Summer Hill Public School

Student Use of Digital Devices and Online Services Procedure

Purpose

This procedure guides student use of digital devices and online services at our school.

Our school acknowledges the educational value of digital devices and online services in supporting and enhancing educational outcomes and student wellbeing. We also recognise they may cause harm if used inappropriately and that we need to support our students to use them in safe, responsible and respectful ways.

Summer Hill Public School has extensive access to computers, including two tech spaces, which include access to desktop computers, laptops and filming equipment. The digital technology provided by the school includes: 8 iPads per class K-2; 3 iPads and 6 laptops per class grades 3 - 6; 14 iPads for use by the Music and Drama classrooms; a bank of 14 iPads and 14 laptops in our school Library and the Learning and Support Teacher (LaST) has access to 4 iPads and 2 desktop computers. All devices use wireless connection which can be used across the school. Each classroom has access to interactive white boards (IWB) or equivalent (promethean panels) and desktop computers with broadband internet access. Bring Your Own Device (BYOD) is available to students in Year 3-6.

The school also has access to a variety of digital learning kits that enhance student learning, engagement and confidence in a modern world. The IT support is provided to our school by both the Department and an external provider which ensures prompt response to all technical issues.

Scope

This procedure provides a consistent framework for the safe, responsible and respectful use of digital devices and online services by students in our school. It sets out the shared responsibilities of school staff, students and parents and carers. It also provides a framework to manage potential risks to student safety and wellbeing.

This procedure covers student use of digital devices and online services in school-related settings, including on school grounds, at school-related activities and outside of school where there is a clear and close connection between the school and the conduct of students. This procedure covers the use of school-provided and personal digital devices and all online services.

Our School’s Approach

At Summer Hill Public school we use a variety of software and hardware to deliver authentic learning experiences. Students are able to use devices during class for educational purposes when instructed by the teacher. Devices are not permitted to be used at recess, lunch, before and after school unless: use is approved by a teacher or principal for an educational purpose; an exemption applies; or, use of digital devices and online services is required medical reasons or for reasonable adjustments made as part of a student’s personalised learning and support plan. When attending excursions and camps use of devices must be approved by the principal.

Students in Year 3 – 6 are able to bring their own device to school to use for educational purposes. These will be signed into their classroom in an identified safe storage spot for use when specified by the teacher. All classrooms are locked when vacated to ensure all devices are safe. Students are responsible for the safe use of their devices by: ensuring they are handled carefully; not loaned to peers; and, used in the classroom designated area.

Mobile phones are a major distraction for students and they present major risks with regard to theft, vandalism and harassment from other students. Students may hand phones in to the school office on arrival and collect them at 3.00pm. Where a student chooses not to hand in their phone to the office the phone must be switched off and kept in their bag. The school will not take responsibility for such equipment if a student brings a mobile phone or electronic device to school.

Note: Recognising some students will bring digital devices to schools, whether for personal or educational use, schools should describe their approach to managing the storage of devices. Although schools are under no obligation to provide storage facilities, it is recommended that schools outline their approach (reference).

Exemptions

Teachers will review possible exemptions for students at their stage team meetings with advice from the Principal and Assistant Principals.

Use of digital devices must be permitted at recess, lunch and during class-time if a student requires a digital device or online service for medical reasons or for reasonable adjustments made as part of their individual education plan. These are not considered exemptions.

Note: Exemptions to any part of this procedure may apply for some students in some circumstances. Parents and carers can request an exemption and these will be considered on a case-by-case basis and granted when required by law or at the principal's discretion.

Consequences for inappropriate use

When a student does not follow the school's policy for online learning Summer Hill Public School uses a three teared flowchart to respond to the issue these are as follows

Minor:

- Teacher will remove device privilege for the teacher's determined length of time. This is based on previous repeat behaviours.
    - *Use of classroom device without teachers permission.*

Intermediate:

- Stage Assistant Principal will be informed. Student portal password changed and/or removal of device for a designated length of time. If the student has access to BYOD parents will be advised to keep this device home for the discussed period. A reminder of the students online policy will be sent home.
    - *Use of another students account without their permission;*
    - *Use to software that has not been assigned by the teacher; gaming platforms; website that are not connected to the lesson*
    - *Use of personal device inside the school grounds without teacher permission.*

Major:

- The assistant and / or deputy principal will be informed and further decisions will be made based on the principals review. Parents will be informed by the assistant or deputy principal.
- Work with the department and the Office of the eSafety Commissioner (if necessary) to resolve cases of serious online bullying and image-based abuse
    - *Use of email, Google Classroom or any other collaborative website to make inappropriate comments that are related to cyberbullying;*
    - *Use of camera features to photograph and post pictures of another student without their consent;*
    - *Use of personal devices at school to create and post videos to inappropriate websites.*

Contact between students and parents and carers during the school day

Should a student need to contact their parent / carer during the school day, they must:

- approach the administration office and ask for permission to use the school's phone;
- During school hours, parents and carers are expected to only contact their children via the school office.

Responsibilities and obligations

Summer Hill Learning Community shares the responsibility to maintain safe behaviour when using all school and personal devices. The following is a list of the expectations of our community.

For students

- Be safe, responsible and respectful users of digital devices and online services, and support their peers to be the same.
- Respect and follow school rules and procedures and the decisions made by staff, knowing that other schools may have different arrangements.
- Communicate respectfully and collaboratively with peers, school staff and the school community and behave in the ways described in the Department of Educations' online policy and our schools' Student behavior Guidelines.

For parents and carers

- Recognise the role they play in educating their children and modelling the behaviours that underpin the safe, responsible and respectful use of digital devices and online services.
- Support implementation of the school procedure, including its approach to resolving issues.
- Take responsibility for their child's use of digital devices and online services at home such as use of online services with age and content restrictions.
- Communicate with school staff and the school community respectfully and collaboratively as outlined in the 2018 School Community Charter.
- Switch off or put their digital devices on silent when at official school functions, during meetings and when assisting in the classroom.
- Provide digital devices that meet school specifications where a school is participating in a bring your own device program and complete any related paperwork.

For the principal and teachers

1. Deliver learning experiences that encourage safe, responsible and respectful use of digital devices and online services. This includes:
    - Establishing agreed classroom expectations for using digital devices and online services, in line with this procedure and departmental policy.
    - Identifying strategies to ensure that all students are able to engage in classroom activities including strategies to accommodate students without a digital device.
    - Reading and abiding by the Terms of Service for any online services they use in teaching, including those limiting use by age.
    - Educating students about online privacy, intellectual property, copyright, digital literacy and other online safety related issues.
2. Model appropriate use of digital devices and online services in line with departmental policy.
3. Respond to and report any breaches and incidents of inappropriate use of digital devices and online services as required by school procedures, departmental policy and any statutory and regulatory requirements. This includes:
    - Reporting the creation, possession or distribution of indecent or offensive material to the Incident Support and Report hotline as required by the Incident Notification and Response Policy and Procedures and consider any mandatory reporting requirements.
    - Working with the department and the Office of the eSafety Commissioner (if necessary) to resolve cases of serious online bullying and image-based abuse.
    - Following the school's Student Behavior Guidelines when responding to any incident of inappropriate student behaviour relating to the use of digital devices or online services.
4. If feasible and particularly as issues emerge, support parents and carers to understand strategies that promote their children's safe, responsible and respectful use of digital devices and online services.
5. Participate in professional development related to appropriate use of digital devices and online services.

For non-teaching staff, volunteers and contractors

- Be aware of the department’s policy, this procedure and act in line with the conduct described.
- Report any inappropriate use of digital devices and online services to the principal, school executive or school staff they are working with.

External learning platform used by Summer Hill Public School include:

Before using external learning platforms, the school uses the risk assessment tool, provided by the eSafety Commissioner. This tool assesses risks and benefits of any new online platforms or technologies. (See Appendix 3)

Annually parents and guardians are updated on the learning platforms used by classroom teachers. The websites recommended by the Department of Education that our school currently uses include the following:-

Class Dojo	Google Classroom / G Suite	Google Earth
Weebly	Kahoot	Typing Club / Typing DanceMat / BBC Typing Website
CanvaEdu	Reading Eggs	Reading Eggs/ Soundwaves/ Mathletics
Soundwaves	Mathletics	Tinker cad
Flip Grid	Read Theory	Google CS
Tinkercad	Scratch	Code.org

Communicating this procedure to the school community

Students will be informed about this procedure through their classroom teacher.

Parents and carers will be advised via the school newsletter. This procedure can be accessed electronically via the school’s website and in hardcopy at the school’s administration office.

Complaints

If a student, parent or carer has a complaint under this procedure, they should first follow our community guide for contacting our school. If the issue cannot be resolved, please refer to the department’s guide for students/ parents/ carers about making a complaint about our schools.

Review

The principal or delegated staff will review this procedure annually.

Appendix 1: Key terms

Bring your own device is an optional program where parents and carers can provide personal digital devices for use at school. Any decision to adopt a bring your own device program is made by the principal in consultation with a school community. All digital devices used in schools are covered by the *Student Use of Digital Devices and Online Services* policy. Schools retain discretion to determine the specifications of personal devices to be used at school.

Digital citizenship refers to the skills and knowledge a person needs to effectively use digital technologies in a positive way so they can participate in society, communicate with others, and create and consume digital content.

Digital devices are electronic devices that can receive, store, process and share digital information and connect to applications (apps), websites and other online services. They include desktop computers, laptops, tablets, smartwatches, smartphones and other devices.

Digital literacy is the set of social, emotional and technological skills and competencies that people need to understand to use digital devices and online services, and to expand their opportunities for education, employment and social participation, including entertainment.

Educational purpose is any use approved by school staff that supports student learning, wellbeing and educational outcomes.

General capabilities are the broad collection of knowledge, skills, behaviours and dispositions described within the Australian curriculum and NSW syllabus.

Online bullying involves using technology such as the internet or mobile devices to bully someone. Bullying behaviour has three key features. It involves the intentional misuse of power in a relationship. It is ongoing and repeated, and it involves behaviours that can cause harm. Bullying behaviour can also involve intimidation, victimisation and harassment, including that based on sex, race, religion, disability, or sexual orientation.

Online safety is the safe, responsible and respectful use of digital media, devices, other technology and online services.

Online services are any software, website or application that can gather, process or communicate information. This includes digital classrooms, chat and messaging, online games, virtual reality, social media and other online spaces.

Reasonable adjustment is a measure or action taken to assist a student with disability to participate in education on the same basis as other students.

School-related settings include school grounds, school-related activities and outside of school where there is a clear and close connection between the school and the conduct of students. This connection may exist in situations where: there is discussion about school taking place outside of school hours; a student is wearing their school uniform but is not on school premises; a relationship between parties commenced at school; students are online in digital classrooms; and where online contact has flow on consequences at school and duty of care requires the school to respond once an incident is reported.

School staff refers to school personnel who have some level of responsibility for implementing policy and the school digital devices and online service procedure. This includes principals, senior staff, teachers, non-teaching staff, school administrative staff, volunteers and contracted staff engaged by schools.

Appendix 2: What is safe, responsible and respectful student behaviour?

Be SAFE

- Protect your personal information, including your name, address, school, email address, telephone number, pictures of you and other personal details.
- Only use your own usernames and passwords, and never share them with others.
- Ask a teacher or other responsible adult for help if anyone online asks for your personal information, wants to meet you or offers you money or gifts.
- Let a teacher or other responsible adult know immediately if you find anything online that is suspicious, harmful, inappropriate or makes you uncomfortable.
- Never hack, disable or bypass any hardware or software security, including any virus protection, spam and filter settings.

Be RESPONSIBLE

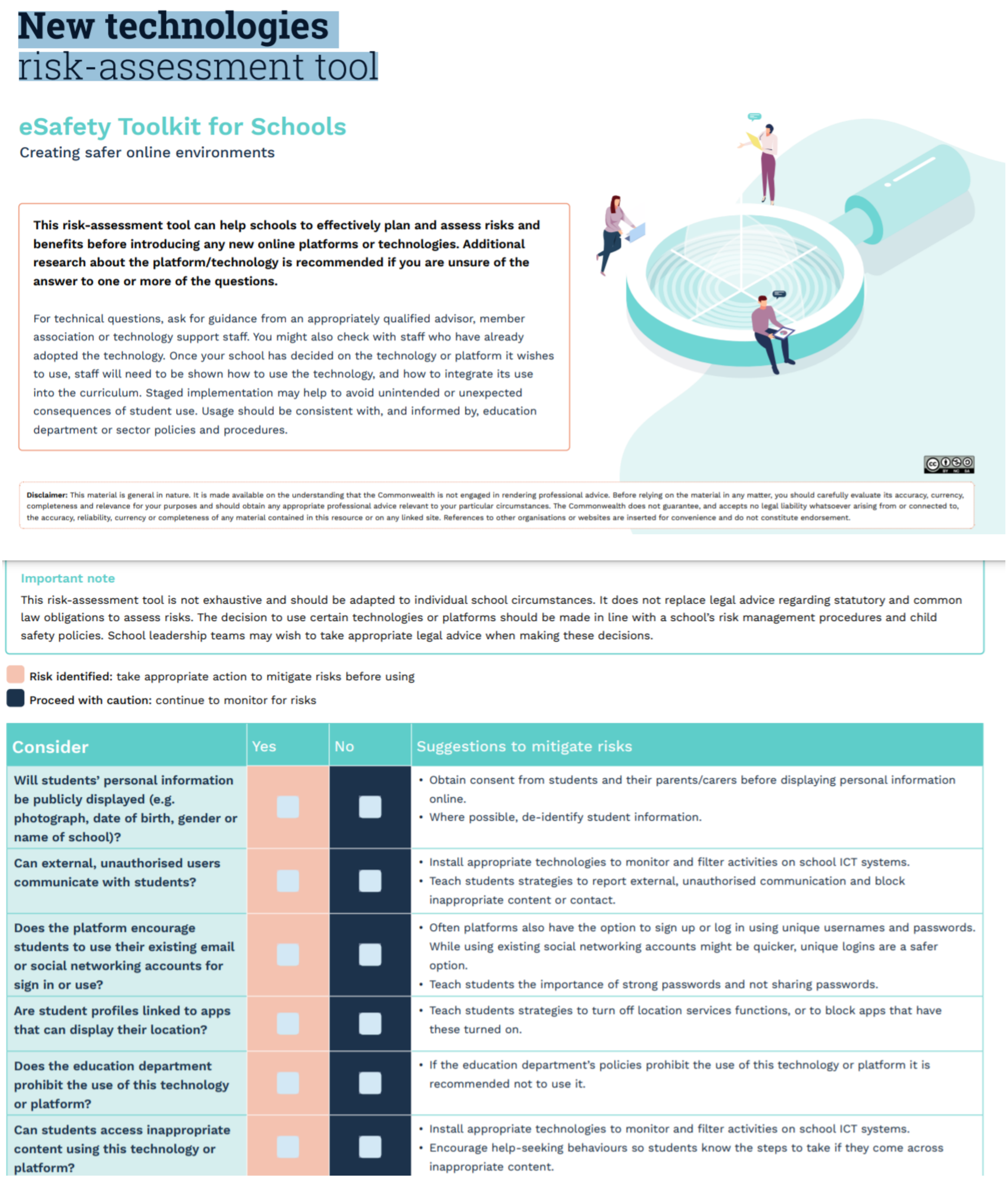
- Follow all school rules and instructions from school staff, including when using digital devices and online services.
- Take care with the digital devices you use.
  - Make sure the devices you bring to school are fully charged each day and are stored appropriately when not in use.
  - Understand that you and your parents and carers are responsible for any repairs or IT support your personal devices might need.
  - Make sure the devices you bring to school have the latest software installed.
  - Take care with the school-owned devices you share with others, so that other people can use them after you.
- Use online services in responsible and age-appropriate ways.
  - Only use online services in the ways agreed to with your teacher.
  - Only access appropriate content and websites, including when using the school's filtered network and personal, unfiltered networks.
  - Do not use online services to buy or sell things online or to do anything that breaks the law
- Understand that everything done on the school's network is monitored and can be used in investigations, court proceedings or for other legal reasons.

Be RESPECTFUL

- Respect and protect the privacy, safety and wellbeing of others.
- Do not share anyone else's personal information.
- Get permission before you take a photo or video of someone, including from the person and from a teacher.
- Do not harass or bully other students, school staff or anyone, this includes cyberbullying using a digital device or online service.
- Do not send or share messages or content that could cause harm, including things that might be:
  - inappropriate, offensive or abusive;
  - upsetting or embarrassing to another person or group;
  - considered bullying;
  - private or confidential; and/or
  - a virus or other harmful software.

Appendix 3: New technologies risk-assessment tool

https://tinyurl.com/cj2ww462 QR CODE:



New technologies risk-assessment tool

eSafety Toolkit for Schools

Creating safer online environments

This risk-assessment tool can help schools to effectively plan and assess risks and benefits before introducing any new online platforms or technologies. Additional research about the platform/technology is recommended if you are unsure of the answer to one or more of the questions.

For technical questions, ask for guidance from an appropriately qualified advisor, member association or technology support staff. You might also check with staff who have already adopted the technology. Once your school has decided on the technology or platform it wishes to use, staff will need to be shown how to use the technology, and how to integrate its use into the curriculum. Staged implementation may help to avoid unintended or unexpected consequences of student use. Usage should be consistent with, and informed by, education department or sector policies and procedures.

Disclaimer: This material is general in nature. It is made available on the understanding that the Commonwealth is not engaged in rendering professional advice. Before relying on the material in any matter, you should carefully evaluate its accuracy, currency, completeness and relevance for your purposes and should obtain any appropriate professional advice relevant to your particular circumstances. The Commonwealth does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained in this resource or on any linked site. References to other organisations or websites are inserted for convenience and do not constitute endorsement.

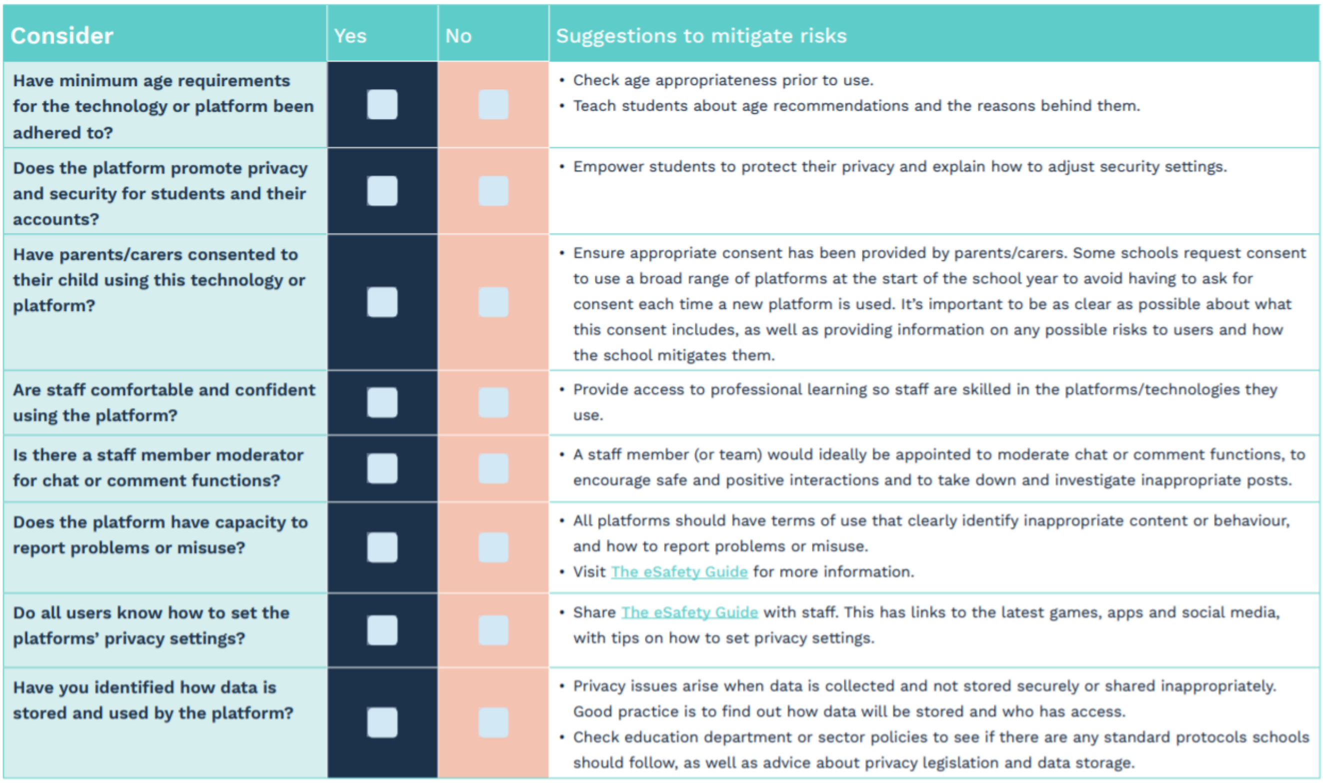
Important note

This risk-assessment tool is not exhaustive and should be adapted to individual school circumstances. It does not replace legal advice regarding statutory and common law obligations to assess risks. The decision to use certain technologies or platforms should be made in line with a school's risk management procedures and child safety policies. School leadership teams may wish to take appropriate legal advice when making these decisions.

🟥 **Risk identified:** take appropriate action to mitigate risks before using

■ **Proceed with caution:** continue to monitor for risks

Consider	Yes	No	Suggestions to mitigate risks
Will students' personal information be publicly displayed (e.g. photograph, date of birth, gender or name of school)?	☐	☐	• Obtain consent from students and their parents/carers before displaying personal information online. • Where possible, de-identify student information.
Can external, unauthorised users communicate with students?	☐	☐	• Install appropriate technologies to monitor and filter activities on school ICT systems. • Teach students strategies to report external, unauthorised communication and block inappropriate content or contact.
Does the platform encourage students to use their existing email or social networking accounts for sign in or use?	☐	☐	• Often platforms also have the option to sign up or log in using unique usernames and passwords. While using existing social networking accounts might be quicker, unique logins are a safer option. • Teach students the importance of strong passwords and not sharing passwords.
Are student profiles linked to apps that can display their location?	☐	☐	• Teach students strategies to turn off location services functions, or to block apps that have these turned on.
Does the education department prohibit the use of this technology or platform?	☐	☐	• If the education department's policies prohibit the use of this technology or platform it is recommended not to use it.
Can students access inappropriate content using this technology or platform?	☐	☐	• Install appropriate technologies to monitor and filter activities on school ICT systems. • Encourage help-seeking behaviours so students know the steps to take if they come across inappropriate content.



Consider	Yes	No	Suggestions to mitigate risks
Have minimum age requirements for the technology or platform been adhered to?	☐	☐	• Check age appropriateness prior to use. • Teach students about age recommendations and the reasons behind them.
Does the platform promote privacy and security for students and their accounts?	☐	☐	• Empower students to protect their privacy and explain how to adjust security settings.
Have parents/carers consented to their child using this technology or platform?	☐	☐	• Ensure appropriate consent has been provided by parents/carers. Some schools request consent to use a broad range of platforms at the start of the school year to avoid having to ask for consent each time a new platform is used. It's important to be as clear as possible about what this consent includes, as well as providing information on any possible risks to users and how the school mitigates them.
Are staff comfortable and confident using the platform?	☐	☐	• Provide access to professional learning so staff are skilled in the platforms/technologies they use.
Is there a staff member moderator for chat or comment functions?	☐	☐	• A staff member (or team) would ideally be appointed to moderate chat or comment functions, to encourage safe and positive interactions and to take down and investigate inappropriate posts.
Does the platform have capacity to report problems or misuse?	☐	☐	• All platforms should have terms of use that clearly identify inappropriate content or behaviour, and how to report problems or misuse. • Visit The eSafety Guide for more information.
Do all users know how to set the platforms' privacy settings?	☐	☐	• Share The eSafety Guide with staff. This has links to the latest games, apps and social media, with tips on how to set privacy settings.
Have you identified how data is stored and used by the platform?	☐	☐	• Privacy issues arise when data is collected and not stored securely or shared inappropriately. Good practice is to find out how data will be stored and who has access. • Check education department or sector policies to see if there are any standard protocols schools should follow, as well as advice about privacy legislation and data storage.

Appendix 4: Specifications required for bring your own devices

Wireless connectivity:

The Department of Education’s secured wireless and filtered Internet.

Operating system:

Devices must be able to run the current version of it's operating system (e.g Windows devices must be running current versions of Windows 10, Mac devices should be running later versions of Mac OS). Chrome operating system should have at least v72 for optimal results. This will ensure that security updates are up to date and not going to put both the student's device and other devices on the network at risk.

Software and apps:

The device must have antivirus installed and up to date, however, the operating systems have built in antivirus which is sufficient for the department.

No apps or software is required as student work will be on web based platforms such as GoogleSuite (this includes Google; classroom; Documents; Slides; Sheets). Students also have access to email and OneDrive via their DET PORTAL.

Battery life:

All devices must be fully charged upon arrival at school. Students will be unable to charge their device at school. Make sure the battery lasts a 6-hour school day Modern processors devices can help stretch battery life further.

Memory and RAM:

Minimum of 4GB - Aim for at least 8GB for most general-use laptops. Cloud Based storage is used for students' work.

Ergonomics:

It is recommended that a device with a 9-14 inch screen size is ideal for ease of use and portability however this is not a requirement. Ensure that the device is light enough for transport to and from school (recommenced no heavier than 1.5kg)

Accessories required:

Headphones

Other considerations:

A protective case is strongly recommended for device transport to and from school. Aim for a l