

## Analysis of Proposal to Ban Mobile Phones in Schools

### CURRENT POLICY AND PRACTICE

- Principals, in consultation with their school community, make decisions about school procedures regarding student access to, or usage of, mobile devices. Considerations informing these decisions may include the educational needs of the students, and parent and community expectations.
- The Advice for State Schools on Acceptable Use of ICT Facilities and Devices, within the Department's Use of ICT systems procedure, outlines acceptable and unacceptable use of mobile devices for students while at school.
- This document also provides schools with a template form to seek agreement from parents and students to abide by the procedures and expectations for use of ICT facilities and devices, including phones.
- Consequences for inappropriate behaviour in regard to mobile phones are implemented according to a school's Responsible Behaviour Plan for Students which clearly outlines the standard of behaviour expected from students and the consequences for students when those standards are not met. The Responsible Behaviour Plan for Students also outlines protocols around temporary removal of a mobile phone if it is being used in inappropriate or unacceptable ways.
- Some examples of the different requirements state schools might apply to access and use of mobile phones include:
  - phones to be turned on to silent mode and out of sight or switched off in the classroom (unless give permission to use them);
  - phones to be placed in a safe place in the room when students arrive for class;
  - phones to be handed in/picked up from a particular location before and after school;
  - students to use mobile phone lockers to store phones during the day;
  - students to only use their mobile phones at break times.
- The notion of 'banning' mobile phones at schools has been interpreted as students having access to the mobile phone during school hours.

### STAKEHOLDER VIEWS – REPORTED IN COURIER MAIL ARTICLE 4/04/2018

- Federal Minister for Education and Training Simon Birmingham called for a ban on phone use in school time 3/02/2018. "There's almost no reason students shouldn't have their phones switched off and in their locker while they're at school. Although learning to work with technology is essential, phones can be a distraction from lessons and a platform for bullying unless schools have the right policies in place."
- Federal eSafety Commissioner, Julie Inman Grant – schools must have "robust policies and procedures in place around technology use".
- Queensland Teachers' Union President, Kevin Bates – it is difficult to ban smartphones at school because parents objected when phones are confiscated. "I don't accept blanket bans. Teachers often deal with the fallout when devices go missing or get damaged."
- Child Psychologist, Michael Carr-Gregg – "Smartphones must be banned in primary schools and kids needing them for 'security purposes' should be given ones with no internet access."
- The Federal Cyber Safety Working Group member, Susan McLean – "there should be no personal devices used during the school day – it has to be against the school rules."
  - Ms McLean's company, cybersafetysecurity<sup>1</sup> is cited as stating: Schools must embrace technology for the wonderful tool that it is, not dwell on the problem that it might become. Be proactive in all areas, educate your whole community, students, parents and staff and make sure that your

<sup>1</sup> <http://www.cybersafetysolutions.com.au/>

## Analysis of Proposal to Ban Mobile Phones in Schools

policy documents are relevant, circulated to all members of the school community and are regularly updated. Students must be encouraged to come forward and report problems and breaches of policy must be dealt with sensitively and efficiently.<sup>2</sup>

PROS OF BANNING MOBILE PHONES AT SCHOOL	CONS OF BANNING MOBILE PHONES AT SCHOOL
The distraction to learning that mobile phones represent if students interact with them in the classroom (e.g. sending text messages and taking phone calls) would be avoided.	Access to technology and mobile devices in schools is a modern-day reality and expectation in order to provide students with a contemporary education that sets them up for success in the modern world.
Cyberbullying at school may be reduced, given students would not be able to send text messages and photos to each other during school hours from their phones.	Responsible and appropriate use of technologies such as mobile phones, tablets and laptops in classrooms is a way of modelling responsible use of the devices in the wider community.
If schools have a policy of confiscating phones where a breach of the school rules occurs, this can become very time consuming and potentially confrontational both with the student and with the parent of the student.	Banning mobile phones doesn't consider other current and emerging digital technologies – smartphones, smart watches, tablets, laptops which all have the functionality to access the internet, take photos, send messages.
Encourages greater social interaction at school.	Many schools use phones as an educational tool for students to research information relevant to an aspect of the curriculum with which they are engaging in the classroom.
Mobile phones are relatively expensive items and theft or losing a phone can create time-consuming consequences for schools.	Schools recognize the importance of mobile phones for student safety and contact with parents. An example may be when students are on an excursion and return to school is later than anticipated and the student will miss the bus. Many parents expect to be able to contact their child directly, if and when needed, and many would not support a school imposing a ban on students bringing phones to school.
Banning mobile phones may reduce the risk of students trying to access information to respond to a test.	Using mobile phones in the classroom provide an important opportunity for teachers to provide instruction regarding on-line safety and students being aware of and protecting their digital footprint.
Some research has found that banning mobile phones at school results in increased performance for low-achieving students <sup>3</sup> (although this research is challenged <sup>4</sup> ).	If the mobile phone has the capacity to locate the whereabouts of the phone/owner this can be very useful when children go missing.
May limit inequities between students.	Communication with the student is facilitated if the school has the number recorded and wishes the student to report to the office for example.

<sup>2</sup> <http://cybersafetysolutions.com.au/for-schools.shtml>

<sup>3</sup> <http://cep.lse.ac.uk/pubs/download/dp1350.pdf>

<sup>4</sup> <https://www.teachermagazine.com.au/articles/mobile-ban-raises-achievement-a-micro-view-of-a-macro-phenomenon>

## Analysis of Proposal to Ban Mobile Phones in Schools

PROS OF BANNING MOBILE PHONES AT SCHOOL	CONS OF BANNING MOBILE PHONES AT SCHOOL
Unrestricted access to the internet via mobile phones can be very problematic in schools as well as at home.	The practical reality of monitoring a ban on mobiles at school will increase administrative burden on school staff.
	The risk of a mobile phone being stolen is reduced if the student has it on their person, rather than in their bag.
	Imposing a consequence on a student for texting or phoning a parent during school time is unlikely to be supported by the parent.
	School contexts vary greatly (e.g. primary, high P-10/12, special, urban, rural, remote) and a blanket ban is not appropriate, nor would it address the core issues of cyberbullying.
	'Technologies contribute appreciably to reducing student alienation, improving student teacher relations, increasing student attention and turning on previously disinterested students.' <sup>5</sup>

### JURISDICTIONAL COMPARISON

JURISDICTION	POLICY	GUIDELINES
<p><b>Victoria</b></p> <p>No state wide ban - policy and procedures vary from school to school.</p>	<p><b>Students Using Mobile Phones</b></p> <ul style="list-style-type: none"> <li>• To ensure schools provide clear policy advice on the use of mobile phones</li> <li>• Varies from school to school</li> <li>• Schools that allow the use of mobile phones must clearly and regularly advise students and parents/guardians of their expectations and policy requirements</li> <li>• Mobile phone cameras (still and video) must not be used:                             <ul style="list-style-type: none"> <li>○ in banned spaces for example changing rooms, toilets, gyms and swimming pools</li> <li>○ to film people and their activities without their knowledge or permission.</li> </ul> </li> </ul>	<p><b>Schools can:</b></p> <ul style="list-style-type: none"> <li>• develop policies about what students can and cannot bring to school</li> <li>• ban anything illegal, dangerous or likely to cause disruption or harm to the smooth running of the school.</li> </ul> <p><b>Students should:</b></p> <ul style="list-style-type: none"> <li>• only use mobile phones when usage will not disrupt the normal school routine</li> <li>• have their mobile phones switched off and out of sight during classes</li> <li>• only use their mobile phones before or after school, or during recess and lunch breaks</li> <li>• display courtesy, consideration and respect for others when using a mobile phone</li> </ul>

<sup>5</sup> Ibid

## Analysis of Proposal to Ban Mobile Phones in Schools

JURISDICTION	POLICY	GUIDELINES
	<ul style="list-style-type: none"> <li>• Mobiles phones must not be used to send harassing or threatening messages</li> </ul>	<ul style="list-style-type: none"> <li>• ensure that their phones are always stored in a safe and secure place.</li> </ul> <p>Note: Students can have access to a mobile phone where there is a need to contact parents/guardians in an emergency.</p> <p><b>Schools should:</b></p> <ul style="list-style-type: none"> <li>• discourage the use of mobile phones in the classroom unless they can be appropriately incorporated into the learning program</li> <li>• inform students and parents that mobile phones are used at their owners' risk</li> <li>• take appropriate action against any student who:               <ul style="list-style-type: none"> <li>- photographs or films other individuals without their consent or who sends harassing or threatening messages</li> <li>- is/are caught using a mobile phone in exams or assessments</li> </ul> </li> </ul>
<p>NSW</p> <p>No state-wide ban - policy and procedures vary from school to school</p> <p><b>No reference to Mobile Phones in any of the following:</b></p> <ul style="list-style-type: none"> <li>• Bullying – Preventing and Responding to Student Bullying in Schools Policy (2011)</li> <li>• Behaviour Code for Students</li> </ul>	<p><b>Bring your Own Device</b></p> <ul style="list-style-type: none"> <li>• An optional strategy for schools</li> <li>• Schools can allow students to bring devices to school for the purpose of learning.</li> <li>• Mobile phone voice and text, SMS messaging or device instant messaging use by students during school hours is a school-based decision.</li> </ul>	
<p>South Australia</p>	<p>Individual school policies relating to mobile phone use during the school day.</p>	

## Analysis of Proposal to Ban Mobile Phones in Schools

JURISDICTION	POLICY	GUIDELINES
No state-wide policy - policy and procedures vary from school to school		
<p><b>Tasmania</b></p> <p>No state wide ban - policy and procedures vary from school to school.</p>		<p><b>Mobile Devices in Tasmanian Government Schools</b></p> <ul style="list-style-type: none"> <li>• The Department of Education understands that mobile devices such as mobile phones, laptops, iPads and iPods are an important part of life and learning in today's world</li> <li>• If your child is using their mobile device as a telephone at school, they need to:               <ul style="list-style-type: none"> <li>○ Check if they can have it in class.</li> <li>○ Keep their phone on silent during class times.</li> <li>○ Only use as directed by the teacher.</li> <li>○ Protect the privacy of others and never post private information about another person.</li> </ul> </li> </ul>
<p><b>Western Australia</b></p> <p>No state wide ban - policy and procedures vary from school to school.</p>	<p><b>Student Behaviour Policy</b></p> <p>The principal will document a whole school plan to support positive student behaviour that includes:</p> <ul style="list-style-type: none"> <li>• measures to address all forms of bullying</li> <li>• the rules regarding personal use of mobile and other electronic devices, and responses to breaches of these rules.</li> </ul>	
<p><b>Northern Territory</b></p> <p>No state wide ban - policy and procedures vary from school to school.</p>	<p><b>Mobile phones and electronic devices in the school environment Policy</b></p> <p><b>Principals</b></p>	<p><b>Mobile phones and electronic devices in the school environment Guidelines</b></p> <p>An acceptable use policy should be developed and implemented before a student is permitted to bring a mobile phone or other electronic device on to school premises. This may include a requirement for</p>

## Analysis of Proposal to Ban Mobile Phones in Schools

JURISDICTION	POLICY	GUIDELINES
	<p>In conjunction with school councils, principals are responsible for developing procedures to govern the use of electronic devices within the school environment.</p> <p>The principal is responsible for ensuring that procedures and guidelines regarding the use of electronic devices are developed and made available to parents/carers and students.</p> <p>The principal is responsible for ensuring that the school's code of conduct includes a statement on appropriate use of electronic devices on school premises.</p> <p><b>Regional Director</b></p> <p>It is the responsibility of the relevant regional director to ensure that procedures governing the use of electronic devices in the school environment are developed and adhere to the requirements of the policy.</p> <p><b>Students</b></p> <p>Students are responsible for ensuring they comply with the schools code of conduct and procedures governing the use of electronic devices in the school environment. Students must ensure that devices are only used appropriately and responsibly, with due regard to the rights of others, including the rights of other students to learn without being unduly disrupted or put at risk.</p> <p>Students are also responsible for ensuring that any electronic devices carried by them onto school premises are stored in a safe place during school hours, in line with any specific arrangements made by the school.</p> <p><b>Parents</b></p>	<p>parents/carers and students to sign an acceptable use agreement before a student is permitted to bring an electronic device onto school premises.</p>

## Analysis of Proposal to Ban Mobile Phones in Schools

JURISDICTION	POLICY	GUIDELINES
	<p>It is the responsibility of parents/carers to support and reinforce the procedures regarding the acceptable use of electronic devices in their child's school and to ensure that their child is complying with those procedures.</p>	
<p><b>Australian Capital Territory</b> No state wide ban - policy and procedures vary from school to school.</p>		<p><b>Appropriate Use of Mobile Phones</b></p> <ul style="list-style-type: none"> <li>• Schools are expected to develop a policy statement and set of procedures which provide guidelines for the appropriate use of mobile phones during school hours</li> <li>• Schools and colleges can make reasonable rules about what students can and cannot bring to school</li> <li>• The use of mobile phones, pagers, Walkmans and similar devices in class is disruptive to the learning environment of all students and should be discouraged.</li> <li>• Students wishing to use these devices in special circumstances should negotiate arrangements with relevant school/college staff</li> </ul>

Released under the RTI Act

# Advice for State Schools on Acceptable Use of ICT Facilities and Devices

This advice supports the Information and Communication Technology (ICT) Procedure.

The department allows restricted access to its ICT facilities and devices which includes network, printers etc. using either departmental or personal owned devices.

If in doubt when implementing technical requirements around the management of personally owned mobile devices and access to the department's ICT facilities and devices, advice can be sought from the Service Centre on 1800 680 445. Policy advice can be sought directly from Manager, Information Policy on 3034 4313. Additionally, information is available at Service Centre Online: <https://qlddet.service-now.com/sco/>.

## Personal mobile device access

The department is aware that limited personally owned mobile device access is essential for the effective running of schools. The department reserves the right to restrict access of personal mobile devices to ensure the integrity of the network and a safe working and learning environment for all network users. These mobile devices include but are not limited to laptops, tablet devices, voice recording devices (whether or not integrated with a mobile phone or MP3 player), games devices (e.g. PSPs, Game Boys), USBs, DVDs, CDs and smart phones.

### School employees personal mobile device access

Principals are to ensure that school employees follow the requirements under the Information and Communication Technology (ICT) Procedure's bring your own (BYO) personal mobile device section.

### Student personal mobile device access

The departmental position is that mass access to the network by students' wholly owned personal mobile devices could compromise the integrity of the ICT network. Principals however can determine that for educational purposes a student can have access to the ICT network. This connection is provided only if the mobile device meets the department's security requirements (see iSecurity site for details) at a minimum installing, running and updating anti-virus software. Schools wanting students to connect to the department's ICT network are required to develop procedures to ensure that such provisions are assessed against the department's security requirements (where necessary undertaking a risk assessment) and that students and their parents/guardians are provided with the necessary education and assistance to be able to meet these departmental requirements.

The procedures are to include:

- providing advice to all students and their parents on appropriate security requirements (see iSecurity site for details)
- advising teacher/supervisor as soon as any breach of security is suspected
- the right to restrict/remove student access to the intranet, internet, email or other network facilities if they do not adhere to the school's network usage and access policy, guideline or statement
- ensuring that students are aware of occupational health and safety issues when using computers and other learning devices.

Schools that are implementing or have implemented the BYOx process need to also ensure steps have been taken to provide a safe and effective learning environment for students while meeting the department's security requirements. This includes advising parents/guardians that the devices provided allows access to their home and other out of school internet services and that such services may not include any internet filtering.



## Student access to the department's ICT facilities and devices

The Smart Classrooms strategy underpins the growth and improvement in innovative programs and resources in schools for teachers and students. Essential tools for providing these innovative educational programs are the intranet, internet, email and network services (such as printers, display units and interactive whiteboards) that are available through the department's/school's ICT network. These technologies are vital for the contemporary educational program provided in schools.

At all times students, while using these ICT facilities and devices, will be required to act in line with the requirements of the Code of School Behaviour and any specific rules of their school. In addition students and their parents should:

- understand the responsibility and behaviour requirements (as outlined by the school) that come with accessing the school's ICT network facilities
- ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email
- be aware that:
  - access to ICT facilities and devices provides valuable learning experiences for students and supports the school's teaching and learning programs
  - ICT facilities and devices should be used appropriately as outlined in the Code of School Behaviour
  - students who use a school's ICT facilities and devices in a manner that is not appropriate may be subject to disciplinary action by the school, which could include restricting network access
  - despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed
  - teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

## School specific ICT responsible use procedure

The *Information Communication and Technology (ICT) Procedure* provides direction to school principals around formulating a school procedure on access to the department's/school's ICT facilities and devices for parents and/or students to understand and acknowledge. This may take the form of a procedure, policy, statement or guideline and may require consultation with the school community. Acknowledging through signing seeks to support an understanding of what is lawful, ethical and safe behaviour when using or accessing the department's network and facilities by students and their parents. Principals may seek sign-off either on enrolment of students or alternatively at the start of each school year.

The following dot points are to assist schools with the formulation of their own procedure. Further guidance on drafting this section can be sought from the *Use of ICT Facilities and Devices Guideline*.

### **Purpose statement**

- Information and communication technology (ICT), including access to and use of the internet and email, are essential tools for schools in the provision of innovative educational programs.
- Schools are constantly exploring new and innovative ways to incorporate safe and secure information and communication technology (ICT) use into the educational program.
- School students, only with the approval of the principal, may be permitted limited connection of personally owned mobile devices to the department's information and communication technology (ICT) network, where this benefits the student's educational program.

### **Authorisation and controls**

The principal reserves the right to restrict student access to the school's ICT facilities and devices if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program. For example, a student with restricted school network access may be allocated a stand-alone computer to continue their educational program activities.

The Department of Education and Training monitors access to and usage of their ICT network. For example, email monitoring will occur to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.

The department may conduct security audits and scans, and restrict or deny access to the department's ICT network by any personal mobile device, if there is any suspicion that the integrity of the network might be at risk.

### **Responsibilities for using the school's ICT facilities and devices**

- Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the *Code of School Behaviour*.
- Students are to be aware of occupational health and safety
- issues when using computers and other learning devices.
- Parents/guardians are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
- Parents/guardians are responsible for appropriate internet use by students outside the school environment when using a school owned or provided mobile device.
- The school will educate students regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices. Students have a responsibility to behave in line with these safe practices.
- Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

- Students cannot use another student or staff member's username or password to access the school network, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.
- Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

### ***Responsibilities for using a personal mobile device***

- Prior to any personal mobile device being used approval is sought from the school to ensure it reflects the department's security requirements.
- Students are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.
- All files are to be scanned using appropriate virus software before being downloaded to the department's ICT network.
- Follow any advice provided on best security requirements e.g. password protection (see [iSecurity](#) site for details).
- Students and parents are to employ caution with the use of personal mobile devices particularly as these devices can store significant numbers of files some of which may be unacceptable at school e.g. games and 'exe' files. An 'exe' file ends with the extension '.exe' otherwise known as an *executable* file. When they are selected they can install programs which may start unwanted processes.
- Any inappropriate material or unlicensed software must be removed from personal mobile devices before bringing the devices to school and such material is not to be shared with other students.
- Unacceptable use will lead to the mobile device being confiscated by school employees, with its collection/return to occur at the end of the school day where the mobile device is not required for further investigation.

### ***Acceptable/appropriate use/behaviour by a student***

It is acceptable for students while at school to:

- use mobile devices for
  - assigned class work and assignments set by teachers
  - developing appropriate literacy, communication and information skills
  - authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, parents or experts in relation to school work
  - accessing online references such as dictionaries, encyclopaedias, etc.
  - researching and learning through the department's eLearning environment
- be courteous, considerate and respectful of others when using a mobile device
- switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning
- use personal mobile device for private use before or after school, or during recess and lunch breaks
- seek teacher's approval where they wish to use a mobile device under special circumstances.

### ***Unacceptable/inappropriate use/behaviour by a student***

It is unacceptable for students while at school to:

- use the mobile device in an unlawful manner
- download, distribute or publish offensive messages or pictures

- use of obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insult, harass or attack others or use obscene or abusive language
- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions for the use of social media, online email and internet chat
- send chain letters or spam email (junk mail)
- knowingly download viruses or any other programs capable of breaching the department's networks security
- use in-phone cameras anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invade someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- use the mobile phone (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school employees.

### **Sign-off**

The implementation of the sign-off process for school students and their parents/guardians should occur on enrolment and every year after through an annual collection, whichever suits the school's normal operations. The following is a suggested format for the signature block to be placed at the end of the procedure:

#### **Student:**

I understand that the school's information and communication technology (ICT) facilities and devices provide me with access to a range of essential learning tools, including access to the internet. I understand that the internet can connect me to useful information stored on computers around the world.

While I have access to the school's ICT facilities and devices: I will use it only for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.

Specifically in relation to internet usage, should any offensive pictures or information appear on my screen I will close the window and immediately inform my teacher quietly, or tell my parents/guardians if I am at home.

If I receive any inappropriate emails at school I will tell my teacher. If I receive any at home I will tell my parents/guardians.

When using email or the internet I will not:

- reveal names, home addresses or phone numbers – mine or that of any other person
- use the school's ICT facilities and devices (including the internet) to annoy or offend anyone else.

I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT facilities and devices inside or outside of school hours.

I understand that if the school decides I have broken the rules for using its ICT facilities and devices, appropriate action may be taken as per the school's *Behaviour Management Policy*, which may include loss of access to the network (including the internet) for a period of time.

I have read and understood this procedure/policy/statement/guideline and the *Code of School Behaviour*.

I agree to abide by the above rules / the procedure/policy/statement/guideline.

\_\_\_\_\_ (Student's name)

\_\_\_\_\_ (Student's signature) \_\_\_\_\_ (Date)

**Parent or guardian:**

I understand that the school provides my child with access to the school's information and communication technology (ICT) facilities and devices (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information on computers from around the world; that the school cannot control what is on those computers; and that a small part of that information can be illegal, dangerous or offensive.

I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend upon responsible use by students/my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT facilities and devices. Furthermore I will advise the school if any inappropriate material is received by my student/child that may have come from the school or from other students.

I understand that the school does not accept liability for any loss or damage suffered to personal mobile devices as a result of using the department's facilities and devices. Further, no liability will be accepted by the school in the event of loss, theft or damage to any device unless it can be established that the loss, theft or damage resulted from the school's/department's negligence.

I believe \_\_\_\_\_ (name of student) understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT facilities and devices (including the internet) under the school rules. I understand where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the *Behaviour Management Policy*. This may include loss of access and usage of the school's ICT facilities and devices for some time.

I have read and understood this procedure/policy/statement/guideline and the *Code of School Behaviour*.

I agree to abide by the above rules / the procedure/policy/statement/guideline.

\_\_\_\_\_ (Parent/Guardian's name)

\_\_\_\_\_ (Parent/Guardian's signature) \_\_\_\_\_ (Date)

The Department of Education and Training through its *Information Management (IM) Procedure* is collecting your personal information in accordance with the *Education General Provisions Act 2006* in order to ensure:

- appropriate usage of the school network
- appropriate usage of personal mobile devices within the school network.

The information will only be accessed by authorised school employees to ensure compliance with its *Information Management (IM) Procedure*. Personal information collected on this form may also be disclosed to third parties where authorised or required by law. Your information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact your child's school. If you have a concern or complaint about the way your personal information has been collected, used, stored or disclosed, please also contact your child's school.

**Note:** The Australian Mobile Telecommunications Association (<http://www.amta.org.au/>) has published materials which may be of use to schools including a template which can assist in creating an acceptable use policy.

# Web filtering - Removing online content

The following information is provided as a guide to state schools when seeking to remove and report the uploading of inappropriate images/ footage to websites, particularly where school employees and/or students are involved, or if the school is in some way associated.

## Incident awareness

The incident may come to your attention through employees, students, parents, community members, the media etc.

### Step 1: Incident investigation

Principal or their delegate undertakes immediate investigation of the incident by reviewing the web content of concern.

#### Website is accessible

Assessing the website of concern to review content to determine if further action is required.

#### Website is inaccessible

If the website is blocked contact the Service Centre by phone on 1800 680 445 to discuss options for available or escalate to the Cybersafety & Reputation Management Team for further investigation.

**Step 2:** Where employees, students or any school community members have been threatened, or are in danger as a result of the incident, the principal should take the school's usual emergency response process or report the incident to the regional director.

### Step 3: Requesting removal of content from a website

If the student responsible refuses to delete the inappropriate or offensive content or the identity of the person who posted the material is not known, then the principal, delegate, or victim should report the content to the site's service provider and ask to have it removed.

#### Where the website provides contact information

Coordinate with those directly involved for removal of information. Alternatively, where possible, directly request the website to remove the content.

**For assistance in removing content** seek advice from the Cybersafety & Reputation Management Team on (07) 3034 5035, [Cybersafety.ReputationManagement@deta.qld.gov.au](mailto:Cybersafety.ReputationManagement@deta.qld.gov.au) or [Regional Technology Manager](#).

### Step 4: Minimising access to offensive content

The principal should assess whether the website housing the offensive content requires blocking through the school and departmental network.

#### Website does not require blocking

No further action is required.

#### Request blocking of a website

**School level:** Request to block a website through school's [Regional Technology Manager](#).  
**Departmental level:** Request to block website through the Service Centre on 1800 680 445.

### Step 5: Reporting incidents

For employee misconduct contact the Ethical Standards Unit, email: [ethicalstandards@deta.qld.gov.au](mailto:ethicalstandards@deta.qld.gov.au) or phone: (07) 3234 1514

For further information about the removal of inappropriate images/footage on websites, contact:  
Cybersafety & Reputation Management Team  
Learning Technologies  
Phone: (07) 3034 5035  
Email: [Cybersafety.ReputationManagement@det.qld.gov.au](mailto:Cybersafety.ReputationManagement@det.qld.gov.au)

Assistance on removing content from the internet can also be sought from your Regional Technology Manager.

Released under the RTI Act by DOE

#### Security and licence

This document has an information security classification of public.

© The State of Queensland (Department of Education and Training) 2013

Unless otherwise noted below, materials included in this paper are licensed under a Creative Commons Attribution 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/3.0/au/>



Last review date: 7 April 2014 Final TRIM Ref: 14/33001

**Uncontrolled copy.** Refer to the Department of Education and Training Policy and Procedure Register at <http://ppr.det.qld.gov.au> to ensure you have the most current version of this document.