NETWORK SECURITY IN THE HOME

Current as of November 2020

It is important to manage your child's screen time at home.

This document will provide basic information on three practical methods to manage digital devices at home and some simple advice for supervision and healthy use in the home.

OUTLINE

Our students are learning to become digital citizens and will naturally be curious about the wider internet and communications technology.

At Leeming Primary School we endeavour to be ahead of the curve on digital literacy and cyber safety however we recognise that parental protection and supervision is key to managing a variety of concerns such as inappropriate online content, digital communication, information security and bad habits or 'digital hygiene' outside of school hours.

It is important to note that many online security measures only monitor internet browsing using client software like Safari or Chrome. This does not regulate other activities like direct messaging, airdrops and email clients which can also be used improperly. In our Apple ecosystem, Screen Time goes some way towards managing this, but at the end of the day supervision, communication and education can be more effective than access restrictions.

The Australian government has made these resources available for further reading.

E-safety for parents (www.esafety.gov.au/parents)

and Taming Technology (www.esafety.gov.au/parents/skills-advice/taming-technology).

Beacon (https://beacon.telethonkids.org.au/) is a service provided by Telethon and Bankwest to keep carers up to date with changing trends in Cyber Safety.

ABOUT SCHOOL NETWORKS

It is important to note that while at school, students are protected under a network wide Department of Education content filter and will not have access to unsecured internet connections including mobile data.

This network protection does not extend outside of schools. We recommend that children should always be supervised while using their devices and that parents and family familiarise themselves with safety features.

A NOTE ON MOBILE DATA

Students are not permitted to use mobile or data enabled devices on school grounds. This includes Wi-Fi and camera-enabled smart devices including smart watches and iPads with mobile data enabled.

Please consult your classroom teacher for the most up-to-date procedures for this if you have any concerns.

Please note that depending on your security solution, a mobile hotspot or data plan can be used to circumvent some security features and browsing protection.

The following paragraphs are outlines of four common strategies used to keep children safe online. These include a list of the most useful features and the 'pros and cons' of each to help you decide what is right for you.

- **Apple Screen Time**
- **Browser Content Filtering**
- **IP Traffic Filtering**
- **Paid Services**
- **Glossary of Terms**

APPLE SCREEN TIME

Screen Time is Apple's bundled control system that offers a wide array of options and solutions from tracking your own social media usage to securing and controlling linked device.

It can be accessed through Settings on iPad or System Preferences on MacOS.

Inside are options for Downtime, App and Communication Limits, Allowed Apps and Content & Privacy. The following are some of the recommended settings for students at Leeming Primary.

-SCREEN TIME: Enabling Screen Time, you can start to build your profile to help customise your child's access and privacy. It is recommended that you set a passcode on Screen Time so other users cannot alter your settings.

In 'Options' it is possible to share settings across a 'family' of devices and accounts. If you plan to use this feature it is advisable to have a named account for each user as by default the system account has Administrator Privileges.

-DOWNTIME: Downtime allows you to schedule control features to turn on and off depending on time and context. During Term time, we recommend that downtime is scheduled to limit access while students are outside of school- 3:30 each afternoon until 8:30 the next day Monday through Friday. This allows you to apply your family settings while at home without limiting their use at school under our network protection and supervision.

> *- NOTE:* If your home requirements are minimal, the Guided Access can be found in iPad settings. This allows you to lock the device into one app with an optional time limit and an override passcode. This is often referred to as Kiosk mode and is useful for younger children.

-ALWAYS ALLOW: For the limited set of educational apps you may like to allow during home time you can set these to "always allow". For other activities you may override the downtime using your secret PIN number on request allowing flexibility and supervision on a case-by-case basis.

Similarly, you can limit communication on apple services to only white-listed contacts (Extended family and close friends only on, for instance)

-LIMITED APP TIME: You can set "App limits", meaning a timer on the amount of use an app can have in a set period by name (Like: Discord, 1 hour per day) or by category (Like: 'social media' 4 hours per week) . This can be extended or overridden with a password when required. Please note that this timer continues to count if the device is left open and inactive. You can find graphical breakdowns of app usage in the Screen Time menu so you can check for anomalies at a glance and identify unhealthy habits.

CONTENT AND PRIVACY- This area allows you to activate web content filters that try to block out specified content such as "limit adult websites" or "allowed websites only". You can also add and remove web addresses from this list manually. This is a good first step.

While this filter is highly recommended, it is not foolproof and is not consistent on browsers outside of Apple's Safari App. It is recommended that other browsers are blocked during downtime at home. On some occasions popular content does not run on Safari and at your discretion children can ask for the security pin to override the setting temporarily and under supervision to use other browsers.

For Android devices and some google applications on IOS the Family Link service is available offering similar features to Screen Time.

BROWSER BASED CONTENT FILTERING

Please ensure that all browsers have the default safe-search or similar enabled in settings, this is a standard feature.

There are many child browsing plugins available for major browsers, due to the wide array of options and regular updates we cannot ensure our advice remains current.

Browsers that are designed for children include *Kiddle.com* and *Safe Search Kids* and could be used as a home alternative to regular browsers like Firefox, Safari and Chrome.

Please keep an eye on the plug-ins and web apps your child is installing as many of them are borderline malware and most of them are very distracting.

IP FILTERING (DIY and PURCHASE)

There are a number of sources offering IP filters. These are special DNS based filters that use constantly updated lists of inappropriate sites and run at the router level, filtering content before it reaches any devices on the network. This will only work when children are on your home network and depending on configuration will filter traffic on every connected device.

CleanBrowsing and *OpenDNS* are examples of free filtering services that you can apply to your router settings, offering Family, Adult and Security filters if you are comfortable editing your router settings.

Check your router and with your internet provider, some offer built in parental control which can be activated with a click.

There are paid services for this and some package deals that include pre-configured hardware, see next section.

SUBSCRIPTIONS AND PAID SERVICES

Several providers offer paid subscription services for content and device management, others offer specialised Wi-Fi extenders and other hardware-based solutions designed to simplify the task of filtering and supervising internet in the home. These are usually IP filters.

Some popular examples are:

Familyzone.com

Qustodio.com

Circle and Disney Circle.

Clean Router.

Glossary:

Blacklist and Whitelist: These are ever evolving lists of web addresses and domains that try to keep up with the ever-changing number of locations that are tagged as blacklisted- adult, malicious or unsafe. A whitelist is a list of locations explicitly regarded as acceptable. These sites can be blocked or filtered. This is a difficult prospect and therefore is regarded as precaution but is far from fool-proof. Using an exclusive whitelist will typically cripple any kind of search engine or online research.

Browser: Unlike the operating system, a browser is simply an installed app or program that facilitates access to the internet and search engines like Google. While a lot of security focuses on online activity through browsers it is important to remember that other avenues like direct messaging, shared files and email can operate outside of the browser.

Client, as in email or browser Client: A Client is an installed piece of software that acts as the portal or access point to a service (usually an online communication network or a service that exists outside of the personal device). All the different browser clients such as Chrome, Safari, Firefox are simply programs to access and display internet content, which its-self does not belong to any one company. An addon that blocks content on a Safari client will not always block that same content on other clients like Chrome or Firefox and this can become a loophole.

Data or Mobile Data: Using the mobile network or mobile data as a temporary internet provider can be handy, but just like using public access wi-fi it can be a risky activity. Children with access to a mobile phone or an alternative internet network can sometimes use this to try and circumvent network-based restrictions or share information inappropriately.

Data Security: Storing sensitive information and files securely or limiting their availability. Loose memory sticks and network shared files are common; however, it extends to phishing or trying to trick passwords and personal information out of people in conversation or over sharing on social media or email.

IOS and Android: IOS refers to the software or Operating System on Apple devices. Android is a common Operating System on other portable devices and is often the underlying software of branded devices like Samsung and and Google devices.

IP and DNS: Internet Protocol and Domain Name System are shorthand for the traffic and addresses online. An IP filter is filtering the data coming in and the DNS is setting boundaries and permissions for the local 'domain'.

Network: A network is typically the locally accessible source of internet and communications technology. While typically this is a Wifi and Ethernet connection consider that at times this will include offline and local communications like AirDrop, Servers, Bluetooth, NFC and mobile communications.

ICT: Information Communications Technology, a catch-all term for digital information and networking technologies right through to robotics and programming.

Malware: Some software is not overtly dangerous or malicious, but is counter-productive, distracting or slows down the computer. This is called malware. Browser toolbars, desktop pets, flashy plug-ins and mouse-pointer animations are examples of this. They often gather data, produce pop-ups and adverts and can be hard to remove.

Router: The router is the hub device that directs all incoming and outgoing internet traffic on the local network and most houses use one. Some forms of security rely on this 'bottleneck' to regulate traffic (See IP Filtering).

Security: Online safety and security is many layered. Not all vulnerabilities are online or on the web- bullying, information theft and scams can take place via internet browsers, unregulated games platforms, messenger clients/email, and even USB and AirDrop transfer can be used improperly. Word of mouth, proxy sites and tunnelling services and other workarounds are common, and the best defence is common sense and supervision.