NEERIM SOUTH PRIMARY SCHOOL
Information, Communications and Technology Usage Policy

Respect **Learning** **Teamwork** **Perseverance**

1. Rationale

1.1 Neerim South Primary School believes the teaching of cybersafety and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school. The school supports the belief that through digital technologies we equip children to participate in a rapidly changing world where work and leisure activities are increasingly transformed by technology. We enable students to find, explore, analyse, exchange, present and create information. We also focus on developing the skills necessary for children to be able to create and use information in a discriminating, effective and creative manner. To be safe and to gain the greatest benefit from the opportunities provided through an online environment, students need to be responsible for themselves and respectful of others online, particularly when using technology independently. The school embraces the benefits of technology and is committed to reducing students' exposure to cyber-risks (such as cyberbullying, online sexual predation, sexting, identity theft and fraud) when using the Internet, mobile phones and other electronic personal devices. This policy applies to all digital technologies, social media tools and learning environments established by our school or accessed using school-owned networks or systems, including (although not limited to): School-owned ICT devices, emailing and instant messaging, Intranet, social networking sites, video and photo sharing websites, blogs, forums, discussion boards, wikis, podcasts, and video / web conferencing.

1.2 **Who -** This policy applies to the users of the Neerim South Primary School and Department computer network and equipment and applies to all staff, students and any other users of digital technologies in the school.

1.3 **Why –** The internet provides students with unprecedented opportunities to obtain information, engage in discussion, and liaise with individuals, organisation and groups world-wide so as to increase skills, knowledge and abilities. However, inappropriate use of digital technology including the internet is strongly discouraged and actively managed within our school community.

1.4 **What equipment -** The policy covers the use of Information and Communication Technology (ICT) equipment owned by the school and personal items such as mobile phones, smart phones and wireless-capable devices that access the internet.

1.5 **What activities -** This policy encompasses the use of all electronic communications whether or not these are published to the web or sent electronically, and includes but is not limited to:

- Publishing and browsing on the internet;
- Downloading or accessing files from the internet or other electronic sources;
- Email;
- Electronic bulletins/notice boards;
- Electronic discussion/news groups;
- Weblogs ('blogs');
- Social networking;
- File transfer;
- File storage;
- File sharing;

Reviewed by: Environment Subcommittee: 20180906
Ratified by School Council: 20180910
Version: 5
Valid To: 6th September 2019
U:\EWC\POLICY__Current\03. Student Welfare\3.4 Additional Evidence\3.4(d) ICT Usage Policy - valid to 20190906.docx

- Video conferencing;
- Streaming media;
- Instant messaging;
- Online discussion groups and 'chat' facilities;
- Copying, saving or distributing files;
- Viewing material electronically; and
- Printing material.

1.6 **How –** see Implementation

2. Aims

- The aim for this policy is:

2.1 To improve student learning outcomes by increasing access to worldwide information and technologies.

2.2 Establish an **eSmart** culture which is keeping in with the values and expectations of the school.

2.3 Develop an **eSmart** culture that follows legislative and professional obligations (Victorian Curriculum).

2.4 Ensure the **eSmart** culture meets the values of the NSPS Student Engagement and Wellbeing policies.

2.5 To educate students on their role and responsibilities as a digital citizen, including awareness of dangers and managing their online identities.

2.6 To reinforce within the school community what bullying is (including cyberbullying), and the fact that it is unacceptable.

2.7 Everyone within the school community to be alert to signs and evidence of cyberbullying and to have a responsibility to report it to staff, whether as perpetrator, observer or victim.

2.8 To ensure that all reported incidents of cyberbullying are investigated appropriately and that support is given to both victims and perpetrators.

2.9 To seek parental and peer-group support and co-operation.

2.10 To use this policy in conjunction with the NSPS **eSmart** use of ICT Guidelines, and Acceptable Use Agreements, to outline the conditions applying to use of all school ICT and behaviours associated with safe, responsible and ethical use of technology.

3. Implementation

- There are four interrelated strategies undertaken by the school:

3.1 **Primary prevention** (educating, building belonging and promoting wellbeing)

- Supporting the rights of all members of the school community to engage in and promote a safe, inclusive and supportive learning environment.
- Using our school core values (respect, learning, teamwork and perseverance):
  - to educate our students to be safe and responsible users of digital technologies; and
  - as the basis for discussions about how we treat others in an online environment.
- Educating our students through the classroom and specific Cybersafety programs, to:
  - develop digital literacy skills and
  - be safe and responsible users of digital technologies.

3.2 **Early intervention** (developing expectations, strengthening coping skills and reducing risk factors)

- Training staff in the philosophies of the eSmart Program and provide the information necessary for Cybersafety education.
- Supporting parents/guardians to understand the importance of safe and responsible use of digital technologies, the potential issues that surround their use and strategies that they can implement at home to support their child
- Raising our students' awareness of issues such as online privacy, intellectual property and copyright.
- Providing a filtered Internet service but acknowledge that full protection from inappropriate content can never be guaranteed.
- Provide supervision when using digital technologies.

3.3 **Intervention** (providing access to support information and treatment)

- Responding to issues or incidents that have the potential to impact on the wellbeing of our students.
- Knowing that some online activities are illegal and as such we are required to report this to the police.
- Advising students to report an incident to their teacher immediately if:
    - They have experienced an incident of Cyberbullying.
    - They feel the welfare of other students at the school is being threatened.
    - They come across sites which are not suitable for our school.
    - Someone writes something they don't like, makes them or their friends feel uncomfortable or asks them to provide private information.
    - They accidentally do something which is against the rules and responsibilities they have agreed to.
- Ensuring that any student who does not follow the rules of the ICT Acceptable Use Agreement and the 'NSPS eSmart Use of ICT Guidelines' loses their ICT privileges for a length of time as deemed appropriate by the Principal, ICT Coordinator or Teacher. They will also be required to complete additional Cybersafety lessons before their privileges are returned.
- Referring all incidents of cyberbullying to the Principal and ICT Coordinator for investigation. Any action taken will be in line with the Student Engagement Policy.
- Notifying parents to meet with school staff if students are involved in any incidents of cyberbullying.

3.4 **Post intervention** (restoring wellbeing, managing trauma and limiting impact)

To an extent, these levels overlap and span the range of provision of care from the support needed for all children and young people to the support needed in crisis situations. In most instances, the first two levels of support (primary intervention and early intervention) will come from the classroom teacher. Intervention and Post intervention strategies will be supported mainly through the ICT Coordinator and Principal.

Each year our ICT Coordinator seeks feedback from our school community in order to enable us to review and confirm support for the program. School procedures are followed for parents and students to seek referral, manage complaints and to opt out of the program.

Student Access

Students at all year levels are offered access to the school network, to the internet and the Department Intranet.

School Network:

Within the school network students are allocated a personal folder for their own work and can access a shared folder of school-wide resources such as shared student work, learning tools, software and educational games. Student access to the school network from F-1 is a single user name and password. Students from 2-6 access the school network by individual login and password.

Wireless Network

The school network and internet is also accessible through wireless access points (waps) located throughout the school. The wireless network is a closed network and can only be accessed with a digital certificate or password. Students are not permitted to access the wireless network using smart phones or other personal wireless capable devices.

Internet:

Students access the internet through use of a student login and password. Many unsuitable or inappropriate sites are blocked by the internet service provider and cannot be accessed with a student account.

The network administrator can also block and unblock sites if deemed necessary. Students will only access the internet when a teacher is directly supervising individuals or a class group. Students will log on using a specified password. The school will monitor student usage and attempted violations.

Email:

Students from 2-6 will be provided with a school specific email that is for educational purposes. This will be restricted to the school (neerimsouthps.vic.edu.au) domain, at school and home, and used for purposes relating to the curriculum. The school expectations apply to all use of the email, both within and outside of school. Outside parties are unable to email without approval from ICT Administrators. At school, students will only access accounts with teacher permission and supervision. The students' email is able to be accessible at home with parent permission and supervision.

At school, Students will not be allowed to check, read or send email from private accounts (e.g.: hotmail, gmail, etc.).

School Website & Newsletter:

Students may contribute to the school's website and newsletter. This can include school work produced by the student and could include images of student groups in the school environment.

The school newsletter is accessible in a digital format and is sent directly to parents/guardians accounts. The newsletter is available on the school's website.

Social Media:

Students are blocked from accessing social media sites such as Facebook, Twitter, etc. on the school network.

The school social media accounts are to be for educational and communicative purposes. These are accessible, maintained and managed by approved staff members.

Classroom blogs and other Social Media tools are designed for communication between students, parents and teachers. The use of social media is to positively engage

parents/guardians and community members. The correspondence is restricted to 'likes', any other comments are encouraged to be submitted directly to the school's email account. All unapproved posts will be removed by the social media administrators.

Mobile Phones:
Neerim South Primary School acknowledges that mobile phones may be used as a safety measure out of school hours for children who travel alone, on public transport or commute long distances to school. Parents are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in any appropriate way. The school acknowledges that some students own or have access to mobile phones and other web capable devices which may enable them to make phone calls, text, browse the web and access social media etc. The school also acknowledges that students who bring mobile phones to school might use them before or after school in an unsupervised environment (e.g. on a bus). However, students are not permitted to have mobile phones at school and must hand them in at the office when they arrive at school and collect them before leaving. The school accepts no responsibility for lost, stolen or damaged mobile phones or other electronic devices.

Acceptable Use – Students
When students use digital technology they must agree to:

- always use appropriate language, volume and tone
- be considerate of people and places around me
- communicate positively on electronic devices
- be polite and considerate.
- ensure that all the work that student do using the internet is their own
- acknowledge the creator, if students copy something from online, letting their audience know by sharing the website link
- understand the school email account is for educational purposes only

When students use digital technologies, they protect personal information by being aware that their full name, photo, birthday, address and phone number is personal information and is not to be shared online.
This means they agree to:

- only use their own login and email.
- protect their friends' information in the same way
- protect their passwords and don't share them with anyone
- only access sites that relate to their work, considering relevance and accuracy
- never join spaces without their teacher's guidance and permission
- never answer questions online that ask for their personal information
- not post three or more pieces of identifiable information about themselves.

When they use digital technologies, they respect themselves and others by thinking about

what they share online.

This means they:

- stop to think about what they post or share online
- use spaces or sites that are appropriate, and if they are not sure they ask a trusted staff for help
- protect their friends' full names, birthdays, school name/s, addresses and phone numbers because this is their personal information
- speak to a trusted staff if they see something that makes them feel upset or if they need help
- speak to a trusted staff if someone is unkind to them or if they know someone else is upset or scared
- don't deliberately search for something rude, violent or inappropriate
- turn off the monitor or close the screen if they see something they don't like and tell a staff member
- are careful with the equipment they use.

At school, they have:

- discussed ways to be a safe, responsible and ethical users of digital technologies
- discussed how to be responsible with equipment and programs/attachments
- presented their ideas around the ways that they can be smart, safe, responsible and ethical users of digital technologies

The Acceptable Use Agreement also applies during school excursions, travelling to and from school, camps and extra-curricula activities. Students must acknowledge and agree to follow these rules. Access to the internet and mobile technology at school will be renegotiated if a student does not act responsibly and follow the guidelines of the agreement.

- **Staff Access**

  All usage of the school network and resources must comply with laws relating to discrimination, equal opportunity, privacy and workplace bullying and harassment, including cyber bullying.

  The school network is primarily a business tool to be used for educational purposes. It is to be used like other business communications and comply with any codes of conduct which apply to the user, such as the Code of Conduct for the Victorian Public Sector, and Teaching Service Orders.

  Users of the network may use communications for limited personal use as long as this does not interfere with their professional responsibilities, is reasonable and not excessive. Unreasonable or excessive personal usage constitutes a failure to abide by this policy and may result in disciplinary action.
  Subject to limited personal use, the school network and internet access must generally not be used to conduct private business or private commercial transactions, to gamble, or carry out research into non-work related topics.

Non-compliance with this policy will be regarded as a serious matter and appropriate action will be taken when a breach of the policy is identified.

Any failure to abide by this policy may result in disciplinary action including revoking or restricting any right to use the equipment or network.
Teachers are responsible for ensuring all students under their responsibility are taught about cyber safety and the ICT Acceptable Use agreement.

4. Evaluation

- This policy is reviewed annually.

5. Resources

- https://www.esafety.gov.au/
- http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/advicecybersafe.aspx
- https://www.eduweb.vic.gov.au/edulibrary/public/govrel/Policy/2011acceptable-use-policy-ICT.pdf (requires login)
- Dept of Education Email and Internet Acceptable Use Policies
- eSmart: https://www.esmart.org.au | https://www.esmart.org.au/esmart-schools/
- Kids Helpline 1800 551 800 http://www.cybersmart.gov.au/report.aspx
- Neerim South Primary School ICT Acceptable Use Agreement
- Neerim South Primary School Privacy Policy
- Neerim South Primary School Anti Bullying and Harassment Policy
- Neerim South Primary School Student Welfare Policy

6. Revision History

- This is based on the prior Internet Usage agreement 2016/2017

Date	Description	Author
13/10/2015	Ratified by School Council	Environment SC
28/06/2016	Add Revision History, Version Number and Valid To date	Environment SC
18/04/2017	Reviewed by Environment SC	Environment SC
22/05/2017	Ratified by School Council	Environment SC
19/09/2017	Reviewed by Caleb Collins, as per eSMART program. Updates from Kirsti Farr	Environment SC
06/09/2018	Reviewed by Environment SC. Minor formatting amendments. Review links	Environment SC