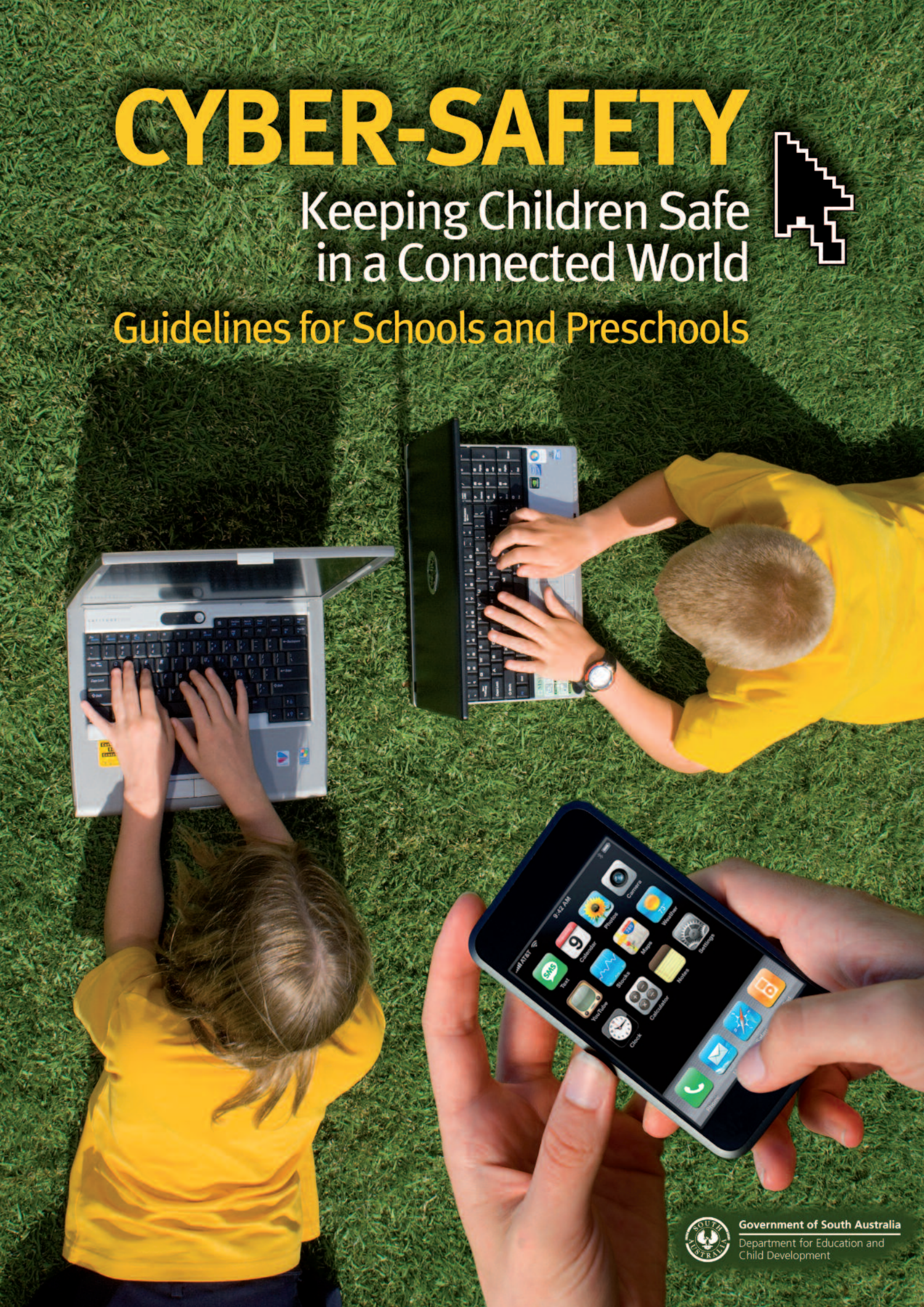
CYBER-SAFETY

Keeping Children Safe in a Connected World

Guidelines for Schools and Preschools



Government of South Australia
Department for Education and Child Development

CYBER-SAFETY

Keeping Children Safe in a Connected World

Guidelines for Schools and Preschools

Government of South Australia
Department for Education and Child Development

Authorised by the Department of Education and Child Developemnt
31 Flinders Street
Adelaide
South Australia 5000
June 2009
Revised December 2011

© Minister for Education and Child Development for and on behalf of the Crown in right of the State of South Australia

The copyright of this document is owned by the Government of South Australia (Department for Education and Child Development (DECD)), or in the case of some materials, by third parties (third party materials). No part may be reproduced by any process except in accordance with the provisions of the Copyright Act 1968, the National Education Access Licence for Schools (NEALS) (see below) or with permission.

NEALS

An educational institution situated in Australia which is not conducted for profit, or a body responsible for administering such an institution, may copy and communicate the materials, other than third party materials, for the educational purposes of the institution.

Grateful acknowledgment is made of material provided by:
Department of Education and Training, Western Australia for 'Students 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 December 2011

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

Government of South Australia
Department for Education and Child Development

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 Child Development (DECD) 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, *Responding to abuse and neglect: Education and care training, Protective Practices for Staff in their Interactions with Children and Young People:, Safer DECD schools* 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 DECD schools and preschools.

Since their release in 2009, the guidelines have been positively received and utilised by education leaders. This second edition provides revisions reflecting the updating and developments in child protection initiates and the changing world of young people's use of modern technologies.

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

Keith Bartley
Chief Executive

Contents

Introduction 6

Cyber-safety Guidelines 7

Child Protection 9

Children Online 11

- Access and Security 12
- User Identification and Passwords 16
- Appropriate Behaviour and Use 17
- Cyber-safe Use Agreement 18

Relevant Legislation and DECD Policies and Guidelines

- South Australian and Australian Government Legislation 20
- DECD Policies and Guidelines 21

Glossary of Terms, Additional Information and References 22

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 for Education and Child Development (DECD) 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 DECD 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, the training of DECD staff and volunteers in *Responding to abuse and neglect* and policy requirements as outlined in *Safer DECD Schools*.

Research shows schools are one of the safest environments for children.[2] DECD 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 when accessing DECD on line services
- providing direction and advice about ICT equipment and devise 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.
- *Responding to abuse and neglect: Education and care training*
- *Safer DECD Schools* which outlines the DECD requirements and recommended practice in support of the National Safe Schools Framework (updated 2011)
- DECD Social networking Policy
- DECS *Sexual Harassment Prevention Policy*
- 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. The Coalition is supporting the *Safer DECD Schools* with information on their website at http://www.decd.sa.gov.au/speced2/pages/bullying/saferschools/

1. Department for Education and Child Development (DECD) (2008) *Keeping Safe: Child Protection Curriculum.* [5 bands] Adelaide, DECS.
2. National Safe Schools Framework (2011). Accessed at: http://www.deewr.gov.au/Schooling/NationalSafeSchools/Documents/NSSFramework.pdf

Cyber-safety Guidelines

There is a range of legislation and policy that schools and preschools need to observe to ensure cyber-safety, listed in this document. Many of the principles covered in the non-ICT-specific government Acts and DECD policies, such as the *Children's Protection Act* 1993 and the DECD 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 in front of the screen, are subject to the same expectations schools and preschools have always applied.

It should be noted that these guidelines apply to DECD staff, children and students accessing online services in any DECD 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 whilst taking further advice from the SAPOL investigation officer.

The *Cyber bullying, e-crime and the protection of children and young people: Advice for families* provides information for parents/caregivers regarding these issues. This pamphlet is available at http://www.decd.sa.gov.au/speced2/files/pages/Cyber%20safety/Cyber_Bullying_2010.pdf

The flowchart on the following page 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 and State Offices, through monitoring the Incident & Response Management System, together with the DECD 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.

Cyber – Safety Guidelines to assist in decision making

A cyber-safety incident has occurred. (This could occur on or off-site and/or out of school hours.)

Yes

Is this a suspected e-crime?

An e-crime can include sexting, using someone else's electronic account to send abusive comments (impersonation), intimidation/ blackmail, offensive and/or untrue material about a person is (defamation), harassment (sexual and racial), transmitting suicide-related material, uploading images of an assault onto social networking sites or making a threat.

Yes →

- Contact SAPOL – 131 444 and follow their advice. Document actions.
- Contact Regional Office & School Care 8463 6564.
- If an electronic device is involved (e.g. mobile phone, iPad), confiscate or keep the evidence and secure to provide it to the SAPOL investigating officer. Do not open and view any evidence on an electronic device as this may compromise the investigation.
- Cease any further investigation of the e-crime, proceed with behaviour management processes (suspension or exclusions under Regulation 41.1.c.)
- Complete and forward Critical Incident Report.

If Police do not proceed because it is not an e-crime, implement site based student behaviour.

No

And/or is this a suspected child protection issue?

Yes → Contact Child Abuse Report Line (CARL) 13 13 78 and where appropriate, Regional Office and submit a Critical Incident Report (IRMS).

No

Is the incident a breach of DECD ICT security?

Yes →

- Report incident without specific details to DECD Customer Support Centre 8204 1866 (Metro) or 1300 363 227 (Country).
- Do not divulge specific information until contacted by ICT Security Team leader or their delegate and follow their instructions.
- All incidents and matters must remain confidential.

No

Does the incident affect the wellbeing of a student or teacher and require a suspension or exclusion under Regulation 41.1.b?

Yes →

- As part of the suspension or exclusion conference, where the police are not involved, include negotiation to permanently remove materials to ensure a feeling of safety for the person who was harassed/ bullied.
- In the event that the student and his/her family refuse to cooperate in the removal of images, seek advice from DECD Legislative and Legal unit 8226 1555 and/or advise student/parents seeking the removal of images to use the complaint processes of the social networking services.

No

Implement other site-based behaviour management process.

Review site-based policies and processes including implementation of the *Keeping Safe* child protection curriculum.

Incident resolved

All site-based policies and procedures reviewed at least every two (2) years and the school's anti-bullying policy annually.

Regional Offices together with School Care can provide additional support if required.

Child Protection

Education and care programs play a significant role in child protection. Child abuse on line or off line and neglect negatively affects a child's or young person's emotional, intellectual and social development. It is vital that child protection risks are identified, protected against and responded to appropriately. The framework for doing this in education and care settings involves two major areas of focus: curriculum for children and young people and professional learning for adults.

Curriculum

The *Keeping Safe child protection curriculum* is an age and developmentally appropriate teaching program for use with children and students from the early years to senior schooling. Its four focus areas are:

- The Right to be Safe
- Relationships
- Recognising and Reporting Abuse
- Protective Strategies.

The core focus of the *Keeping Safe child protection curriculum* is to educate children and students about how to recognise abuse and protect themselves from it. More broadly, however, the curriculum has a focus on rights, responsibilities, relationships and ethical behaviour as core building blocks for children and students to build the skills that will help them recognise and protect themselves from abuse.

Teaching respectful relationships to children and students makes an important contribution to increasing protective factors and decreasing bullying, harassment and violence in schools. Both bullying and cyber-bullying are ultimately relationship issues that require relationship-focused solutions (Pepler 2006).

Professional learning

All staff members in education and care settings undertake mandatory pre- and in-service training titled *Responding to abuse and neglect: Education and care (RAN-EC) training*. Used across the government and non-government education and children's services sectors, this training aims to give staff an understanding of:

- what underlies child abuse and neglect and its impact on children's development and wellbeing
- how staff can help prevent and lessen the impact of abuse and neglect through their daily work with children and young people.

A primary protective factor for all children and young people is a safe and respectful learning environment and this forms the core of the *Responding to abuse and neglect: Education and care (RAN-EC) training* professional learning program.

Supporting child protection policies, guidelines and programs

- *Protective practices*[1] *for staff in their interactions with children and young people: Guidelines for staff working or volunteering in education and care settings* – a framework for the establishment of positive, caring and respectful relationships between adults and children and young people in education and care settings
- *Suicide postvention guidelines*[2] – a framework to assist staff in supporting their school communities in responding to suspected, attempted or completed suicide
- *Information sharing: Guidelines for promoting the safety and wellbeing of children, young people and their families*[3] – a framework for information sharing between all government agencies and relevant non-government agencies
- *Responding to problem sexual behaviour in children and young people: Guidelines for staff in education and care settings*[4] – a framework to assist education and care staff to respond effectively to incidents of problem sexual behaviour involving children and young people
- *SMART: Strategies for Managing Abuse Related Trauma professional learning for staff*[5,6] – a professional learning program designed to enhance the capacity of school and early childhood personnel to effectively respond to the needs of children and young people who have experienced abuse and trauma

1. http://www.decd.sa.gov.au/docs/documents/1/ProtectivePracticesforSta.pdf
2. http://www.crisis.sa.edu.au/pages/EM05/30674/
3. http://www.decs.sa.gov.au/docs/documents/1/InformationSharingGuideli.pdf
4. Refer to Appendix 1 (p 34) for a prevention checklist http://www.decs.sa.gov.au/docs/documents/1/RespondingtoProblemSexual.pd
5. http://www.decd.sa.gov.au/speced2/pages/childprotection/cpProfessionalDevelopment/

The 2011 update of the *Protective Practices for Staff in their Interactions with Children and Young People* is specific about violations of professional boundaries in relation to on line communications. These include the following:

Boundary	Example of violation
Communication	Correspondence of a personal nature via any medium (eg phone, text message, letters, email, internet postings) that is unrelated to the staff member's role. This does not include class cards/bereavement cards etc
Place	Allowing children and young people access to a staff member's personal internet locations (eg social networking sites)

In addition a section on Using social networking sites is included in the *Protective Practices* document. It states;

Staff in education and care settings are expected to model responsible and respectful conduct to the children and young people with whom they work. Staff need to consider the electronic social environments they utilise as part of this community and employer expectation.

The internet does not provide the privacy or control assumed by many users. Staff must appreciate that no matter what protections they place around access to their personal sites their digital postings are still at risk of reaching an unintended audience and being used in ways that could complicate or threaten their employment. Staff should be aware of the following expectations in considering their use of social networking sites:

- they have considered the information and images of them available on their sites and are confident that these represent them in a light acceptable to their role in working with children and young people
- they do not have children or young people in their education community as 'friends' on their personal/private sites
- comments on their site about their workplace, work colleagues or children or young people, if published, would not cause hurt or embarrassment to others, risk claims of libel, or harm the reputation of the workplace, their colleagues or children and young people.

Children online

DECD 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 DECD policies. 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 (131 444) with potential evidence confiscated and kept securely until given to a police officer whilst taking further advice from the SAPOL investigating officer. Educators must make a mandatory notification to the Child Abuse Report Line (13 1478) if they suspect child abuse or neglect.

The school may suspend or suspend pending exclusion the student(s) involved in a suspected e-crime or where their behaviour affects the wellbeing of a student teacher or parent even if off site provided the principal believes on reasonable grounds that the student has

- threatened or perpetrated violence or
- acted in a manner that threatens the safety or well being of a student or member of staff of, or other person associated with, the school or
- interfered with the ability of a teacher to instruct students or
- acted in a manner that threatens the good order of the school.

It is advisable not to use 'acting illegally' whilst the SAPOL investigation is ongoing.

Examples of scenarios are available on the DECS website at http://www.decd.sa.gov.au/speced2/pages/cybersafety/scenarios/ This document could support schools in their decision making in regard to cyber events.

The *Keeping Safe Child Protection Curriculum* is the DECD curriculum response to child protection which provides information to children and young people so they understand how to remain safe including on line. This curriculum is enhanced by resources available from the Australian Communication and Media Authorities' (ACMA) cybersmart website at www.cybersmart.gov.au

The DECD Customer Support Centre can provide assistance in determining an appropriate response when any ICTs are misused. Your Regional Manager Student Support can provide advice in response to student behaviour management.

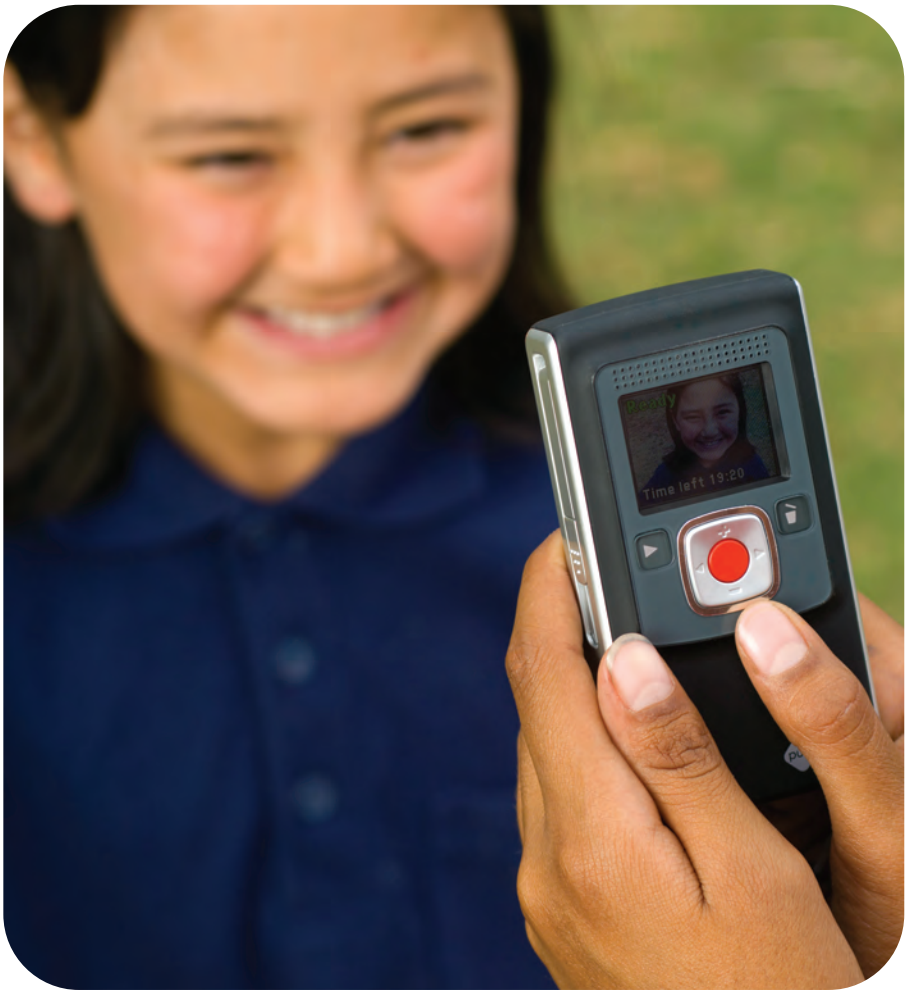
Access and Security

POLICY

DECD 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 (131 444) if cyber behaviour is suspected to be an e-crime. The principal or director must make an entry on the Incident & Response Management System (IRMS).
- Educators must make a mandatory notification to the Child Abuse Report Line (13 1478) if they suspect child abuse or neglect.

DECD, 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 DECD online services, including children, principals and directors, educators, ancillary staff, volunteers and supervisors of children and students in any DECD location, 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 or has embedded Global Positioning System (GPS) coordinates in an image that can be used to locate a child or young person. Digital photos with GPS data embedded will need to be reformatted prior to use on the schools website. Advice can be accessed at http://www.decd.sa.gov.au/speced2/pages/cybersafety/digitalphotos/
- gain written permission from parents before publishing video, photographs, comments or work samples of their child using the DECS Permission Form available at http://www.decs.sa.gov.au/docs/documents/1/CybersafetyPermissiontoPu.doc or for adults at http://www.decs.sa.gov.au/docs/documents/1/CybersafetyPublishImageso.doc

If there is a suspected e-crime;

- Report incident to SAPOL 131 444 and follow their advice. Document actions.
- Confiscate the equipment (eg mobile phone) and hand over to the SAPOL investigating officer
- Do not open or view any evidence as this may compromise the investigation.
- Cease any further investigation of the e-crime
- Contact Regional Office and School Care 8463 6564. Submit a Critical Incident Report (IRMS).
- If SAPOL do not proceed with the investigation treat the incident as a student behaviour management issue
- Where the incident is perpetrated by a student and affects the wellbeing of other students or staff members, leaders should follow the school discipline procedures. (See CE Circular DECS 09/3677)

Where violence or the electronic recording of violence is involved then an appropriate leader in the school is required to

- notify the parent(s) or caregiver(s) or nominated contact person of the victim at the earliest possible time
- telephone the Regional or Assistant Regional Director and School Care informing them of the incident
- 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.
- ensure that an easily locatable and well publicised link on the school website to the relevant anti-bullying policy or antibullying section within an existing policy is available. This is to link to the schools' resolution process for bullying.

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
- Place on all school computers the Australian Government's Cybersafety Help Button which provides information and assistance on cybersafety issues for children. This Help Button is available at http://www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_download
- 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 template is available online at http://www.decs.sa.gov.au/docs/documents/1/CybersafetyPermissiontoPu.doc.
  Photographs of single individuals and of children and students in swimming attire or similar should be avoided
- advise parents that, while DECD will make every reasonable effort to provide a safe and secure online learning experience for children and students when using DECD 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, from other non-DECD sites and via mobile devises belonging to the student whilst at school will not occur via DECD online services and therefore will not be filtered by DECD
- 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 at http://www.educonnect.sa.edu.au/educonnect/files/links/EdAdmin_User_Guide_v_2_9.pdf
- encourage educators to attend the face to face ACMA's Cybersafety Outreach Professional Development for Educators program or to access the equivalent online training program (Connect.*ed*). 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.
- be aware of the advice provided in
  - *Making Our Sites Safer: E-Crime Guidelines for Site Leaders* at http://www.decs.sa.gov.au/speced2/files/links/MossECrime_1.pdf
  - the Chief Executive's statement on *Can Principals suspend or exclude students for cyber events beyond the school gate* at http://www.decs.sa.gov.au/speced2/files/links/Cyber_bullying.pdf
  - the child protection documents listed in this document
  - The Safer DECD Schools at http://www.decd.sa.gov.au/speced2/pages/bullying/saferschools/

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 in order for them to become a responsible digital citizen
- 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 enhanced by resources available from the Australian Communication and Media Authorities' (ACMA) cybersmart website at www.cybersmart.gov.au
- attend the ACMA's free, accredited, interactive Cybersafety Outreach Professional Development for Educators program or complete the equivalent training on line (Connect.*ed)*.

User Identification and Passwords

POLICY

DECD 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 such as pet names, middle names, nick names or street names.
- 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

DECD 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 supported by resources available from ACMA and their website www.cybersmart.gov.au
- familiarise students with the Australian Government's Cybersafety Help Button which provides information and assistance on cybersafety issues for children. This Help Button is available at http://www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_download
- Support the school in placing on all school computers the Australian Government's Cybersafety Help Button.
- 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. Advice on removal of comments on social network sites can be accessed at http://www.decd.sa.gov.au/speced2/pages/cybersafety/socnetadvice/
    - 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

DECD 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 DECD 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 and consideration as to when and for what purpose student owned technology can be used on the school site
  - 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 DECD 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 DECD 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 DECD policies.
- be involved in the development, approval and signing of a Cyber-safety Use Agreement which suits local needs and is consistent with the DECD 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*.
- be familiar with this policy document and the information in *Protective Practices for Staff in their Interactions with Children and Young People: Guidelines for staff working or volunteering in education and care settings* available at http://www.decd.sa.gov.au/docs/documents/1/ProtectivePracticesforSta.pdf

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 2006
Australian Government summary at
http://www.ag.gov.au/www/agd/agd.nsf/Page/Copyright_IssuesandReviews_CopyrightAmendmentAct2006

Copyright Amendment (Moral Rights) Act 2007
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.aspx

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

Policies and Government Guidelines

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

Advice on removal of comments on social network sites
http://www.decd.sa.gov.au/speced2/pages/cybersafety/socnetadvice/

Bullying and Harassment at School: Advice for parents and caregivers
http://www.decd.sa.gov.au/speced2/files/links/Bullying_Brochure_DEC_1.pdf

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

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

Choosing and Using Teaching and Learning Materials
http://www.decd.sa.gov.au/policy/files/links/Choose_use_booklet_FA.pdf

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

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

Critical Incident Report available on the Incident & Response Management System (IRMS)
http://www.decd.sa.gov.au/hrhealthsafety/pages/incident/irms/

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

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

DECD Permission Form (to use media in which children appear or whose written comments or student work samples is to be published) http://www.decs.sa.gov.au/docs/documents/1/ConsentFormChild.pdf

DECD Permission Form (to use media in which adults appear or whose written comments or student work samples is to be published) http://www.decs.sa.gov.au/docs/documents/1/ConsentFormAdult.pdf

DECD Standards – School/Preschool Websites http://www.decd.sa.gov.au/docs/documents/1/SiteWebStandards.pdf

Digital Photos/GPS http://www.decd.sa.gov.au/speced2/pages/cybersafety/digitalphotos/

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

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

Example Scenarios http://www.decd.sa.gov.au/speced2/pages/cybersafety/scenarios/

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

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

Making Our Sites Safer: E-Crime Guidelines for Site Leaders
http://www.decd.sa.gov.au/speced2/files/links/MossECrime_1.pdf

National Education Access Licence for Schools (NEALS) http://www.decd.sa.gov.au/services/pages/leglegal/copyright/

National Safe Schools Framework
Safe Schools (Australian Government) website
http://www.deewr.gov.au/Schooling/NationalSafeSchools/Documents/NSSFramework.pdf

Protective Practices for Staff in their Interactions with Children
http://www.decd.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)

Safer DECD schools http://www.decd.sa.gov.au/speced2/default.asp?id=42827&navgrpp=3195

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

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 DECD 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/CyberBullyingECrimeandthe.pdf

For further advice, direction or to report an ICT security incident or threat, contact the DECD 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 DECD 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 DECD 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) Cybersmart website
http://www.acma.gov.au/cybersafety

Budde Stay Smart On Line https://budd-e.staysmartonline.gov.au/index.html

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

Code of Ethics for the Teaching Profession in South Australia
http://www.trb.sa.edu.au/code_of_ethics.php

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

CyberNetrix http://www.cybersmart.gov.au/cybernetrix

CyberQuoll http://www.cybersmart.gov.au/cyberquoll

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

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

Cybersafety help button download page
http://www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_download

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

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

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/

Think U Know http://www.thinkuknow.org.au/

WiseuptoIT http://www.cybersmart.gov.au/wiseuptoit/

Local Cyber-safety Policies and Use Agreements

Attach Here

Government of South Australia
Department for Education and Child Development