Government
of South Australia

Department for Edu

G

of

of South Australia

RESPONDING TO ONLINE SAFETY INCIDENTS IN SOUTH AUSTRALIAN SCHOOLS.

This guideline is a recommended course of action under the operational policy framework. South Australian schools should use this guideline to inform responses to online safety incidents.

BACKGROUND

Children and young people have the opportunity to learn and thrive through the use of digital technology. Positive and safe engagement in the digital world can support healthy development, creating positive opportunities for children and young people. However, it may also introduce risks. Children and young people are developing their skills in assessing information, weighing up risks and taking steps to protect themselves. Until these skills are fully developed, they have an increased level of vulnerability online and need adult guidance and support.

South Australian schools are child safe organisations. Education communities work across sectors, organisations and settings to keep children and young people safe online, and respond to online safety incidents. The goal is to improve the quality of online experiences for children and young people. It is to encourage their safe engagement in the digital world by building their skills and knowledge so they can fully participate as global citizens.

OVERVIEW

These guidelines are for the government, Catholic and independent education sectors. They are written for educators, school principals and other professionals who have responsibility to establish and maintain safe and inclusive learning environments for children and young people.

The purpose of these guidelines is to help school staff to:

- respond consistently to online safety incidents
- recognise which online incidents need to be escalated for additional support
- identify which online safety incidents need cross sectoral and interagency coordination.

SCOPE

The guidelines apply to online safety incidents involving children and young people who are under the care and control of teachers. The incidents relate to behaviour by children and young people and adult behaviour targeted at children and young people.

Online safety incidents that involve allegations of staff member misconduct are not covered by these guidelines. Cross sector guidelines for staff interactions with children and young people and staff sexual misconduct are:

- protective practices for staff in their interactions with children and young people
- managing allegations of sexual misconduct in SA education and care settings guidelines.

- nature of the child or young person’s behaviour
- child protection concerns
- behaviour may be illegal
-

RESPONSE PATHWAYS

Online safety incidents may be responded school may2 r school may2 r clineentraliseddinnlinetedCIC)sponded may2 rOnli

STEPS FOR RESPONDING TO ONLINE SAFETY INCIDENTS QUICK GUIDE

The circumstances of online safety incidents will be different. The circumstances will determine what actions are undertaken, the order of actions and the urgency of the response.

3

1

Gather information

- Who is involved?
- What occurred?
- When did it occur?
- Where did it occur?
- îf u™r B`e)“

4

2

5

6

7

1-2-3

STEPS FOR RESPONDING TO ONLINE SAFETY INCIDENTS

These guidelines provide the steps to respond to an online safety incident, including incidents that involve behaviours that are suspected to be illegal. The circumstances of each online safety incident will be different. The circumstances will determine what actions are undertaken, the order of actions and the urgency of the response.

1. Identification and gathering of information

The school principal is responsible for collecting relevant information and conducting an assessment of that information to inform the response. The school principal may delegate actions to staff members.

Early actions should focus on clarifying the nature of the online safety incident and who is involved. Sources of information include:

- verbal reports from children, young people, staff and other adults such as parents and carers
- direct observations
- digital content (eg screen shots, text messages, video footage)
- student records (eg previous behaviours which may be similar or related).

Be careful not to disclose sensitive or confidential information when gathering information. Inappropriate disclosure may result in contamination and loss of potential evidence required for court processes.

Staff should address any immediate safety concerns that are raised in this process.

Secure digital content if appropriate. This information may be used for a school enquiry or police investigation. Step 4 provides information on working with South Australia Police.

Government schools may contact the Cyber Security Team for assistance on collecting evidence. eSafety provides advice on their website.

Maintain clear, accurate and timely documentation of the information obtained, advice sought and obtained, decisions made and actions taken.

2. Initial planning and immediate referrals

Develop an initial response plan and team. Consult with the response team and senior leadership to:

- ensure a comprehensive understanding of the incident
- support decision making and problem solving
- identify clear roles and actions.

Review the factors (see pages 3-4) to determine the most appropriate response pathway:

- school response
- school response with supporting services
- centralised interagency coordinated (CIC) response.

Immediate referrals:

- Government schools must refer to the South Australia Police if illegal behaviours are suspected.
- Staff in education settings must make a child protection notification if they suspect on reasonable grounds that a child or young person is, or may be, at risk - Children and Young People (Safety) Act 2017 (SA).

Document referrals and outcomes.

3. Ensure the safety and wellbeing of those involved

Consider what is required to support the safety of children and young people and others directly involved in the incident. This may include:

- creating a safe place within the school for the children and young people involved
- modifying class schedules/timetable for children and young people involved to manage interactions
- organising a school staff member to provide additional support and monitoring of the children and young people involved
- communicating appropriate levels of information to the children and young people involved. Seek their opinion about their needs
- contacting parents or carers and seeking their involvement and support. Communicate appropriate levels of information

Conducting searches

School staff do not have the legal authority to conduct a search for an electronic device for the

Schools may need to:

- obtain legal advice about what information can be communicated, in what form, to what audience and when
- seek sector office advice about the appropriate approvals for media responses
- remind all school staff of the procedures for dealing with media enquiries
- obtain advice from the South Australia Police, when they are involved.

Consider including relevant children, young people and their families in the planning of communication. Public communication should not cause further harm to the children and young people involved.

Schools must obtain advice from the Department for Child Protection for matters involving children and young people who are under the guardianship or custody of the Chief Executive of the Department for Child Protection.

7. Documentation

Collate and securely store all written and electronic records. This includes:

- details of the incident
- the management of the incident.

Records may be used for legal purposes and must be stored in accordance with records disposal schedules.

8. Ongoing support to children, young people and their families

Following the immediate response to the online safety incident, further planning will be required to resolve the incident. Consider:

- school based responses, page 3
- school responses with supporting services, page 4.

9. Review of the response

Following an online safety incident, the school principal may lead a review of the response. The importance of completing a review is that:

- outstanding tasks arising from the online safety incident are identified and completed
- it provides an opportunity for school staff to refine or change the response to online safety incidents
- learning needs of the whole school community can be identified and responded to
- it supports the school to implement or enhance preventative strategies to support online safety
- it provides the school community an opportunity to provide feedback on the response to the school to support learning and improvement.

1-2 week follow up

Ensure all documentation has been completed and secured.

Examine whether further communication or reporting is required (ie with school staff, with broader school community, governing councils/boards).

Review any training and learning needs for staff involved in the incident, including employee assistance debriefing and support.

3-6 week follow up

Review school documents related to behaviour and online safety to see if they require updating. This may include school rules, local policies and procedures additionally, acceptable use of digital technology agreements.

Consider the learning needs of children, young people and their families, staff members and volunteers relating to the safe use of digital technology. Develop a plan to address the learning needs of the school community.

Provide opportunities for all school staff involved in the management of the incident to provide and obtain feedback and/or outcomes. This contributes to learning and system improvement.

7-10 week follow up, then follow up as required

Identify and attend to outstanding tasks.

Ensure all documentation is up to date, accurate and appropriately stored.

ROLES AND RESPONSIBILITIES

School principals

For online safety incidents, the role of the school principal is to:

- respond to online safety incidents in a way that supports the safety and wellbeing of children and young people and the school community
- use these guidelines and ensure compliance with school or sector policies and procedures
- work collaboratively with their sector office and interagency stakeholders.

In response to racist online safe incidents, school leadership may consider their school's/ sector's strategic plan to address racism, promote relationships and respect and, address the barriers to engagement and participation in education for Aboriginal children and young people.

Catholic Education South Australia

The role of Catholic Education South Australia is to support Catholic schools and sector to respond to online safety incidents and to put these guidelines into operation.

Catholic Education South Australia may be contacted on 8301 6600 www.cesa.catholic.edu.au

Association of Independent Schools of South Australia

The role of the Association of Independent Schools of South Australia is to support independent schools to respond to online safety incidents.

Association of Independent Schools of South Australia may be contacted on 8179 1400 www.ais.sa.edu.au

Department for Education

Incident Management Directorate

The Incident Management Directorate receives and assesses reports of suspected or alleged employee serious misconduct and other critical incidents for government schools.

Critical incidents are reported on the critical incident reporting system. Reports are assessed by the Incident Management Directorate and referred for support based on the seriousness of the incident, and the supports required.

Cyber Security Team - Information Communication Techn80.083 0.206 0.364 scn /T1_0 1 T

Student Support Services, including Social Work Incident Support Service

The role of Student Support Services is to work in partnership with government schools to support learning and wellbeing of children and young people. Services available include:

- behaviour support
- support for children and young people in care
- special educator (children and young people with additional needs, including disability, sensory impairment and complex health needs)
- support with critical incidents (via Social Work Incident Support Service).

Truancy social workers work across government, Catholic and independent schools to support children and young people with ongoing attendance and engagement issues, or those who have been identified as at risk of non-attendance.

Engagement and Wellbeing Directorate

The role of the Engagement and Wellbeing Directorate is to support the government education sector to use these v0eReoAnes. This includes providing policy advice on behaviour, cyberbullying and onoAne safety.

SUPPORTING INFORMATION

External contacts

South Australia Police

000 (emergency police, fire, ambulance).
131 444 (police assistance line for non-urgent police assistance).

Child Abuse Report Line

13 14 78 (to report a reasonable suspicion that a child or young person is, or may be, at risk).

If you are a mandated notifier and the case is less serious, consider making a notification on the online child abuse reporting system. Access the Department for Child Protection website for information www.childprotection.sa.gov.au

eSafety Commissioner

www.esafety.gov.au

Kids Helpline

www.kidshelpline.com.au 1800 55 1800

headspace

National youth mental health foundation
www.headspace.org.au

Resources

eSafety Commissioner

www.esafety.gov.au

Reconciliation SA

www.reconciliationsa.org.au

Youth Law Australia

www.yla.org.au

ThinkUknow Australia

www.thinkuknow.org.au

Child safe organisations

https://childsafe.humanrights.gov.au

Definitions

child safe organisation

A child safe organisation puts the best interests of children and young people first. For more information see

APPENDICES APPENDIX 1: TYPES OF ONLINE RISKS

Cyberbullying

Cyberbullying is bullying that is done using digital technology. Cyberbullying involves:

- a misuse of power that occurs within a relationship
- behaviour that is repeated or can be repeated over time (ie being shared or viewed multiple times)
- harm.

Examples of cyberbullying include:

- online gossip and rumours
- leaving people out (this includes starting campaigns on social media to exclude people)
- creating sites that mock or humiliate others
- sharing someone's personal information online without consent

c.MC /P <</Lang (en-GB)/MCID 1434 >>BDC4ne x</ActualTexlTe14en-0m [(pos338.799 B)Tj[(Certag 2typesenc)3 (oc)3 (c)3buen

- sharing someone's information to cause embarrassment
- inappropriate image tagging (ie adding abusive comments, messages and hashtags to a photo or video)
- creating fake accounts in someone's name. This might be done to trick someone or make them feel humiliated
- forcing, threatening or coercing someone to obtain nude, nearly nude or sexual images
- non-consensual sharing of nude, nearly nude images or sexual images
- intimidation and threats.

Cyberbullying often occurs along with face to face bullying. Cyberbullying can have serious negative effects on a child or young person's wellbeing and mental health. The potential for harm is higher when cyberbullying is anonymous and has a large or unknown audience.

Certain types of cyberbullying behaviour may be illegal.

Online abuse (cyber-abuse)

Cyber abuse is a broad label used to describe behaviours that:

- use technology to threaten, intimidate, harass or humiliate someone
- is intended to hurt the other person socially, psychologically or emotionally.

Cyber abuse may occur between individuals of equal power. The individuals involved may not have an existing relationship.

Examples of cyber abuse:

- targeted and persistent attacks aimed at ridiculing, insulting, damaging or humiliating a person
- posting someone's personal information online without consent, often with the intention of encouraging others to harass them ('doxing')
- posting digitally manipulated images of a person, including explicit images
- unauthorised access, use or control of another person's online accounts

and receiver's control. This may have implications for the child and young person's current and future relationships with peers, partners, family and employers. A further risk is the use of these images on child exploitation sites.

Illegal and harmful content

Children and young people may be exposed to or seek out inappropriate online content. They may become involved in distributing inappropriate content. Online content includes text, imagery, animations, sound and video.

Examples include content that depicts or promotes:

- child sexual abuse
- physical or sexual violence against people and animals
- criminal activities
- discrimination, racism and other forms of hate-based intolerance (eg hate speech)
- terrorist acts
- harmful behaviour (eg advice in support of problematic eating habits, eating disorders or self-harm)
- sexually explicit behaviour
- abhorrent violent material (ie terrorist acts leading to serious injury or death; murder or attempted murder; torture; rape; kidnapping involving violence or the threat of violence).

Children and young people may intentionally or accidentally access:

- age restricted gambling sites
- age restricted online games
- pornography.

Unwanted contact

APPENDIX 2: FACTORS THAT MUST BE CONSIDERED IN ASSESSING AN ONLINE SAFETY INCIDENT

Schools have a duty of care to respond to online incidents for children and young people who are in their care and control. The duty is to take reasonable steps to prevent foreseeable harm to children and young people.

Schools are to provide a timely intervention to online safety incidents that occur out of school hours or off school premises when this is connected to the school.

The greater the connection, the greater the obligation placed on staff. Where a connectiongreater the e s3eater the

Child or young person's characteristics

Some children and young people may have existing vulnerabilities, conditions or circumstances that place them at greater risk of harm from online incidents. Some children and young people may be at higher risk of exclusion from learning. These may include children and young people who:

- are Aboriginal
- have a disability or additional needs
- are under the guardianship or custody of the Chief Executive of the Department for Child Protection
- are gender diverse, intersex or sexually diverse
- have existing mental health conditions
- are culturally and/or linguistically diverse
- have experienced other forms of victimisation (including violence, bully225 •

SAMPLE

uth Australia