

# **Caulfield South Primary School**

**C.S.P.S.**

**Policy #1.8**

## **Information and Communications Technology (ICT) Policy**

### **RATIONALE**

Caulfield South Primary School (C.S.P.S.) supports the embedded use of Information and Communication Technologies for students and staff to research, publish and communicate in accordance with the Department of Education and Training's *Using Digital Technology to Support Learning and Teaching Policy* (Appendix 1). Usage of eLearning and ICT tools at C.S.P.S. is directed by their effectiveness to support student learning as outlined in the *AusVELS* and International Baccalaureate Primary Years Programme.

eLearning provides support and enhances student learning in an ever-changing, global community. It is flexible, personalised and develops 21st Century competencies by being embedded into the core principles and practices of teaching and learning at C.S.P.S.

It is commonly understood that a student-centric approach to education is most closely aligned with academic success. When students have a personal device they are able to use it as a tool integrated into all areas of the curriculum. Teachers are able to unite knowledge and creativity in closely integrated learning experiences that maximise student engagement and learning. A school setting where students have a device solely for their use, as the C.S.P.S. Chromebook program provides, is described as 1:1.

Through a variety of web-based applications, teachers can empower students to access learning tasks where they are able to work at their own pace, individually and collaboratively, to create, present and share work with their classmates, school and the world.

By having their own device, our students can remain signed into apps, store their work and customise their devices to suit their needs. Teachers can assume immediate access to technology and closely integrate it into learning tasks. They can innovate the curriculum, designing learning tasks that are rich, engaging and focused on the needs of individual students. Students can access their work everywhere, at home, in other classes, on excursions; every moment can become a learning opportunity.

## **DEFINITIONS OF TERMS USED IN THESE GUIDELINES**

**'Google Apps for Education' (GAPE)** refers to a suite of web-based applications to which students at Caulfield South Primary School have access, as part of the secure @caulfieldsouthps domain. These can include 'Docs', 'Sheets', 'Slides', 'Mail', 'Calendar', 'Drive', and 'Classroom'.

**'Authorised Device'** refers to the selected model available for purchase through the CSPS Chromebook program.

**'Chromebook'** refers to the Lenovo e11 Chromebook which is the selected device for the C.S.P.S Chromebook Program. A Chromebook is a computer that runs the "Chrome" operating system.

**'Authorised user'** means a person who has signed the eSmart Agreement (or has had it signed on their behalf by a parent) and is authorised by the school to use school ICT.

**'eSmart'** refers to the name of the cybersafety guidelines that are followed at Caulfield South Primary School to promote the safe, responsible and ethical use of ICT.

**'ICT'** stands for 'Information and Communication Technologies' and includes network facilities, communication technologies, eLearning tools and ICT equipment/devices.

**'Network facilities'** includes, but is not limited to, the Google Apps for Education suite of tools and Internet access to files, web sites and digital resources via the school network.

**'Communication technologies'** includes, but is not limited to, communication made using ICT equipment/devices such as Internet, Google Apps for Education, email, instant messaging, online discussions/surveys and mobile phone activities and related applications.

**'eLearning'** refers to the use of ICT for educational purposes.

**'ICT equipment/devices'** include, but are not limited to, computers (such as Chromebooks, desktops, laptops, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, and any other, similar technologies as they come into use.

**'Agreement'** refers to the C.S.P.S ICT Acceptable Use Agreement which will be reviewed annually.

**'School-related activity'** includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.

**'School ICT'** refers to any ICT owned or operated by the school including, but not limited to, network infrastructure, computers, cameras, tablet devices, Google Apps for Education domain.

**'Inappropriate material'** includes, but is not limited to, pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be detrimental to the well-being of students or unsuitable to a school environment.

**'Unacceptable student conduct'** includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft or copyright infringement.

**'Educational purposes'** means activities that are directly linked to curriculum-related learning.

**'Personal electronic devices'** includes, but is not limited to, handheld gaming consoles (including but not limited to Nintendo DS, PSP Wii U), MP3 players (including but not limited to iPod, iPod Touch), e-readers (including but not limited to Kindle, Kobo) other Internet and 3G accessible devices, and any other similar such devices as they come into use.

**'Screen Time'** is the time you spend watching TV or DVDs, using the computer, playing video or hand-held computer games, and using a mobile phone.

## **GUIDELINES**

### **AUTHORISED USAGE AND ESMART AGREEMENT**

C.S.P.S. will use the '*eSmart Schools*' framework to guide the school in maintaining a smart, safe and responsible use of information and communications technology to support student learning. The '*eSmart Schools*' program was developed by RMIT University in consultation with cybersafety, bullying, education and industry experts from across Australia. In 2010, eSmart was piloted in 159 schools across Australia with funding from the Commonwealth Department of Education, Employment and Workplace Relations (DEEWR).

As C.S.P.S. provides network access, the contents of the school ICT system, including email messages, remain the property of the DET. C.S.P.S. has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

All C.S.P.S. students, whether or not they make use of network facilities and communication technologies on school-owned or personal ICT equipment/devices, will be issued with this Agreement. This document should be read carefully with the acknowledgement page signed and returned to the student's class teacher by the date specified.

The school's ICT, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the acknowledgement page of this Agreement has been signed and returned to the student's class teacher. Signed Agreements will be filed in a secure place.

The school encourages anyone with a query about these guidelines or the Agreement to contact your child’s class teacher in the first instance.

**INTENDED USE:**

This ICT Policy has been developed to inform Caulfield South Primary School community (students, staff, parents and administration) of the roles and responsibilities and expectations in order to maintain responsible, safe and effective school-based ICT programs including a 1:1 Chromebook program.

**EQUITY AND ACCESS**

Caulfield South Primary School understands that eLearning programs may present a financial burden to some families. As part of its responsibilities, the school has developed a process where it will provide a comparable device for non-participating student use during class time. On occasions these devices may need to be shared with other students within the class.

Year 6 students will be able to borrow a school-owned device for the 2016 academic year only. This will be facilitated through the student and parent signing the C.S.P.S *Permission to Borrow ICT* form (Appendix 9).

**RIGHTS AND RESPONSIBILITIES OF C.S.P.S. STAKEHOLDERS**

**SCHOOL**

Right	Responsibility
<ol style="list-style-type: none"> <li>1. To access and review the accounts of students.</li> <li>2. To suspend or delete a student account where deemed appropriate.</li> </ol>	<ol style="list-style-type: none"> <li>1. To ensure access to ICT for all students.</li> <li>2. To deliver ICT programs consistent with AusVELS and the PYP framework.</li> <li>3. To provide a safe physical and digital environment for our students to learn and grow.</li> <li>4. To provide technical limitations that prevent access to damaging content.</li> <li>5. To provide education to support students navigating digital content.</li> <li>6. To manage the @caulfieldsouthps domain with the appropriate level of security.</li> <li>7. To ensure students and parents are aware of the legal ramifications of inappropriate digital interactions.</li> </ol>

	8. To ensure student privacy is maintained in accordance with the school's Privacy Policy.
--	--

## STUDENTS

Right	Responsibility
<ol style="list-style-type: none"> <li>1. To be taught using contemporary ICT through programs consistent with AusVELS and the PYP framework.</li> <li>2. To be supported to know how to navigate and evaluate online content and situations.</li> <li>3. to have access to contemporary resources.</li> <li>4. To know their legal obligations in regard to practices.</li> <li>5. To be taught the correct actions to take when encountering inappropriate material or unacceptable student conduct online.</li> </ol>	<ol style="list-style-type: none"> <li>1. To abide by the expectations that are negotiated in the <i>C.S.P.S. ICT Acceptable Use</i> document (Appendix 10).</li> <li>2. To report inappropriate behaviour following the guidelines laid out in the <i>C.S.P.S. Incident Response</i> flow chart (Appendix 11 ).</li> <li>3. To look after their individual devices.</li> <li>4. To abide by the negotiated Essential Agreements for each year level.</li> </ol>

## PARENTS

Right	Responsibility
<ol style="list-style-type: none"> <li>1. To be informed about the student's expected behaviour while online.</li> <li>2. To understand the security measures put in place.</li> <li>3. To understand the intended purpose of the program.</li> <li>4. To be aware of the process for reporting incidents of inappropriate online behaviour.</li> </ol>	<ol style="list-style-type: none"> <li>1. To be an active participant in their child/ren's digital practices.</li> <li>2. To attend information and education sessions provided by the school.</li> <li>3. To model appropriate online behaviour.</li> <li>4. To ensure that age restrictions for home use of social media applications are upheld.</li> </ol>

## **IMPLEMENTATION**

- C.S.P.S. will appoint an ICT coordinator to manage an eLearning team of teachers to coordinate the ICT programs in the school.
- The use of the school's network is subject to the Agreement (appendix 2). These procedures are intended to be consistent with other school policies including the *Student Engagement & Privacy Policy*.
- Where there is a reasonable belief that illegal activity may have occurred the Principal will report the suspected illegal activity to the police.
- Obtaining unauthorised access to electronic files of others, or to email electronic communications of others, is not permitted and may constitute a criminal offence under the Crimes Act 1958 (Vic) or other legislation.
- C.S.P.S. ICT systems must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or DET liability. The audience that views an electronic message may be unexpected and widespread.
- The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and downloaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or C.S.P.S. liability, despite the belief that the use of such material was permitted.
- Illegal or unlawful use includes but is not limited to use of pornography under the Crimes Act 1958 (Vic), offences under the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic), defamatory material, material that could constitute racial or religious vilification, unlawfully discriminatory material, stalking under the Crimes Act 1958 (Vic), use which breaches copyright law, fraudulent activity, computer crimes and other computer offences under the Cyber Crime Act 2001 (Cth) or Crimes Act 1958 (Vic) (as amended by the Crimes (Property Damage and Computer Offences) Act 2003 (Vic)) or any other relevant legislation.
- Users of C.S.P.S. ICT systems who receive unsolicited offensive or inappropriate material electronically should notify their classroom teacher and follow the DET *Guide for Responding to Incidents of Inappropriate Behaviour Affecting Students*.(Appendix 11)

## **LEGAL**

### **Copyright, Licensing, and Publication**

Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images.

All material submitted for internal publication must be appropriate to the school environment and copyright laws.

Students will be informed of these laws during class instruction.

## **INCIDENT RESPONSE**

Caulfield South Primary School will respond to inappropriate use of ICT and online behaviour that affects students, using the DET *Guide for Responding to Incidents of Inappropriate Behaviour Affecting Students*.(Appendix 11) and the Caulfield South Primary School *Student Engagement Policy*.

## **PRIVACY**

School ICT and electronic communication should never be used to disclose personal information of another except in accordance with the school's privacy agreement or with proper authorisation. The DET Privacy Policy (Appendix 8) and related legislation requires the school to take reasonable steps to protect the personal information that is held by the school, from misuse and unauthorised access. Authorised users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

While after school use of communication technologies by students is the responsibility of parents, school policy requires that no student attending the school may identify, discuss, photograph or otherwise publish personal information or personal opinions about school staff, fellow students or the school. Any such behaviour that impacts negatively on the public standing of the school may result in disciplinary action.

The school takes a strong position to protect privacy and prevent personal information and opinion being published over school network facilities, school ICT and any future technologies used at Caulfield South Primary School.

## **NETWORK CONNECTIVITY**

Caulfield South Primary School will ensure access to the schools eduSTAR network through school-owned or authorised devices. This network is provided by the DET and complies with their security and filtering requirements. C.S.P.S. makes no

guarantee that the network will be operational 100% of the time. In the rare case that the network is down, the School will not be responsible for lost or missing data.

## **MOBILE PHONE AND OTHER PERSONAL DEVICE USE AT SCHOOL**

Caulfield South Primary School accepts that some parents provide their children with mobile phones and other personal electronic devices. However, whilst on school property and during school excursions and camps, use of mobile phones or personal electronic devices is not permitted by students unless specifically authorised by the Principal or classroom teacher.

### **RESPONSIBILITY**

It is the preference of the school that mobile phones and personal electronic devices are not brought to school.

It is the responsibility of students who do bring mobile phones or personal electronic devices onto school premises to adhere to the guidelines outlined in this document.

Parents should be aware if their child takes a mobile phone or personal electronic device onto school premises, the child's class teacher must be advised.

Students are to switch off their phone or personal electronic device when they enter the school grounds and ensure that it is kept in their bag at all times unless an educational use is agreed upon by the classroom teacher.

Students are required to mark their mobile phone or personal electronic device clearly with their name.

The school accepts no responsibility for replacing lost, stolen or damaged mobile phones or personal electronic devices. Their safety and security is wholly in the hands of the student.

The school accepts no responsibility for students who lose or have their mobile phones or personal electronic devices stolen while travelling to and from school.

It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

When using mobile phones, students must behave according to the C.S.P.S. ICT Acceptable Use Agreement, and protect the privacy and dignity of individuals and security of information, to maintain the public standing of the school and compliance with State and Federal laws.

The school strongly advises that for safety reasons, headphones should not be used when students are traveling to and from school, eg. walking, riding a bike, moving on and off buses.

In accordance with school policies, any mobile phone or personal electronic device being used during the school day will be confiscated.

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 the appropriate way. Phone calls home to parents are to be made with a staff member.

### **CHROMEBOOK PROGRAM**

Please refer to the C.S.P.S. Chromebook Program Information Pack for specific details relating to the implementation of this program.

### **PRICE**

Caulfield South Primary School does not take responsibility for the retail costs associated with the purchase of the device. Device costs are set by the retail supplier Learning With Technology (LWT), a Department of Education and Training authorised school supplier. They reserve the right to alter the cost without notice. The school eLearning team will review the program device on a yearly basis and reserves the right to alter the device for each new year based on a measure of fit for purpose and cost effectiveness.

### **WARRANTY & SERVICING**

C.S.P.S. will provide a contact person at the school who will be responsible for logging warranty and servicing claims directly with LWT. Servicing of devices will be conducted at school by LWT authorised technicians. While a device is being serviced, the school will make a replacement device available for use while the student is at school.

### **TRANSPORTING YOUR DEVICE**

When students are transporting their devices in and around the school (for example to a specialist subject), they must ensure that the device is closed and in its carry case. Students should never run with these devices as this may lead to damage if the device is dropped. Students should avoid carrying their device in their backpack, as other items may place unnecessary pressure on the device and damage may occur.

### **CHROMEBOOKS LEFT IN UNSUPERVISED AREAS**

Under no circumstances should a student's device be left in an unsupervised area (including, but not limited to, school grounds, open building spaces, computer lab, specialist areas, library, offices, unlocked classrooms or toilets). Any device left in these areas is at risk of being stolen or damaged. If a device is found in an unsupervised area, it will be taken to the office.

## **MONITORING BY THE SCHOOL**

The school:

Reserves the right at any time to check work or data on the school's computer network, email, Internet, computers and other school ICT equipment/devices, without obtaining prior consent from the relevant Authorised User.

Reserves the right at any time to check work or data on privately owned ICT equipment on the school site or at any school-related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the school for purposes of any such check and to otherwise cooperate with the school in the process. Before commencing the check, the school will inform the Authorised User of the purpose of the check.

Has an electronic access monitoring system, through Netspace (in accordance with DET requirements), which has the capability to restrict access to certain sites and data.

Uses the GAFE learning platform and Chromebook hardware together to provide a high level of monitoring and security measures at school and at home, using the Chrome management console.

1. Devices are only accessible to students within the @caulfieldsouthps domain.
2. Access to online content is strictly filtered according to age and curriculum content.
3. Teachers at C.S.P.S. can curate and supervise content to achieve maximum guided learning.
4. The Australian Government's 'Cybersafety Help Button' is installed on all devices.
5. Devices can be remotely disabled at specific times to manage the amount of screen time.
6. Email is limited to sending to people within our secure @caulfieldsouthps domain, and in Year 4, only to members of each child's own year level.
7. Outside accounts are unable to send unsolicited emails.
8. Because these settings are managed centrally and are connected to the student accounts, these restrictions are transferred to the home environment when using the Chromebook.
9. The school has access to all student emails/communications and activities through their @caulfieldsouthps account to enable effective monitoring.
10. Filters for inappropriate content are applied to student emails.
11. Google removes ads for @caulfieldsouthps domain users.
12. Adblocker Plus application is installed on all devices.

Monitors traffic and material sent and received using the school's ICT infrastructures. This may be analysed and monitored to help maintain an eSmart learning environment.

# 1.8 Information and Communications Technology (ICT) Policy

## **SCREEN TIME**

At Caulfield South Primary School teachers recognise that a balanced approach to learning is essential. The C.S.P.S. Chromebook program does not advocate for our students' ICT usage to become the dominant mode of communication or to replace face to face communication. Our whole-school ICT programs aim to use these tools to support more efficient inquiry learning. Screen time at Caulfield South Primary School will be guided by the DET *Safe Usage Guideline* (Appendix 3) and the curriculum and pedagogical needs, as identified by the classroom teacher.

Students in Prep to Year 3 will have 1 hour of screen access per week scheduled in the school Computer lab. Student screen time will increase with the supplementary use of school ICT for eLearning purposes.

## **APPENDIX LIST**

1. [DET Using Digital Technologies to Support Learning and Teaching Policy](#)
2. [C.S.P.S. Student ICT Acceptable Usage Agreement](#)
3. [DET safe usage guideline](#) (ergonomics & duration)
4. [DET Benefits of personal learning devices](#)
5. [DET Copyright Policy](#)
6. [Childrens eSafety Commissioner](#)
7. [Google Apps for Education Customer Usage Agreement](#)
8. [DET Privacy Policy](#)

**C.S.P.S. PERMISSION TO BORROW ICT**

Chromebooks borrowed on student loan are not covered by school insurance. It is therefore necessary for a parent to sign this form to indicate that you guarantee to pay for repairs or replacement, if required, due to damage or loss of the loaned equipment caused by your son/daughter. This allows Caulfield South Primary School to expect compensation to cover replacement or repair of borrowed equipment, as needed. When students borrow C.S.P.S.' equipment, they accept responsibility for maintaining it and returning it in perfect working order. The student who has borrowed the equipment is responsible for any damage or loss when that item is borrowed in their name, regardless of whether other students are also involved in the loss/damage of the device. If other students are directly involved in the loss/damage of the item, the cost of repairing/replacing the item may be apportioned between the students involved (at the discretion of the C.S.P.S. leadership team).

Students must check the equipment before returning it, ensuring nothing is missing and it is all working properly. Students are responsible for reporting any faults or loss. All items must be returned at the end of the period.

**Students must sign & return this form:**

**Student's name:** \_\_\_\_\_

**Signed:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**This section must be completed by the parent/guardian of the student:**

**I \_\_\_\_\_, the parent/guardian of**  
**have read and understand**

**this Acceptable Use Policy. I agree that my child shall observe these guidelines and conditions and I**

**understand I will pay the costs of any repair or replacement required.**

**Signed:** \_\_\_\_\_ **Date:** \_\_\_\_\_

## **CSPS Student ICT Acceptable Use Agreement**

### **School profile statement**

At Caulfield South Primary School we support the rights of all members of the school community to be provided with and engage in a safe, inclusive and supportive learning environment. This extends to the use of digital tools and online communities and is underpinned by our expectation of safe and responsible behaviour of all members of the school community. At our school we:

- have a Student Engagement Policy that states our school's values and expected standards of student behaviour, including actions and consequences for inappropriate online behaviour
  - educate our students to be safe and responsible users of digital technologies.
  - raise our students' awareness of issues such as online privacy, intellectual property and copyright
  - supervise and support students when using digital technologies within the classroom and establish clear protocols and procedures when working in online spaces, including reviewing and considering the safety and appropriateness of online tools and communities.
  - provide a filtered Internet service but acknowledge that full protection from inappropriate content can never be guaranteed
  - respond to issues or incidents that have the potential to impact on the wellbeing of our students, including those reported through online services
  - know that some online activities are illegal and as such, we are required to report this to the appropriate authority, including Victoria Police.
  - support parents/guardians to understand safe and responsible use of digital technologies, potential issues and the strategies that they can implement at home to support their child;
- providing this Acceptable Use Agreement and current information from both the Department of Education and Training and Cybersmart:

- o [Bullystoppers Parent Interactive Learning Modules](#)
  
- o [Parents Cybersafety guide](#)

## **Safe and responsible behaviour**

When I use digital technologies and the Internet, I communicate respectfully by:

- always thinking and checking that what I write or post is polite and respectful
- being kind to my friends and classmates and thinking about how the things I do or say online might make them think or feel
- working to stop bullying. I don't send mean or bullying messages or pass them on to others
- creating and presenting my own work and if I do copy something from the Internet, letting others know by sharing the website link to acknowledge the creator.

When I use digital technologies and the Internet, I protect personal information by being aware that my full name, photo, birthday, address and phone number is personal information and is not to be shared online. This means I:

- protect my friends' information in the same way
- protect my passwords and don't share them with anyone except my parent/s
- only ever join spaces with my parents or teacher's guidance and permission
- never answer questions online that ask for my personal information
- know not to post three or more pieces of identifiable information about myself.

When I use digital technologies and the Internet I respect myself and others by thinking about what I share online. This means I:

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

At school we/I have:

- discussed ways to be a safe and responsible user of digital technologies and the Internet.
- presented my ideas around the ways that I can be a smart, safe and responsible user of digital technologies and the Internet. I will use this

knowledge at school and everywhere I use digital technologies and the Internet.

### **My ideas on safe and responsible behaviour**

When I use digital technologies and the Internet I communicate respectfully.

This means I: (write or draw...)

When I use digital technologies and the Internet I protect personal information.

This means I: (write or draw...)

When I use digital technologies and the Internet I respect myself and others.

This means I: (write or draw...)



# A Step-by-Step Guide for Responding to Online Incidents of Inappropriate Behaviour Affecting Students

## School Staff Duty of Care

Schools have a duty of care to take reasonable steps to protect students from any harm that should have reasonably been foreseen. The nature and scope of the duty in these circumstances will vary according to a number of factors, for example: the role and responsibilities of the employee, whether the incident occurred inside or outside of school hours, etc. You are concerned about a student because you have:

- received a disclosure from the student who has been subjected to inappropriate behaviour that is occurring or has occurred in the digital world.
  - received a report from an adult or another student about inappropriate behaviour that is occurring or has occurred in the digital world.
- For further information visit about Duty of Care: [www.education.vic.gov.au/management/ol/manage/care.htm](http://www.education.vic.gov.au/management/ol/manage/care.htm)

<p><b>Step 1</b></p> <p><b>IDENTIFYING CONCERNS</b></p>	<p><b>Step 2</b></p> <p><b>FURTHER ACTIONS</b></p>	<p><b>Step 3</b></p> <p><b>REPORTING</b></p>	<p><b>Step 4</b></p> <p><b>WELLBEING REFERRAL</b></p>	
<p><b>An incident of concern may include one or more of the following:</b></p> <p><b>An event which causes distress to a student</b> including cyberbullying, sexting, exposure to pornographic images or a breach of the school's Student Engagement Policy.</p> <p><b>A student has been EXPOSED to and affected by inappropriate behaviour online and:</b></p> <p>The student is at risk of suffering significant physical, psychological or emotional harm and may be in need of immediate protection.</p> <p><b>Go to Step 3</b></p>	<p><b>A student has ENGAGED in inappropriate behaviour online that:</b></p> <p>a) May cause psychological or emotion harm to another student(s). <b>Go to Step 2</b></p> <p>b) Could be deemed as criminal activity. <b>Go to Step 3C</b></p> <p>c) Could be psychologically and/or emotionally damaging to themselves (e.g. sexting). <b>Go to Step 2</b></p>	<p><b>If you suspect that inappropriate behaviour has occurred, it is important to make sure the student's are in a safe environment. It is also important to take detailed notes of the action that may include one or more of the following:</b></p> <p><b>A.</b> Inquire into the inappropriate behaviour. This may include discussions with all staff/students who have been directly or indirectly in the incident and/or its effects.</p> <p><b>B.</b> If you become aware during your inquiry that a criminal offence may have occurred contact the relevant authorities. <b>Go to Step 3B &amp; C</b></p> <p><b>C.</b> Where appropriate, contact the parents of all students involved. *If a school is unsure whether parents should be contacted, the Department's Legal or Emergency and Security Management Unit can assist to make a decision. <b>Go to Step 3D</b></p> <p><b>D.</b> Provide reasonable and ongoing wellbeing support to all students and staff who were involved in or witness to the incident. <b>Go to Step 4</b></p> <p><b>E.</b> Where appropriate, refer to the school's Student Engagement Policy and follow the appropriate processes and procedures. <b>Go to Step 5</b></p>	<p><b>A. Report to School Leadership</b> Staff member immediately advises and consults a member of the school's leadership team to report the incident and plan the appropriate response.</p> <p><b>B. Report to Emergency and Security Management</b> All reportable incidents should be reported to Emergency and Security Management Unit (03 9589 6286). This will alert regional staff.</p> <p><b>C. Report to Victoria Police</b> It is expected that an staff member will contact police if there has been possible criminal activity. In such cases seek advice about contacting the parents of ALL students involved in the incident. *If a school is unsure whether an incident should be reported the Police will advise the school as to whether they will investigate or whether the school should handle the situation.</p> <p><b>D. Report to Parents and/or Guardians</b> Contact the parents/guardians of the student who has been exposed to and/or engaged in inappropriate behaviour (where appropriate). *If a school is unsure whether parents should be contacted, the Department's Legal or Emergency and Security Management Unit can assist to make a decision.</p> <p><b>E. Provide a Wellbeing Referral and Support</b> Consult with relevant regional staff as appropriate. <b>Go to Step 4</b></p>	<p><b>Wellbeing Referral</b> Contact your school's Leadership and/or Student Wellbeing Team to discuss strategies that can be used to respond to and support ALL students at risk from the inappropriate behaviour. This may include counselling and support or the development of an action plan to implement targeted strategies.</p> <p>Keep a record of the action plan and make notes on any relevant observations. Review the action plan as necessary.</p>
<p><b>Step 5</b></p> <p><b>ACTIONS AND CONSEQUENCES</b></p> <p>Each Victorian government school has developed a Student Engagement Policy that sets out the rights, responsibilities and shared expectations of everyone in the school community, including students, parents, teachers and school staff. The policy clearly defines the consequences for students who behave inappropriately. In responding to online incidents of inappropriate behaviour, principals and teachers should refer to their Student Engagement Policy for appropriate actions and consequences.</p>				
<p>For additional information, see: Building Respectful and Safe Schools Resource <a href="http://www.education.vic.gov.au/respect">www.education.vic.gov.au/respect</a></p>				