the school.

4.1.9 The camera is only to be used in class with teacher permission. Photos of another person must be with their permission.

4.2 Cyber Safety

4.2.1 Staff, students and parents/caregivers must familiarise themselves with the content of the 2009 document *Cyber-safety: keeping children safe in a connected world: Guidelines for schools and preschools (available at www.decs.sa.gov.au/speced2/pages/cybersafety).*

4.2.2 The following is an excerpt from the overview of the Cyber-safety document:

"Learning is a social activity. It happens when people interact with other people and their ideas, knowledge and perspectives. ICTs provide children and students with new and engaging ways to learn. ICTs expand social and knowledge networks so that children and students access current information, interact with experts and participate in peer teaching and learning."

4.2.3 Using ICTs they can publish their learning, as evidence of achievement or to invite feedback for improvement. It is important to both protect and teach children, students and adults, while they learn to use ICTs and become responsible digital citizens. This includes adults thinking ahead of new risks and children and students learn how to avoid exposure to inappropriate material or activities, and protecting themselves when they are online. They need to learn how to use ICTs, including mobile technologies and social networking sites, in responsible and ethical ways. In addition, they need to feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate events. In response, these adults need to take appropriate actions to protect the child or young person.

4.2.4 Key aspects of Cyber Safety include:

- Students must not give out identifying information online, use only their first name and not share their home address, telephone number or any other personal information such as financial details (e.g. credit card), telephone numbers or images (video or photographic) of themselves or others.

- Students must not use their school e-mail address in non-school online communications as this e-mail address contains their personal name and school details.

- Students must use the Internet, e-mail, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.

- Students must not forward inappropriate material to others.

- Students should never respond to message or bulletin board items that are suggestive, obscene, belligerent, threatening or make them feel uncomfortable - these messages should be reported to a teacher.

- Students must inform their teacher immediately if they see anything on a website that is inappropriate, unpleasant or makes them uncomfortable.

- Parents/caregivers and teachers should actively monitor online behaviour and encourage their child/student to follow Cyber-safe strategies.

4.3 Internet Usage at School

4.3.1 According to The Department for Education ICT Security, Internet Access and Use, and Electronic Mail and Use policies, students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and students may not access or distribute inappropriate material. This includes:

- distributing spam messages or chain letters
- accessing or distributing malicious, offensive or harassing material, including jokes and images
- bullying, harassing, defaming or giving offence to other people
- spreading any form of malicious software (e.g. viruses, worms)
- accessing files, information systems, communications, devices or resources without permission
- using for personal financial gain
- using non-approved file sharing technologies (e.g. Torrent)
- using for non-educational related streaming audio or videos
- using for religious or political lobbying
- downloading or sharing non-educational material.

4.3.2 Norwood Morialta High School will make every reasonable effort to provide a safe and secure online learning experience for children and students. However, internet filtering is not 100 per cent effective and it is not possible to guarantee that children and students will not be exposed to inappropriate material.

4.3.3 The cost to access the Internet at school is currently included in the school fee and allows for students to make reasonable use of the Internet for the purpose of learning. Internet traffic is monitored and students making unreasonable downloads will incur an additional fee.

NB: Norwood Morialta High School accepts no cost for Home-Internet provision. In order to ensure equity of access to the curriculum, school learning tasks that require compulsory Internet access outside of the subject lesson will have a due date greater than two nights.

The Internet Service Provider provides Home-Internet logon details, and it is the responsibility of the student/parent/caregiver to setup the Home-Internet connection on the device(s).

4.4 YouTube Access

4.4.1 Norwood Morialta High School provides a filtered internet service. Filtering that is applied to internet content is in line with DfE regulations and applies to websites such as YouTube.

4.4.2 The school always endeavours to keep students protected from inappropriate internet content. At this time the school is asking for consent from parent/caregiver to access the website www.youtube.com.

4.4.3 YouTube is a video-sharing website. The site allows users to upload, view, rate, share, and comment on videos. Most of the content on YouTube has been uploaded by individuals, but commercial entities also provide content and advertisement. Videos deemed potentially offensive are available only to registered users affirming themselves to be at least 18 years of age.

4.4.4 Norwood Morialta High School will be unblocking YouTube for students who return this consent form. YouTube attempts to filter and remove inappropriate content, however, it is not guaranteed that students who have consent will not be exposed to this content.

4.5 Passwords

4.5.1 The Department for Education ICT Security and Internet Access and Use policies contain the following main provisions with regard to passwords:

- Passwords must be kept confidential and not displayed or written down in any form.
- Passwords must not be words found in a dictionary, or based on anything somebody else could easily guess or obtain using person-related information.
- Students must not disclose their personal passwords to any person.
- Students will be accountable for any inappropriate actions (eg bullying, accessing or sending inappropriate material) undertaken by someone using their personal user-ID.

4.6 Copyright

4.6.1 Students must realise their responsibilities regarding intellectual property and copyright law and ethics, including acknowledging the author or source of information.

4.6.2 To ensure compliance with copyright laws, students must only download or copy files such as music, videos or programs, with the permission of the owner of the original material.

4.6.3 If students infringe the Copyright Act 1968, they may be personally liable under this law.

4.7 Printing

Staff and students are encouraged to upload work electronically and lessen the need to print documents. Students will be permitted to print to printers from all devices. Printing restrictions and charges apply.

4.8 Software installation, games and music on loan devices

4.8.1 Students may have Administrator access on loaner devices and may be permitted to install certain types of software and files provided they have acquired a legitimate license.

4.8.2 Student installed software must be educational in nature or have a direct relationship to student learning.

4.8.3 Non-educational software, games and music are not recommended as they will unnecessarily use space on the hard drive and therefore impede use of the device for learning. Students using non-educational software, games and files at school will be subject to consequences according to the 'Acceptable Use' section.

4.8.4 In instances where the device performance is restricted due to student installed software and files the hard drive will be erased and re-imaged by ICT Team.

4.8.5 Under no circumstances may software and files be installed without the appropriate license. Students doing so will be liable to prosecution.

Parents/caregivers are encouraged to regularly monitor the contents of the device.

4.9 Social Networking

4.9.1 Under certain circumstances social networking sites may be beneficial for learning. However, in many instances social networking sites can be a distraction and potentially unsafe. Students must seek permission from their teacher or parent/caregiver before accessing social networking sites.

4.9.2 School Internet filters block many social networking sites.

4.9.3 Parents wishing to filter Home-Internet on the MacBook should refer to the section titled 'Parental Control'.

4.9.4 Students using social networking sites without permission during lessons will be subject to consequences according to the 'Acceptable Use' section.

4.9.5 Students are reminded to use Cyber-safe strategies and use the Internet in a safe and ethical manner.

4.10 Private Laptops and Personal Devices

4.10.1 Private laptops and personal devices add complexity to the functionality and maintenance of the school network. Only BYOD iPads and school-supplied devices, providing they have the standard image applied, can be supported by the school.

4.10.2 Only staff, students, and other school-approved users are permitted to access the school's network.

4.10.3 Middle Campus students will be also required to comply with the MC Mobile Phone Guidelines.

4.11 Occupational Health Safety and Welfare

4.11.1 Students are advised to consider the following advice when using their device:

- taking regular rest breaks within the confines of the classroom and at the discretion of the teacher
- not using the device for more than 2 hours in any one session
- working in an environment free from glare
- using the device on a desk rather than on the lap whenever possible
- angle the screen to minimise the need to bend the neck
- maintaining good posture.

4.11.2 The main feature of mobile devices that causes problems is the minimal amount of ergonomic adjustment – this promotes poor posture. Students should be aware of their mobility while using the device.

4.12 Preventing Eye Strain

4.12.1 Eye-strain and headaches can be caused by the constant viewing of small objects on small screens, incorrect monitor position, or glare or reflection from lighting sources.

4.12.2 The risk of eyestrain can be reduced by ensuring students:

- work in environments free from glare or reflection
- have adequate lighting
- increase font size for comfortable viewing
- position the screen for comfortable viewing distance
- take frequent breaks from the screen, for example: every 20 minutes look at something 20 feet away (approx 6 metres) for 20 seconds
- regularly blink to lubricate your eyes.

5.0 Definitions and Abbreviations

5.1 Definitions

Nil.

5.2 Abbreviations

- BYOD — Bring Your Own Device
- NMHS — Norwood Morialta High School
- ICT — Information Communication Technology
- SAPOL — South Australian Police
- DfE — Department for Education (formally DECD)

6.0 Attachments and References

6.1 Attachments

Nil

6.2 References

- Promoting Responsible Behaviour Policy
- ICT laptop Agreement Form
- MC Mobile Phone Guidelines
- YouTube Consent Form
- Copyright Act 1968
- DECD Standard – Information Management System
- DECD Standard – School ICT Network Security
- DECD Standard – ICT Security
- DECD Standard – Internet Access and Use
- DECD Standard – Electronic Mail Access and Use
- DECD Procedure – Mobile Communication Devices
- DECD Guidelines - Cyber-safety: keeping children safe in a connected world.

7.0 Review

Review Date	Reviewed By	Accepted Date	Comments
1/5/2018	Executive	1/7/2018	Next review 2019