**LARA LAKE PRIMARY SCHOOL IPAD PROGRAM 2022**

**Rationale**

* Lara Lake Primary School believes the teaching of cyber safety and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school
* Students in the 21st century students spend increasing amounts of time online; learning and collaborating. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online, particularly when no one is watching.
* Safe and responsible behaviour is explicitly taught at our school and parents/carers are requested to reinforce this behaviour at home. Some online activities are illegal and as such, may be reported to police.
* Lara Lake Primary School uses the Internet and Digital Technologies as teaching and learning tools. We see them as valuable resources, but acknowledge they must be used responsibly.
* This agreement aligns with Child Safe Standards (for more information see our Child Safe Policy)
* Lara Lake implements a BYOD program in grade 5/6 area and uses school owned devices in Grade P-4

**THE SCHOOL WILL:**

* maintain eSmart accreditation/membership which outlines how schools develop safe online practices (see more at https://www.**esmartschools**.org.au/)
* have a cyber safety program at the school which is reinforced regularly
* have policies in place that outline the values of the school and expected behaviours when students use digital technology and the internet
* provide a filtered internet service
* provide access to the Department of Education and Early Childhood Development’s search engine Connect (www.education.vic.gov.au/primary) which can be used to direct students to websites that have been teacher recommended and reviewed
* provide supervision and direction in online activities and when using digital technologies for learning
* support students in developing digital literacy skills
* use mobile technologies for educational purposes
* provide support to parents/carers via information evenings and through the document attached to this agreement
* provide a student-centred 1:1 program to support personalised learning

**When cyber bullying has occurred, the incident(s) will be handled in the following manner:**

* ensure parents/guardians are informed
* ensure a member of the school leadership team is informed
* provide appropriate support to students who are targets of bullying and those who demonstrate bullying behaviours
* ensure offender is addressed by a relevant staff member
* inform Police (where appropriate or necessary)
* contact the website or online service, if applicable, to ensure offending content is removed
* take appropriate actions and apply relevant consequences, as appropriate (such as suspension of privileges for a period of time depending on the severity of the incident)

**GENERAL INFORMATION**

Being online can make students feel that they are anonymous and sometimes students may say things online that they would never say to someone’s face. The web space or online chat environment that they use in leisure time might also have explicit language and they may feel they have to be part of it. Bullying online can take a number of forms from repeated messages to exclusion from social spaces. Students who forward on messages or participate in the exclusion may not see themselves as bullying. These actions also contribute to the hurt and distress of others.

Incidents online often go unreported. Reasons include feelings of embarrassment, a belief that online issues are theirs to solve as adults don’t understand, a feeling that reporting it will make it worse and the most common reason given is a fear that they will lose access to their technology.

Seek to understand the terms and conditions of websites and online communities and be aware that content uploaded or posted leave a digital footprint. Many websites/spaces have conditions of use, such as ownership of the content and the age of participants. For example: Children under 13 years of age are not permitted access to Facebook, Instagram or Snapchat. Students like to publish information about themselves and their friends in online spaces, including using popular communication applications such as Tik Tok or Roblox. This can put them at risk of being approached, groomed or bullied online.

It is important to realise that there is a time for fun and a time for work even on the Internet. By taking care with the equipment, and thinking carefully about printing and downloading from the internet students can save time, money and the environment. Staying on task will reduce the risk of inappropriate access and teach students strategies to use the Internet or mobile technologies for their learning.  If your child is spending hours online ‘doing their homework,’ it may be that they are multitasking in many other applications, some of it study related and other interaction may be social.

Web tools and social networking spaces allow students to be contributors to the web and to work collaboratively online with other students. Creating or contributing to blogs, wikis, digital stories and podcasts can all be legitimate educational activities which allow students to publish, share and inform others and be active contributors to the web. It is important for students to understand that working in a collaborative space as part of a learning task, has a very different purpose to using a social networking space to link up with friends in their own time.

Music, information, images and games on the Internet are owned by someone. The term ‘Copyright’ is a legal one and there are laws to enforce it. Not only is breaking copyright morally, ethically and legally wrong, it can introduce potential risks. By downloading a ‘freebie’ you can risk bringing a virus or spyware to the computer or system. These can destroy a computer system or provide hackers with details such as passwords and bank accounts.

Not everything on the Internet is true, accurate or unbiased. The school is working to teach digital literacy skills, which enable students to locate, evaluate, and use information effectively on the Internet. It is important that your child respects the Intellectual Property of people who contribute resources online. Students should use their own thoughts and language to express what they have learnt, and avoid simply copying and pasting information from the Internet.

In school settings, Internet service providers set up filters to block out a lot of inappropriate content, but these filters are not always foolproof. Students, who deliberately seek out inappropriate content or use technologies, which bypass filters, will have their Internet access reviewed and their parent/carers will be immediately informed.

Students are responsible for everything done using their accounts, and everything in their home directories.  To this end, students need to keep their password secret and not gain access to other students’ login details. The school connects all of the computers through a network. The introduction of unknown games or files could introduce viruses, etc. and these put all school equipment and student work at risk.

**THE STUDENTS WILL:**

**Broad Guidelines**

* Follow the guidelines of our Student Engagement/Wellbeing Policy
* Be a safe, responsible and ethical user of ICT at school
* Communicate respectfully via ICT at all times
* Talk to a teacher if anything uncomfortable or unsafe online occurs
* Identify concerns to teachers if they see others participating in unsafe, inappropriate or hurtful online behaviour
* Report incidents if they feel that the welfare of themselves or other students at the school is being threatened
* Report websites they come across sites which are not suitable for their school
* Report to teachers when someone writes something they don’t like, or makes them and their friends feel uncomfortable or asks them to provide information that they know is private
* Password protect any spaces or accounts they have
* Protect privacy rights and those of other students by not giving out personal details including full names, telephone numbers, addresses and images
* Abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary)
* When posting information online, a good rule is, “Don’t post what you wouldn’t want your Grandparent, Principal, or future boss to read.”
* Understand the terms and conditions of any website or online community that they might join
* Take a screenshot of any content they deem to be inappropriate as evidence that they can show a trusted adult
* Think critically about other users’ intellectual property and how I use content posted on the Internet, not simply copy and paste information from websites.
* Only take photos and record sound or video when it is part of a class or lesson
* Seek permission from individuals involved before taking photos, recording sound or videoing them  (including teachers) during camp and excursions
* Seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space
* Be respectful in the photos I take or video captured and never use these as a tool for bullying
* Protect devices at all times. This includes not using devices in the schoolyard without supervision and supplying a sturdy case for its protection (the device must not come to school without a case (Grades 4-6)).

**STUDENTS WILL NOT**

* Share personal details, including images of themselves or their friends online
* Allow anyone they don’t know to join their chat or collaborative space
* Use full names in reference to individuals in any image, movie or sound recording
* Interfere with network security, the data of another user or attempt to log into the network with a user name or password of another student
* Reveal their password to anyone except the system administrator or classroom teachers
* Bring or download programs without permission, including games, to the school or run them on school computers
* Deliberately enter or remain in any site that has obscene language or offensive content (e.g. racist material or violent images)
* Write or participate in online bullying
* Use any device in the school yard before school, after school or during recess or lunchtimes

**SUPPORT FOR FAMILIES**

**Research shows that students are reluctant to report issues and put at risk their internet/phone access**

* Encourage your child to set their space to ‘private’ if they use a social networking sites (they are then in control of who can contact them and access their information).
* Ensure that all Internet activities occur in a shared place – not your child’s bedroom. Negotiate appropriate times for online activities and use of mobile phones. Consider the use of “safe search filters” freely available as settings on Google, Bing etc.
* Set restrictions on the iPad to prevent your child from accessing harmful content.

**Advice to support the safe and responsible use of digital technologies at home**

At school the Internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet and chat. The term “space” is used here to describe a website or app that works like a community with live interaction and the capacity for your child to chat with others, personalise their space and share information. Each space has a purpose, audience and tool set including those around security and protection. The Internet also provides access to websites with information, images and videos for students to view. Not all content is presented as a space.

**Key discussion questions for parents to ask**

At home we recommend you make some time to find out how your child is using the Internet. Make some time to sit with them online and ask questions such as:

* What are you looking at right now?
* What is it that is so enjoyable about the site or space you are using? What is the purpose of the site or space?
* How does it work? How do you set it up? What are the conditions of use?
* Who is else is sharing this space? Do you know them or did you ‘meet’ them online? How can you control who is in your space?
* Can you see any risks or dangers in the activity? What would you say to warn/inform a younger child?
* What are you doing to protect yourself or your friends from these potential dangers?
* When would you tell an adult about an incident that has happened online? Who would you tell?
* When wouldn’t you tell and why not?

**About the agreement**

In signing this agreement your child will be agreeing to behave in a certain way online and to take appropriate action when and as required. Elements of agreement are explained below. Please contact the school to clarify or receive additional information.



**Lara Lake Primary School – Individually Owned Devices and Age Appropriate Apps**

While the vast majority of individually owned devices utilised at school do comply with age restriction conditions, some do not. Some individually owned devices are problematic in that the content contained on those, which is generated out of school hours, can impact on school life and the wellbeing of young students. Students who are not old enough to access apps are using them and some of the content being distributed out of school hours is alarming and disturbing. Inappropriate content including images, text, cyber-bullying and other conversations are being posted by some students and shared with other students and this is alarming parents and school staff. This is happening in the homes of some of Lara Lake Primary School’s students.

The age ratings that come with games, apps, films and social networks are a good guide to whether they’re suitable for your child. If the age restriction is 13 years and your child is younger than that, they should not be accessing that app.

**All of the Apps listed below require users to be at least 13 years old:**

Tik-Tok, Facebook, Messenger, Snap Chat, Instagram, Twitter, Pinterest, Tumblr.

A thorough list of age appropriate apps is provided by the Australian Government at <https://esafety.gov.au/education-resources/iparent/staying-safe/social-networking/is-there-an-age-limit-for-kids-on-social-media>

Devices that have Apps with age restrictions of 13 or above will not be permitted on to Lara Lake Primary School property or given access to school WiFi or Servers. Devices are monitored centrally by school servers as a matter of duty of care. In the instance where a student’s device is found to have inappropriate Apps installed, the following process will be implemented:

**1st time** Device shut down at school and student given warning. Parents notified.

**2nd time** Device shut down at school and student given warning. Parents notified.

**3rd time** Device banned from school for three weeks.

**4th time** Device banned from school at Principal’s discretion.

Any student whose device has been banned will have shared access to school-provided devices.

Please be assured that a firewall, filter system and other protective measures are implemented at all Government schools and are updated continuously.

The following information provides some hints around ensuring your child is safe:

**INTERNET SAFETY CHECKLIST FOR PRE-TEENS**

**Have free and frank discussions**

Encourage your child to talk to you about how they use the internet and show you what they do. Discuss with them the kinds of things they might come across. A good time to talk is when they get a new device or mention a new website.

**Manage their devices**

Encourage them to use their tech devices in a communal area such as the living room or kitchen and set up a user account for your child. If you think they aren’t old enough to have a mobile phone or tablet, stay firm and explain the reasons why. Don’t permit use while your child is unsupervised.

**Put yourself in control**

Activate parental controls on your home broadband, all devices including mobile phones and games consoles. Safe search settings can also be activated on Google (and other search engines), YouTube and on entertainment sites like iTunes and iPlayer.

**Stay safe on the move**

Be aware that if your child is accessing the internet using public WiFi they may not have safety features active. Some providers are part of family friendly WiFi schemes with filters to block inappropriate content. Look out for friendly WiFi symbols like Mumsnet Family Friendly WiFi and RDI Friendly WiFi symbols when you’re out and about.

**Have an agreement**

Agree and set boundaries with them or have a [family contract](https://www.fosi.org/good-digital-parenting/family-online-safety-contract/) for their internet use, including when and where they can use portable devices and for how long, before they get used to doing their own thing.

**Start discussions about social networking early**

Talk to children about the benefits and risks of social networking before they join any age appropriate sites. Let them know that anything they upload, email or message could stay around forever online.

**Keep private information private**

If your child (over 13 years old) does have a social networking profile, teach them to block or ignore people and how to set strict privacy settings. Request that you or someone you both trust becomes their ‘friend’ or ‘follower’ to check that conversations and posts are appropriate.

**Check age ratings**

The age ratings that come with games, apps, films and social networks are a good guide to whether they’re suitable for your child.