Government of South Australia
Department for Education and Child Development

Long Street Primary School
Growing Together

NAME OF POLICY	CYBER SAFETY POLICY
RATIONALE	This policy is designed to give students the tools to deal with and manage a variety of issues they may encounter while accessing online resources.
PUBLICATION DATE	MAY 2017
REVIEW DATE	MAY 2019
RELATED POLICY	Cyber-Safety: Keeping Children Safe in a Connected World

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.

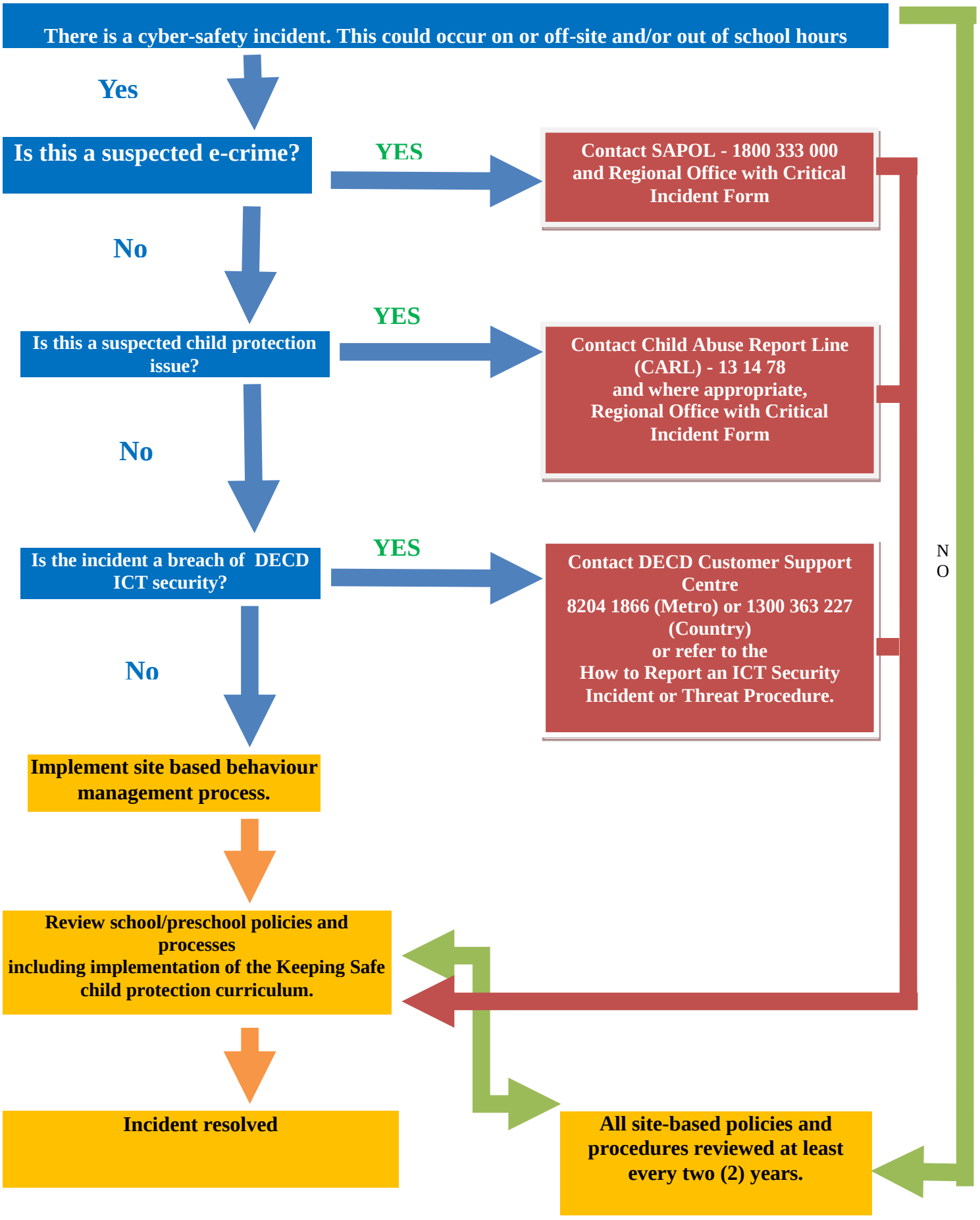
The Department of Education and Child Development (DECD) invests in network systems to manage and protect the welfare of children. However, the explosion of wireless and mobile devices allows children to bypass conventional network systems. This has the potential to expose young people to risks previously 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, 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.

In matters relating to cyber-safety, DECD 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.


There is a cyber-safety incident. This could occur on or off-site and/or out of school hours
Yes
Is this a suspected e-crime?
YES
Contact SAPOL - 1800 333 000 and Regional Office with Critical Incident Form
No
Is this a suspected child protection issue?
YES
Contact Child Abuse Report Line (CARL) - 13 14 78 and where appropriate, Regional Office with Critical Incident Form
No
Is the incident a breach of DECD ICT security?
YES
Contact DECD Customer Support Centre 8204 1866 (Metro) or 1300 363 227 (Country) or refer to the How to Report an ICT Security Incident or Threat Procedure.
No
Implement site based behaviour management process.
Review school/preschool 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.
NO

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.decd.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.
- 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 locations, including schools and preschools.

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
- Make use of a range of cyber-safety resources.

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.

Cyber-safe Use Agreement

DECD ICT Security policy and the DECD 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 DECD 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 DECD 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.

Glossary of Terms

There are important terms used in this document:

'Children and students' denotes all learners enrolled in DECD 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.