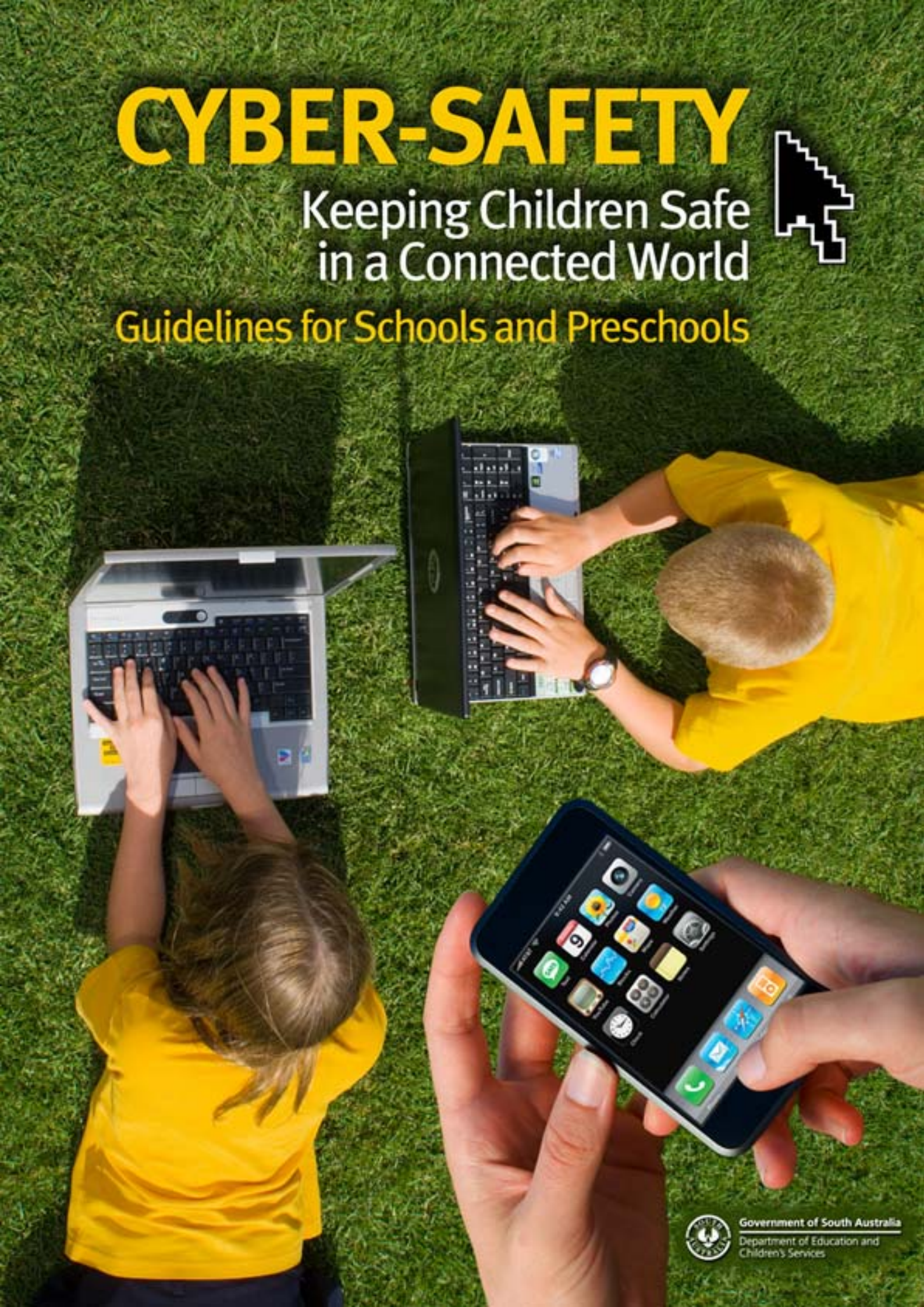
CYBER-SAFETY

Keeping Children Safe in a Connected World

Guidelines for Schools and Preschools



Government of South Australia
Department of Education and Children's Services

Authorised by the Department of Education and Children's Services
31 Flinders Street
Adelaide
South Australia 5000
June 2009

Grateful acknowledgment is made of material provided by:
Department of Education and Training, Western Australia for 'Children online' (2008). Accessed at http://policies.det.wa.edu.au/ 19/03/08.
NetSafe New Zealand. Accessed at http://www.netsafe.org.nz/ 08/05/09.

All web addresses in this document were current at 26 June 2009.

This document is also available on the internet at:
http://www.decs.sa.gov.au/speced2/pages/cybersafety/

Government of South Australia
Department of Education and Children's Services

Cyber-Safety

FOREWORD

South Australian schools and preschools are exciting places in which to teach and learn: our children naturally take advantage of developments in technologies to personalise and expand their learning opportunities, and our educators provide rich learning environments for children as they engage with people and resources, locally and globally.

In this dynamic, connected world of communication and learning, we need to ensure such opportunities do not place the young people in our schools and preschools at risk. Many of these risks are not new and educators are familiar with strategies and processes that maximise learning opportunities and outcomes, while minimising risk to children's safety and wellbeing.

The Department of Education and Children's Services (DECS) invests in network systems to manage and protect the welfare of children. However, the explosion of wireless and mobile devices allows children to bypass conventional network systems. This has the potential to expose young people to risks previously managed by filtered departmental and local systems. While the department will continue to protect children's identity and learning artefacts, we need to instil confidence in them to keep themselves safe and inform the adults around them if or when they feel uncomfortable, threatened or bullied - even if that occurs away from their school or preschool environment.

As mobile and fixed networks and technologies evolve rapidly, events may confront or challenge our current practices. *Cyber-safety - Keeping Children Safe in a Connected World* will assist leaders, educators and parents to share in the delights of young people learning online, while observing legislation, policies and practices that promote learning, protection and safety.

Cyber-safety - Keeping Children Safe in a Connected World, the *Keeping Safe: Child Protection Curriculum* introduced in 2008, and the work of the Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools are significant steps towards the achievement of safe learning environments for all children in DECS schools and preschools.

I commend this resource to you in the best interests of our children.

Chris Robinson
Chief Executive

Contents

Introduction

Opportunities for young people and adults to learn and engage with each other have exploded in recent times with the proliferation of computer networks, mobile devices, broadband connections to the Internet and virtual communities. With such exciting opportunities comes the need to ensure that leaders, educators, children and parents consider the implications for safe use of information and communication technologies (ICTs).

Learning is a social activity. It happens when people interact with other people and their ideas, knowledge and perspectives. ICTs provide children and students with new and engaging ways to learn. ICTs expand social and knowledge networks so that children and students access current information, interact with experts and participate in peer teaching and learning. Using ICTs they can publish their learning, as evidence of achievement or to invite feedback for improvement.

It is important to both protect and teach children, students and adults, while they learn to use ICTs and become responsible digital citizens. This includes adults thinking ahead of new risks and children and students learn how to avoid exposure to inappropriate material or activities, and protecting themselves when they are online. They need to learn how to use ICTs, including mobile technologies and social networking sites, in responsible and ethical ways. In addition, they need to feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate events. In response, these adults need to take appropriate actions to protect the child or young person.

These guidelines have been developed to assist staff in Department of Education and Children's Services (DECS) schools and preschools to put in place policies and procedures that will both protect and inform children, students and their parents. It collates and outlines legislation and DECS policies, and provides resources and sources of advice to help shape good cyber-safe practices.

It also complements the teaching and learning topics and resources available in the *Keeping Safe: Child Protection Curriculum*[1] introduced to schools and preschools in 2008.

Research shows schools are one of the safest environments for children.[2] DECS and each of its schools and preschools make every reasonable effort to achieve this by:

- developing programs to educate and inform children, students and parents about the opportunities and challenges of ICTs in learning programs
- monitoring and logging e-mail traffic and Internet use, and providing filters to help guard against access to inappropriate materials
- providing direction and advice about ICTs (including the Internet and mobile phones) use and misuse, such as bullying and e-crime
- supporting police officers in undertaking an investigation and the collection of evidence following a principal or director reporting a suspected e-crime.

In matters relating to cyber-safety, DECS works with, and is advised by:

- the *Keeping Safe: Child Protection Curriculum* - a child protection teaching and learning program in South Australian government schools and preschools, developed by experienced South Australian educators and child protection experts.
- the Abuse and Neglect Training program (previously Mandatory Notification Training)
- the Australian Communications and Media Authority (ACMA), which manages a national cyber-safety education and awareness program and is also responsible for monitoring online content, including Internet and mobile phone content, and enforcing Australia's anti-spam law.
- South Australia Police (SAPOL)
- the Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools, which has representatives from the three schooling sectors and eminent international researchers Professor Ken Rigby, Professor Phillip Slee and Drs Barbara Spears and Shoko Yoneyama.

1. Department of Education and Children's Services (2008) *Keeping Safe: Child Protection Curriculum.* [5 bands] Adelaide, DECS.
2. National Safe Schools Framework. Accessed at http://www.mceetya.edu.au/verve/_resources/natsafeschools_file.pdf

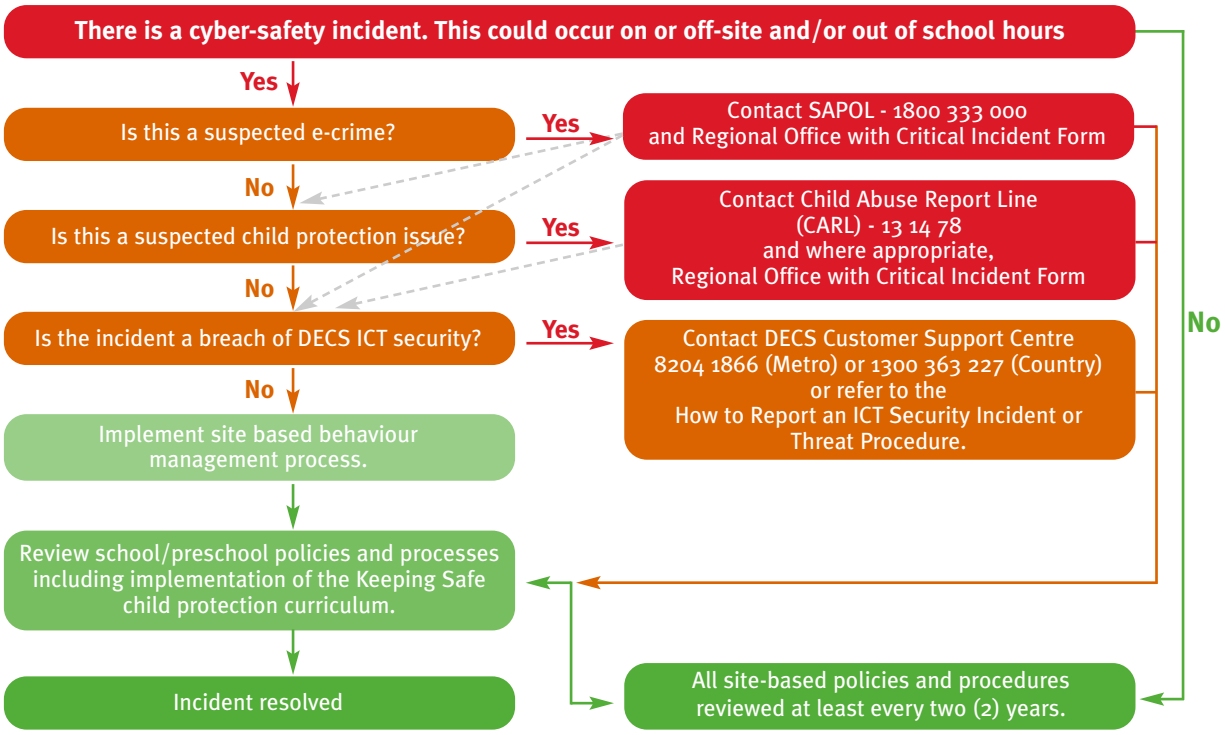
Cyber-safety Guidelines

There is a range of legislation and policy that schools and preschools need to observe to ensure cyber-safety, listed on pages 18-19. Many of the principles covered in the non-ICT-specific government Acts and DECS policies, such as the Children's Protection Act 1993 and the DECS Child Protection and School Discipline policies, apply in all learning environments. Children's behaviour and safety, whether online or offline, whether face to face or through text messaging, are subject to the same expectations schools and preschools have always applied.

It should be noted that these guidelines apply to DECS staff, children and students accessing online services in any DECS location including, but not limited to, schools and preschools and, where appropriate, to volunteers. If a child or student who is enrolled in a school behaves online in a manner that threatens the wellbeing of a child, student, parent or member of the school community, even if this occurs off-site and/or out of school hours, the principal has the authority under the Regulation pursuant to the Education Act 1972 to suspend or exclude a student from attendance at school. If the child attends a preschool, then the preschool director is guided by *Supporting and managing children's behaviour: An early childhood resource* (DECS 2004).

If a principal or director suspects an electronic crime has been committed, this must be reported to SAPOL. Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device, the device should be confiscated and handed to the investigating police officer. It is important that the device is not opened to view any video clips as this may make this information inadmissible in a court of law. The principal or director must cease any further investigation once he/she has decided to hand the investigation to SAPOL.

The following flowchart may assist in decision making if an incident occurs. It is critical that the safety and welfare of the child, children or students are considered as paramount throughout the process. This flowchart is consistent with the widely adopted prevention, preparation, response, recovery model for the management of such critical incidents. Regional Offices, through the use of the Critical Incident Form, together with the DECS Customer Support Centre can direct schools and preschools to resources or personnel when additional support is required. Specialist advice can be accessed from State Office personnel.



Children online

DECS provides online services in government schools and preschools. The information about the policies and advice to be observed is organised in four sections:

- **Access and Security**
- **User Identification and Passwords**
- **Appropriate Behaviour and Use**
- **Acceptable Use Agreement**

School and preschool policy on the use of mobile technologies is to be informed and guided by existing DECS policies. Draft templates are available online at www.decs.sa.gov.au/speced2/pages/cybersafety/.

This also applies to misuse. For example, an act of cyber-bullying through text messaging or image exchange should be treated as a behaviour management issue and dealt with through the school behaviour code or preschool behaviour policy, with appropriate consequences, even if this incident was off the school or preschool site and/or out of school hours. However, if it involves, for example, suspected child pornography or threats to safety, it may constitute an e-crime, requiring police notification. E-crime occurs when a computer or other electronic communication device (eg mobile phone) is used to commit an offence, is targeted in an offence, or acts as a storage device in an offence. It is important that students understand that the production or distribution (including texting and posting) of lewd images of themselves or others may constitute child pornography with a potential criminal penalty. Suspected events must be referred to SAPOL with potential evidence confiscated and kept securely until given to a police officer. The school may suspend or suspend pending exclusion the student(s) involved in such events. The DECS Customer Support Centre can provide assistance in determining an appropriate response when any ICTs are misused. Your Regional Manager Support Service can provide advice in response to student behaviour management.

Access and Security

POLICY

DECS ICT Security and Internet Access and Use policies contain the following main provisions.

- Cyber-safety Use Agreements must be in place for all children and students. The age-appropriate agreement must be agreed to and signed by the child/student and his/her parents. Draft templates are available online at www.decs.sa.gov.au/speced2/pages/cybersafety/
- Children and students must use the Internet in a safe and considerate manner.
- Children and students must follow the copyright and licensing laws with respect to software, information and other material retrieved from or published on the Internet.
- Schools and preschools must make sure children, students and staff are aware of the importance of ICT security and safety, and how to properly react and deal with ICT security incidents and weaknesses.
- Schools and preschools must report to SAPOL if cyber behaviour is suspected to be an e-crime. The principal or director must also forward a Critical Incident Form to the regional director.
- Educators must make a mandatory notification to the Child Abuse Report Line (13 1478) if they suspect child abuse and neglect.

DECS, through Technology & Knowledge Management Services may record and monitor Internet use for the purposes of managing system performance, monitoring compliance with policies, or as part of disciplinary or other investigations. This applies to all users of DECS online services, including children, principals and directors, educators, ancillary staff, volunteers and supervisors of children and students in any DECS locations, including schools and preschools.

Responsibilities of Principals and Directors
Requirements - Summarised from Policy and Legislation

Principals and directors must:

- approve the posting of any information to Internet web pages, news groups, web-based forums etc. and ensure it conforms to minimum standards
- ensure that private information is not accessible on any publicly available web page. This includes the requirement that images should never include any names identifying any of the children/students in images
- gain written permission from parents before publishing video, photographs, comments or work samples of their child
- report to SAPOL any incident suspected to be an e-crime and provide to the investigating officer confiscated evidence. The following steps should be followed
    - Ensure the confiscated evidence is placed in a secure location
    - Do not open and view any evidence on an electronic device as this will compromise the evidence
    - Cease any further investigation
    - Complete and forward a Critical Incident Form.
- support staff members in making a mandatory notification if they suspect child abuse and/or neglect
- ensure that a developmentally appropriate child protection curriculum is being made available to every learner every year.

Recommendations - Good Practice Advice
Principals and directors should:

- inform parents and educators of the existence of these guidelines and the information provided by the Australian Communications and Media Authority (ACMA)
- provide a direct link from the school's or preschool's website to the websites of the ACMA, Kids Helpline and Bullying - No Way
- as an alternative to identifying children personally in photographs published online, identify only the school or preschool, or just describe the activity instead (eg 'children from Somewhere Area School performing at the Somewhere Show'). It is also recommended that only group photographs with subjects in standard school uniform or day clothing are used which show the least amount of children's faces (eg with their backs turned or heads down), unless signed consent has been obtained from the parent/guardian. A draft template is available online at www.decs.sa.gov.au/speced2/pages/cybersafety. Photographs of single individuals and of children and students in swimming attire or similar should be avoided
- advise parents that, while DECS will make every reasonable effort to provide a safe and secure online learning experience for children and students when using DECS online services, Internet filtering is not 100 per cent effective and it is not possible to guarantee that children and students will not be exposed to inappropriate material
- inform parents that Internet browsing by their child at home or from other non-DECS sites will not occur via DECS online services and therefore will not be filtered or monitored by DECS
- after highlighting learning opportunities and risks, gain written permission from parents before modifying Internet access safeguards, such as the Internet filtering, for targeted programs and projects
- ensure log-in scripts remind children, students and staff of their responsibilities when using DECS online services
- develop local procedures for the customisation of local Internet filtering. This should be done with care and due consideration. Instructions for schools and preschools about how to modify their local Internet filtering are included in the edADMIN User Guide
- encourage educators to attend the ACMA's Cybersafety Outreach Professional Development for Educators program. This professional development program aims to educate teachers on the potential risks associated with the Internet, such as identity theft, cyberbullying, scams and inappropriate contact and content. It also gives them the tools and confidence to engage children and young people on a range of related issues. Internet safety general awareness presentations are also available for parents and students. All presentations and resources are free of charge.

Responsibilities of Educators

Requirements - Summarised from Policy and Legislation

Educators must:

- observe a duty of care - this means they will take reasonable care to protect children and students from foreseeable risk of injury when using DECS online services
- provide appropriate supervision for children and students so that they comply with the practices designed for their own safety and that of others
- design and implement appropriate programs and procedures to ensure the safety of children and students
- teach children and students about dangerous situations, materials and practices
- fulfil their responsibilities to deliver child protection curriculum within whole of site planning for such delivery
- must make a mandatory notification to the Child Abuse Report Line if child abuse or neglect is suspected.

Recommendations - Good Practice Advice

Educators should:

- teach strategies for personal safety and advise children and students that they should not reveal personal or identifying information including names, addresses, financial details (eg credit card), telephone numbers or images (video or photographic) of themselves or others
- encourage children and students not to use their school e-mail address in non-school online communications as this e-mail address contains their personal name and school details
- teach responsibilities associated to intellectual property and copyright law and ethics, including acknowledging the author or source of information that is used
- teach topics and use resources contained in the *Keeping Safe: Child Protection Curriculum* introduced to schools and preschools in 2008
- attend the ACMA's free, accredited, interactive Cybersafety Outreach Professional Development for Educators program
- make use of a range of cyber-safety resources.

User Identification and Passwords

POLICY

DECS ICT Security and Internet Access and Use policies contain the following main provisions.

- To log on, children and students must use a unique user identification (user-ID) that is protected by a secure password.
- Passwords must be kept confidential and not displayed or written down in any form.
- Passwords must not be words found in a dictionary, or based on anything somebody else could easily guess or obtain using person-related information.
- Passwords must not be included in log-on scripts or other automated log-on processes.
- Children and students must not disclose their personal passwords to any other person. Where other users are authorised to use group user-IDs, the password must not be disclosed to unauthorised people.
- Children and students will be accountable for any inappropriate actions (eg bullying, accessing or sending inappropriate material) undertaken by someone using their personal user-ID.

The use of shared group user-IDs will occur only in special circumstances and only after approval from the principal or director.

Responsibilities of Principals, Directors and Educators Recommendations - Good Practice Advice

Principals and directors should:

- consider ways of maintaining confidentiality of child and students' passwords, with additional consideration given to younger children or those with special needs
- provide appropriate supervision for children and students using the Internet at school or preschool.

Appropriate Behaviour and Use

POLICY

DECS ICT Security, Internet Access and Use, and Electronic Mail and Use policies contain the following main provisions.

- Children and students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and children may not access or distribute inappropriate material. This includes:
    - distributing spam messages or chain letters
    - accessing or distributing malicious, offensive or harassing material, including jokes and images
    - bullying, harassing, defaming or giving offence to other people
    - spreading any form of malicious software (eg viruses, worms)
    - accessing files, information systems, communications, devices or resources without permission
    - using for personal financial gain
    - using non-approved file sharing technologies (eg Torrent)
    - using for non-educational related streaming audio or video
    - using for religious or political lobbying
    - downloading or sharing non-educational material.

All children and students must have annual access to developmentally appropriate child protection curriculum.

Recommendations - Good Practice Advice

Educators should:

- teach topics and use resources contained in the *Keeping Safe: Child Protection Curriculum* introduced to preschools and schools in 2008
- encourage children and students to inform a teacher if they come across inappropriate material or anything online that makes them feel uncomfortable
- teach strategies to manage online presence, protect identity through privacy settings, examine 'terms and conditions' associated with user agreements of Internet services, highlight the opportunities to report abuse or offensive online behaviour to the appropriate service provider or authority
- teach children and students (in an age appropriate way) how to identify and avoid inappropriate materials. These can include
    - pornography - both illegal and legal pornography. It is prevalent on the Internet and can be accessed through websites, sent as spam via e-mails, shared in peer-to-peer networks or sexting through mobile phone messaging
    - hate groups - including racial, religious, political, homophobic and other groups that are discriminatory
    - violence or illicit drugs - websites containing explicitly violent behaviour (like rape or assault), material regarding illicit drugs or inciting suicide, vigilante or violent groups' websites, and instructional websites (like weapon or bomb making)
    - illegal activity - content that promotes illegal activity (like copyright infringement on music), security breaches (like hacking) or fraudulent schemes online
    - extremist groups and cults - groups online that offer information about their extremist or cult activities, goals and missions; these groups can use the Internet to recruit new members or incite action
    - social networking - many social networking sites place children and students at some risk through exposing their identity, invading privacy and providing opportunities for bullying
    - online advertising - some online advertising can be inappropriate for children and students; the Internet is an inexpensive medium for advertisers and is therefore widespread
    - online gambling - websites which contain and promote gambling practices.

Cyber-safe Use Agreement

POLICY

DECS ICT Security policy and the DECS Standard - Acceptable Use Policies for Schools, Preschools and Children's Services Sites contain the following main provisions regarding acceptable use policies and agreements.

- Cyber-safety Use Agreements must be in place for all children and students who use DECS online services.
- Policies must be implemented in the form of written agreements, signed by staff and children/students and/or their parents.
- Agreements may be modified by the school or preschool but they must outline the key terms and conditions of use of DECS online services, online behaviour and access privileges, and the consequences of non-compliance.
- These agreements must be reviewed and updated regularly to ensure their appropriateness and effectiveness.

Policies must be regularly reinforced to all users.

Responsibilities of Schools and Preschools

Recommendations - Good Practice Advice

Principals and directors should:

- create and implement age appropriate Cyber-safety Use Agreements that
    - involve young people in the authoring of such an agreement and a commitment to personal and cyber-safe learning environments, for themselves and others regardless of age. Draft templates are available online at www.decs.sa.gov.au/speced2/pages/cybersafety/
    - are read, understood and signed by children/students and/or their parents
    - reinforce the fact that the agreement is taken seriously and is part of the partnership between school or preschool and home
    - clearly describe strategies for personal safety and privacy (eg children and students must not give out identifying information online, use only their first name, and not share their home address, telephone number or any other personal information)
    - make clear that children and students should never respond to message or bulletin board items that are suggestive, obscene, belligerent, threatening or make them feel uncomfortable, and that these messages should be reported to a teacher. Specific examples of unacceptable behaviour could be included, such as 'I will not respond to any messages that are inappropriate, unpleasant or that make me feel uncomfortable in any way and I will tell my teacher immediately' and 'I will click on the HOME button and tell my teacher immediately if I see anything on a website that is inappropriate, unpleasant or makes me feel uncomfortable'
    - for younger children, are signed by the parent/s, who agree to ensure their child is aware of personal safety strategies
    - for older children and students, outline the expectation that they take increasing responsibility for their own actions by agreeing to use DECS ICT facilities in a responsible manner, but with parents acknowledging on the agreement the responsibility their child undertakes
    - are linked to the policies, goals and objectives of the school or preschool, particularly in relation to the purposes of providing ICT facilities and services
    - are visible in school or preschool life (eg included in child/student's diaries, put on log-in splash screens and on the intranet, printed as an occasional reminder in school newsletters, and displayed in learning areas)
    - include the potential consequences of unacceptable use, such as removal of access to school or preschool ICT facilities, suspension or exclusion from school or referral to SAPOL
    - include DECS policies on what information might be recorded from a child/student's online services use and who has access to this information
    - are signed and a copy of the agreement is placed in the child/student's file for reference.

Responsibilities of Educators
Recommendations - Good Practice Advice

Educators should:

- keep up to date about the relative risk and educational benefit of online activity in learning programs
- check that any material planned for publication on the Internet or intranet has the approval of the principal or director, as per the DECS ICT Security policy, and meets copyright and privacy requirements
- be aware of the steps to take and advice to give if children and students notify them of inappropriate or unwelcome activity online by other children/students or members of the public; such steps may include:
    - collecting as much information as possible about the incident, including copies of communications
    - emphasising to the children and students that the event is not necessarily their fault
    - identifying any risky behaviour on the part of the reporting child or student and counselling them on the need to adopt more protective behaviour
    - if the incident warrants further attention, escalating it to school or preschool and/or department authorities as per the DECS policies.
- be involved in the development, approval and signing of a Cyber-safety Use Agreement which suits local needs and is consistent with the DECS Standard - Acceptable Use Policies for Schools, Preschools and Children's Services Sites and Code of Ethics for the South Australian Public Sector.
- ensure that their 'digital footprints' from their personal online identities, including social networking sites, are consistent with the role of educators, the Code of Ethics for the South Australian Public Sector and the Teacher Registration Board of South Australia's Code of Ethics for the Teaching Profession in South Australia.

Legislation and Guidelines

These guidelines have been informed by relevant sections of the following SA Government Legislation and associated DECS policies and guidelines:

Broadcasting Services Act, 1992
http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401834?OpenDocument

Children's Protection Act 1993
http://www.legislation.sa.gov.au/LZ/C/A/CHILDRENS%20PROTECTION%20ACT%201993.aspx

Classification (Publications, Films and Computer Games) Act 1995
http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401401?OpenDocument

Copyright Act, 1968
Australian Government summary at
http://www.ag.gov.au/www/agd/agd.nsf/page/Copyright

Copyright Amendment (Digital Agenda) Act 2000
Australian Government summary at
http://www.ag.gov.au/www/agd/agd.nsf/Page/Copyright_IssuesandReviews_CopyrightAmendmentAct2006

Copyright Amendment (Moral Rights) Act 2000
Australian Government summary at
http://www.ag.gov.au/www/agd/agd.nsf/Page/Copyright_IssuesandReviews_Moralrights

Education Act 1972
http://www.legislation.sa.gov.au/LZ/C/A/EDUCATION%20ACT%201972/CURRENT/1972.154.UN.PDF

Education Regulations 1997
http://www.legislation.sa.gov.au/LZ/C/R/EDUCATION%20REGULATIONS%201997.aspx

Information Privacy Principles Instruction
http://www.archives.sa.gov.au/privacy/principles.html

DECS Policies and Government Guidelines

Acceptable Use Policies for Schools, Preschools and Children's Services Sites
http://www.decs.sa.gov.au/docs/documents/1/DecsStandardAcceptableUse.pdf

Bullying and Harassment at School: Advice for parents and caregivers
http://www.decs.sa.gov.au/speced2/files/links/link_97419.pdf

Child Protection
http://www.decs.sa.gov.au/speced2/default.asp?navgrp=childprotection

Child Protection Information for Parents/Caregivers
http://www.decs.sa.gov.au/curric/files/links/CP_ENGLISH.pdf

Choosing and Using Teaching and Learning Materials
http://www.decs.sa.gov.au/policy/default.asp?id=16717&NAVGRP=61

Code of Ethics for the South Australian Public Sector
http://www.decs.sa.gov.au/HR1/pages/default/CodeOfEthics/

Computer Security Awareness for School, Preschool and Children's Services Staff
http://www.decs.sa.gov.au/docs/documents/1/BrochureComputerSecurit-1.pdf

Critical Incident Report
http://www.decs.sa.gov.au/docs/documents/1/CriticalIncidentReport.doc

Cyber Bullying, E-crime and the Protection of Children
http://www.decs.sa.gov.au/docs/documents/1/CyberBullyingECrimeProtec.pdf

DECS A–Z of Policies, Procedures and Guidelines
http://www.decs.sa.gov.au/policy/default.asp?navgrp=OSPP&id=policy_index

DECS Standards - School/Preschool Websites
http://www.decs.sa.gov.au/docs/documents/1/SiteWebStandards.pdf

Duty of Care
http://www.decs.sa.gov.au/docs/documents/1/DutyofCare.pdf

Electronic Mail and Use Policy
http://www.decs.sa.gov.au/docs/documents/1/DecsPolicyEmailAccessandU.pdf

How to Report an ICT Security Incident or Threat
http://www.decs.sa.gov.au/docs/documents/1/DecsProcedureHowtoReporta.pdf

ICT Security
https://ssonet.central.sa.edu.au/it_support/pages/csc/security/

ICT Security Policy
http://www.decs.sa.gov.au/docs/documents/1/DecsPolicyIctSecurity

Internet Access and Use Policy
http://www.decs.sa.gov.au/docs/documents/1/DecsPolicyInternetAccessa.pdf

National Education Access Licence for Schools (NEALS)
http://www.decs.sa.gov.au/docs/documents/1/CopyrightGuidelinesNation.pdf

National Safe Schools Framework
Safe Schools (Australian Government) website
http://www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/overview.aspx

Protective Practices for Staff in their Interactions with Children
http://www.decs.sa.gov.au/docs/documents/1/ProtectivePracticesforSta.pdf

Reducing Bullying in Schools: A Professional Development Resource
Provided to all DECS schools in 2004 (not available online)

School Discipline Policy
http://www.decs.sa.gov.au/docs/documents/1/SchoolDisciplinePolicy.pdf

Student Online Policy
http://www.decs.sa.gov.au/portal/aboutdept.asp?group=Aboutdept&id=policy

Supporting and managing children's behaviour: An early childhood resource
http://www.schools.sa.gov.au/speced/files/links/link_61315.pdf

Glossary of Terms

There are important terms used in this document:

'Children and students' denotes all learners enrolled in DECS schools and preschools who are minors.

'Parent' used throughout this document refers to natural parents, legal guardians and caregivers.

'ICTs' in this document refers to 'information and communication technologies'.

'Cyber-safety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

'Cyber bullying' is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person. Examples include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

'Digital footprints' are traces left behind by someone's activity in a digital environment. These traces can be analysed by a network manager or the police.

'Sexting' is where a person takes a sexually-explicit digital photograph of him or herself or of someone else, and sends it as an MMS and SMS via a mobile phone. These images can then be posted on the internet or forwarded electronically to other people. Once posted on the internet these images can leave a permanent digital footprint and be accessed at any time in the future. It is illegal to take sexual photos or videos of children and young people.

'Social networking' sites offer people new and varied ways to communicate via the Internet, whether through their computer or mobile phone. These sites allow people to easily and simply create their own online page or profile and to construct and display an online network of contacts, often called 'friends'. Users are able to build a network of connections that they can display as a list of friends. These friends may be offline actual friends or acquaintances, or people they know or have 'met' only online, and with whom they have no other link. Social networking sites are not limited to messaging, communicating and displaying networks. Nearly all sites allow users to post photos, video and often music on their profiles and share them with others.

'School and preschool ICT' refers to the school's or preschool's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

'ICT equipment/devices', as used in this document, includes but is not limited to computers (such as desktops, laptops, netbooks, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies.

'Inappropriate material' in this document means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

'E-crime' occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence. For examples of what constitutes an e-crime, please refer to the Cyber Bullying, E-crime and the Protection of Children parent brochure.

Additional Information & References

The following brochure produced by DECS may be a useful reference and/or handout to children and their parents:

Cyber bullying, e-crime and the protection of children brochure, available at
http://www.decs.sa.gov.au/docs/documents/1/CyberBullyingECrimeProtec.pdf

For further advice, direction or to report an ICT security incident or threat, contact the DECS Customer Support Centre:
Telephone: Metropolitan 08 8204 1866, Country 1300 363 227
E-mail: csc@saugov.sa.gov.au

Alternatively, refer to the How to Report an ICT Security Incident or Threat Within DECS procedure, available at
http://www.decs.sa.gov.au/docs/documents/1/DecsProcedureHowtoReporta.pdf

For further advice regarding learner behaviour or learner wellbeing, contact the Manager Regional Support Services in your region.

Specialist advice can be accessed through senior policy advisors attached to the following DECS directorates:
Curriculum (eg Child Protection Curriculum Officer)
Schools and Regional Operations (eg Student Behaviour Management and Child Protection Policy Advisors)
Technology and Knowledge Management Services (eg Learning Technologies and Customer Support Centre).

Customer Support Centre
Telephone: Metropolitan 8204 1866, Country 1300 363 227
E-mail: csc@saugov.sa.gov.au

edADMIN User Guide
http://www.educonnect.sa.edu.au/educonnect/files/links/EdAdmin_User_Guide_v_2_9.pdf

Australian Communications and Media Authority (ACMA)
http://www.acma.gov.au/cybersafety

Bullying No Way http://www.bullyingnoway.com.au/

Code of Ethics for the Teaching Profession in South Australia
http://www.trb.sa.edu.au/pdf/Code%20of%20Ethics%20A4.pdf

Creative Commons copyright licensing http://creativecommons.org/

Cyber bullying stories http://www.cyberbullyingstories.org.au/

CyberNetrix http://www.cybernetrix.com.au/

CyberQuoll http://www.cyberquoll.com.au/

Cybersmart Detectives http://cybersmart.engagelive.net/

Cybersmart Kids Online http://www.cybersmartkids.com.au/

Cybersmart materials for public libraries http://www.acma.gov.au/libraries

Equal Opportunity for Schools 'EO 4 Schools' http://www.eo4schools.net.au/

Kids Helpline http://www.kidshelp.com.au/

NetAlert website http://www.netalert.gov.au/

NetAlert education programs http://www.netalert.gov.au/programs.html

NetSafe (New Zealand) http://www.netsafe.org.nz/

Parenting SA http://www.parenting.sa.gov.au/

Safe Schools (Australian Government website)
http://www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/overview.aspx

Smartcopying http://www.smartcopying.edu.au/

Stay Smart Online http://www.staysmartonline.gov.au/

Super Clubs PLUS Australia http://www.superclubsplus.com.au/

WiseuptoIT http://www.wiseuptoit.com.au/

Local Cyber-safety Policies and Use Agreements

Attach Here