RESPONDING TO ONLINE SAFETY INCIDENTS IN SOUTH AUSTRALIAN SCHOOLS

GUIDELINES FOR STAFF WORKING IN EDUCATION SETTINGS

Government of South Australia
Department for Education

catholic education south australia

AISSA Association of Independent Schools of South Australia

CONTENTS

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.

RESPONSE PATHWAYS FLOW CHART

ONLINE SAFETY INCIDENT OCCURS
(see appendix 1 for examples)

Schools consider factors to determine response pathway:
(see appendix 2 for expanded description)

- nature of the child or young person's behaviour
- child protection concerns
- behaviour may be illegal
- scale of the incident
- prior efforts made by school to address the behaviour
- child or young person's characteristics
- involves targeted behaviour towards particular cohorts
- anonymity and use of overseas servers
- impact and extent of support needed for resolution.

SELECT A RESPONSE PATHWAY

School Response

School resolves with on-site resources.

*Under this pathway there are no child protection concerns, or the concerns are low level. For low level child protection concerns mandatory reporting obligations still apply.

School Response with Supporting Services

School resolves with on-site and off-site resources.

Referrals may include:

- South Australia Police
- child protection notification
- learning and wellbeing supports
- ICT and cyber safety advice
- eSafety Commissioner.

Centralised interagency coordinated (CIC) response

Criteria for severe online safety incident (one or more indicators are present):

- suspected illegal behaviours
- multiple schools or sectors are involved
- severe risk of harm to children or young people
- specific cohorts of children or young people are targeted by organisations or persons
- use of anonymous or covert technologies
- high level of media coverage.

If criteria met, schools may request a CIC response.

Referral process for CIC response

Non-government schools
Referral via sector office – sector office to contact Incident Management Directorate (IMD).

Government schools
Referral via a critical incident report to IMD.

Referral assessed by Incident Management Directorate

Accepted
IMD to coordinate response.
School and/or sector allocates representative and coordinates activities in their school and/or sector.

Not accepted
Return to school response with supporting services.

RESPONSE PATHWAYS

Online safety incidents may be responded to in the following ways:

- school response
- school response with supporting services
- centralised interagency coordinated (CIC) response for severe online safety incidents.

Schools should ensure that the response pathway is proportionate to the situation. This involves schools reviewing and adjusting their response to address emerging issues.

School response

Schools are able to respond effectively to many online safety incidents using on-site resources.

Factors to consider

A school-based response may be appropriate when it has been assessed that:

- the behaviour of the child or young person is a developmentally appropriate transgression or low-level behaviour that breaches school rules
- the behaviour of the child or young person is not persistent. The behaviour is responsive to support and re-direction by school staff and parents or carers
- there are no child protection concerns, or the concerns are of a low level
- the behaviour is not suspected to be illegal
- the scale of the incident is small. A small number of children or young people are involved and the incident is contained within a class or school
- the child or young person does not have existing vulnerabilities which increases the risk of harm
- the school is able to effectively support the wellbeing of the children or young people involved. With support the children and young people involved are able to re-engage with their learning environment.

See appendix 2 for an expanded description of factors to consider.

Responses

School-based responses to these incidents may include:

- planning with the children or young people involved, their families and school staff to support and meet learning needs. Schedule review dates
- school based consequences for the child or young person who has engaged in the behaviour. The nature of the response will be equitable and reflect the child's needs and what's required to support positive and respectful behaviour in the future
- behaviour support strategies for the children or young people involved. For example:
  - social and emotional skills development
  - positive replacement behaviours
  - adjusting the environment to provide support and encouragement for preferred behaviours
  - explicitly teaching expected behaviour and the skills to meet those expectations
  - providing opportunities to practice new and/or positive behaviours offline and online
- increased monitoring
- restorative practices
- wellbeing supports for the child or young person who has been harmed by the incident
- educative responses by school staff for all children and young people. This may involve:
  - incorporation of online safety curriculum (eg teaching digital citizenship and literacy; teaching about specific online risks; explicitly teaching the acceptable use of digital technology agreement and other school expectations, values and school/class procedures)
  - revisiting specific content in the Keeping Safe: Child Protection Curriculum
- education and awareness raising activities with the school community.

School response with supporting services

Some online safety incidents will involve increasing levels of seriousness and complexity.

Factors to consider

A school response with supporting services may be needed in situations where there are one or more indicators of seriousness present. This may include circumstances where:

- the nature of the child or young person's behaviour is challenging, complex or unsafe due to the severity, frequency or duration
- there are child protection concerns
- the behaviour is suspected to be illegal
- the incident may involve multiple children and young people and/or occur across schools or education sectors
- prior efforts have been undertaken by the school to address the same or similar behaviours
- the child or young person has existing vulnerabilities which increases the risk of harm
- the incident results in the school being felt as culturally unsafe, particularly for Aboriginal children and young people, their families and community
- the online content attacks specific groups of people. The content is from individuals or groups that promote hate-based intolerance
- online content is being shared through anonymous or fake social media accounts
- the impact and extent for support needed for resolution is beyond general on-site resources.

See appendix 2 for an expanded description of factors to consider.

Responses

To respond to these types of online safety incidents, schools will use their on-site resources as outlined on page 3. In addition, schools will work with sector off-site supports and/or government and community resources. Schools may:

Seek advice, refer and report:

- request the online site remove the offensive content. Consider the need to retain evidence for suspected illegal behaviours
- seek advice and intervention from the eSafety Commissioner. eSafety receives complaints about image-based abuse and serious cyberbullying material for children and young people. In response, eSafety may:
  - request the online site removes the offensive content
  - offer advice, assistance and resources
  - work with the school and parents or carers to help stop the cyberbullying
- make a child protection notification to the Child Abuse Report Line and/or seek advice from the Department for Child Protection. A notification must be made if the legal threshold for mandatory notification has been reached
- seek advice from South Australia Police and/or refer the matter to police for investigation. Government schools must refer suspected illegal behaviours to police
- seek advice from the relevant sector office:
  - policy advice on behaviour, cyberbullying and online safety
  - technical advice on digital technology (ie technical solutions such as filters, blocking, monitoring software)
- seek advice from and refer to internal sector and external community supports. Options for referral and support may be discussed with the child or young person and their family.

Collaborate:

- engage educative responses from trusted providers (eg eSafety Commissioner and South Australia Police for delivery of the ThinkUKnow online safety program)
- collaborate with:
  - other schools, within and across the education sector
  - local community, government and non-government organisations.

Support school safety:

- targeted use of suspension, exclusion and expulsion if required to provide immediate safety while further supports are put in place.

Schools should consider the need for cultural consultation for all online safety incidents involving Aboriginal children and young people. Seek guidance from Aboriginal staff members about the issue and on the cultural appropriateness of their involvement. In some circumstances, factors such as family connection may result in indirect involvement or the need to obtain cultural support from an alternative source such as an Aboriginal staff member from another site.

Centralised interagency coordinated response

In rare situations, an online safety incident may be considered a severe incident.

For a severe online safety incident one or more of the following indicators will be present:

- suspected illegal behaviours (eg child abuse and extreme abhorrent content)
- multiple schools or sectors are involved
- severe risk of harm to children and young people
- specific cohorts of children and young people are targeted by organisations or persons
- use of anonymous or covert technologies, including overseas web hosting services
- high level of media coverage.

Severe online safety incidents may require a centralised interagency coordinated (CIC) response that involves professionals from specialist areas.

A CIC response is coordinated by the Incident Management Directorate – Department for Education.

Referral process for centralised interagency coordinated response

Catholic and independent education sectors

Where the criteria for a severe online safety incident is met and a CIC response is believed to be required, schools are recommended to contact their sector office for support. The sector office may then contact the Incident Management Directorate to request a CIC response.

Government education sector

A critical incident report will be completed on the critical incident reporting system for assessment by the Incident Management Directorate.

Role of Incident Management Directorate

The Incident Management Directorate may coordinate a CIC response to the severe online safety incident for non-government and government schools, upon receipt of a referral. The Incident Management Directorate will determine whether the referral for a CIC response is accepted.

When coordinating a CIC response the Incident Management Directorate will:

- coordinate an interagency cross-sector process to oversee the response to the incident
- assign the matter to a case manager
- chair CIC meetings, document plans and actions
- brief the Minister for Education about the incident and CIC response
- support the sharing of information across stakeholders, consistent with legal requirements.

Each school and/or sector affected by the incident will nominate a representative to contribute to the CIC process, and coordinate activities within their school and/or sector.

Examples of supporting services and other offices or departments that may participate in CIC responses include:

- South Australia Police
- eSafety Commissioner
- Department for Child Protection.

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.

1 Gather information

- ☐ Who is involved?
- ☐ What occurred?
- ☐ When did it occur?
- ☐ Where did it occur?
- ☐ Other relevant information (ie past incidents, vulnerabilities).
- ☐ Address immediate safety concerns.
- ☐ Secure digital content, if appropriate.
- ☐ Begin documentation.

2 Planning and immediate referrals

- ☐ Establish response team, allocate roles/responsibilities.
- ☐ Review factors to determine appropriate response pathway, pages 3-4.
- ☐ Consult as appropriate.
- ☐ Determine response pathway:
  - school response
  - school response with supporting services
  - centralised interagency coordinated (CIC) response.
- ☐ Immediate referrals:
  - South Australia Police for suspected illegal behaviour
  - mandatory child protection report.

3 Safety and wellbeing

- ☐ Manage interactions, establish safe places.
- ☐ Staff members to support and monitor.
- ☐ Contact parents or carers.
- ☐ Organise after school supports.
- ☐ Communicate appropriate levels of information.
- ☐ Ensure safety of school community.
- ☐ Immediate consequences, if required, to provide safety to the school whilst further supports are put in place.

4 South Australia Police

Make a plan with police about:

- ☐ initial response to children and young people involved
- ☐ secure evidence – discuss with police:
  - management of sexually explicit content
  - confiscation of devices
  - conducting searches
- ☐ information to be provided to parents, carers and staff members.
- ☐ Police reference number.
- ☐ Establish key contact.
- ☐ Document instructions provided by police.

5 Reporting

- ☐ Critical incident reporting (adhere to specified timeframes).
- ☐ Other reporting:
  - Department for Child Protection for children and young people under the guardianship or custody of the Chief Executive of the Department for Child Protection
  - mandatory child protection report.

6 Communicating

If appropriate:

- ☐ communicate with school community
- ☐ develop plan and seek approvals to respond to media enquires.

Seek advice from:

- ☐ legal and media services within sector
- ☐ sector office/senior leadership
- ☐ South Australia Police, when involved
- ☐ Department for Child Protection, where relevant.

7 Documentation

- ☐ Collate and securely store all written and electronic records.

8 Ongoing support

- ☐ Further planning for resolution:
  - school response, page 3
  - school response with supporting services, page 4.

9 Review and follow up

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

- with consent organise additional off-site supports (eg counselling)
- providing details of telephone and online support services (eg Kids Helpline and headspace)
- targeted use of suspension, exclusion and expulsion if required to provide immediate safety while further supports are put in place.

4. Work with South Australia Police

Where school principals suspect that illegal behaviour has occurred, they should refer the matter to the South Australia Police and follow police instructions. Government schools must refer suspected illegal behaviours to police.

Initial planning with police should consider the following:

- initial response to children and young people involved
- securing evidence (ie electronic content and/or digital devices)
  - management of sexually explicit material
  - confiscation of devices
  - conducting searches
- what information can be disclosed to parents, carers and staff members.

Record the police reference number. This includes recording the details of the person the report was made to, the date and time. Maintain a written record of conversations had with police, including decisions made, and instructions provided by police.

Advise the police if the child or young person involved is under the guardianship or custody of the Chief Executive of the Department for Child Protection.

Initial response to children and young people

The initial response to the child or young person will be guided by police involvement and their advice. Unless instructed otherwise by police, tell the relevant child or young person what is occurring. Disclose only what is relevant to them to ensure confidentiality.

If the police are conducting enquires, do not ask the child or young person direct questions about the matter under police investigation or ask for a written statement. Document any conversations including disclosures and inform police.

Management of sexually explicit material

If information suggests that digital content may involve nude, nearly nude or sexual images of a child or young person, it is recommended that school staff do not view this content. Intentional viewing, sending, copying and storage of this content may place staff members at risk. Police advice and instructions must be sought when responding to an online safety incident involving nude, nearly nude or sexual images of children and young people. In these incidents, securing digital evidence is a matter for the police.

Confiscation of devices

If a child or young person has used their device in an online safety incident (see appendix 1), schools should refer to their school rules.

Teachers may ask the student to hand over their device for a set period of time. This must be done with the student's cooperation. Should a student refuse to cooperate with the teacher, this may escalate the response taken by the school. This may include seeking the assistance from the principal and use of school level consequences.

There is no lawful authority for school staff to use physical or coercive force to confiscate an electronic device from a child or young person.

Where a principal has confiscated an electronic device:

- confiscation must occur with student cooperation
- the device must be securely stored, with the principal being accountable for the handling and management of the device
- the electronic device is to be minimally handled by school staff members
- the device must remain unopened and not accessed by school staff members
- the device must be provided to police upon request. Alternatively, returned to the student, parent or carer if not required by police. In both circumstances, this is to occur in a timely manner
- the principal or delegate must maintain an accurate written record of all actions undertaken and decisions.

If the school principal suspects the behaviour may be illegal, it may be more appropriate that police use their legal authority to confiscate the electronic device from the child or young person.

A staff member should remain with the child or young person until police arrive. This is to ensure the device is not tampered with by the child or young person resulting in lost evidence.

Conducting searches

School staff do not have the legal authority to conduct a search for an electronic device for the purpose of confiscation. School staff do not have the legal authority to conduct a search of digital content contained on an electronic device without the child or young person's informed consent.

Schools may secure digital content that is stored on the school's electronic systems.

Informing parents and carers

The severity of the incident and police involvement will determine the type of contact, frequency and urgency of parent or carer contact.

When police are involved, they must be specifically asked whether the school may inform parents or carers.

Consider:

- Advise parents or carers as soon as possible, unless the police have directed the school not to contact parents or carers. This direction must be documented.
- In some instances, a legal guardian may be required to be present should police choose to conduct an interview of the child or young person. Schools must be guided by police about this.
- Ensure parents or carers have the name and number of school staff who can be a key contact about the incident.
- Ensure parents or carers have information about additional support services, including those provided by other government departments and community services.

5. Reporting

Reporting of critical incidents

Report critical incidents according to school or sector requirements.

Department for Education

Reporting of critical incidents occur through the critical incident reporting system. These reports are reviewed by the Incident Management Directorate.

For a critical incident of extreme seriousness, the school principal must also notify the education director. If unavailable they must contact the Director or Assistant Director of the Incident Management Directorate.

Reporting for incidents of extreme seriousness must occur within 24 hours. Other incidents which are not classified as extreme seriousness, must be reported within two working days. The definition of incidents of extreme seriousness and other incidents can be found in the reporting critical incidents and injuries procedure.

Independent Schools

Independent schools are recommended to contact the Association of Independent Schools of South Australia for advice.

Catholic Schools

Principals in Catholic schools should report serious matters (eg critical incidents) to the appropriate nominated contacts in the sector office. In the first instance this may be the School Performance Leader for the region. If this person is unavailable, contact should be made with the Catholic Education Office (People, Leadership and Culture section) or an Assistant Director.

Other reporting

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). Child protection notifications are made to the Child Abuse Report Line.

For Catholic schools, mandatory notifications must also be reported to the sector office.

In addition to complying with mandatory reporting obligations, all online safety incidents involving children and young people who are under the guardianship or custody of the Chief Executive of the Department for Child Protection are to be reported to the:

- child or young person's allocated worker or office within the Department for Child Protection
- child or young person's foster carer or kinship care (as appropriate).

6. Communicating with the school community and responding to media enquiries

Careful consideration should be given to communication with the school community and responses to media enquiries. Communication should ensure an appropriate balance

between working in partnership with all those affected, and meeting legal obligations about privacy and confidentiality.

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 Technology services

The role of the Cyber Security Team is to provide expert technical advice and practical information communications and technology (ICT) support for online safety incidents for government schools.

Examples of advice and practical support include:

- removal of digital content
- securing information on school technology
- responding to threats (eg viruses, malware and spam)
- putting in place technical protections (eg removing ability to be contacted, use of filters)
- support to school-based ICT teams.

Government schools may contact the Cyber Security Team:

ICT service desk on 8204 1866 (metro) and 1300 363 227 (country).

Legal Services Directorate

The role of Legal Services Directorate is to provide legal and policy advice to the government education sector.

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 guidelines. This includes providing policy advice on behaviour, cyberbullying and online 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 https://childsafe.humanrights.gov.au

Abhorrent content

Abhorrent violent material is defined by the Criminal Code Act 1995 (Cth). The Act defines abhorrent violent material as material that involves a terrorist act leading to serious injury or death, murder or attempted murder, torture, rape, kidnapping involving violence or the threat of violence.

Web hosting services

Web hosting services enable individuals/ organisations to make their websites accessible.

Related legislation

Children and Young People (Safety) Act 2017 (SA)

Education and Children's Services Regulations 2020 (SA)

Related cross sector guidelines for education sectors

Protective practices for staff in their interactions with children and young people.

Managing allegations of sexual misconduct in SA education and care settings guidelines.

Related policies/procedures for government schools

Reporting critical incidents and injuries procedure.

Student use of mobile phones and personal devices policy.

Duty of care policy.

Behaviour Support Policy.

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
- 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
- distributing or directly sending offensive and shocking material
- threatening violence or inciting others to do the same
- encouraging someone to self-harm, suicide or engage in other dangerous acts
- stalking a person online.

Certain types of online abusive behaviour may be illegal.

Explicit image sharing (sexting, nudes)

Young people may take nude or nearly nude images of themselves and share those images consensually with another person of equal power, age or development, in the context of a relationship. The exchange may be felt as a positive or neutral experience for some young people.

The consensual sharing of these images carries a number of serious risks for children and young people. The behaviour may be illegal as children and young people are not able to legally consent to the production and sharing of their own explicit images because of their age. Children and young people must not create, send or receive nude, nearly nude or sexual images.

There is potential for these images to be distributed and made public, outside of the original sender

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

Unwanted contact is any type of online communication that makes a child or young person feel uncomfortable or unsafe. In some circumstances, unwanted contact may be grooming behaviour.

Online grooming (cyber-grooming)

Grooming, and online grooming plays a key role in the sexual abuse of children and young people. It involves forming a relationship with a child or young person to enable abuse to occur. Abuse may occur within the online or offline environment, or both.

Individuals who groom children and young people may also manipulate parents, carers and other adults associated with the child or young person. Their aim may be to validate, justify or minimise their behaviour, and maintain control and access to the child or young person.

A child or young person may not know they are being groomed. They may not understand the intentions of the individual, or identify the risks and potential for harm.

Child sexual abuse

Children and young people may experience sexual abuse which involves digital technology. An individual may force, entice, manipulate, blackmail, deceive or coerce a child or young person to take part in sexual activity online. This activity may be streamed or recorded for the person's self-gratification, for the gratification of others, or for other gains.

There can be an overlap between online grooming, unwanted contact and child sexual abuse. These experiences may occur across offline and online environments.

Breaches of personal data and information

Children and young people's personal information can be accessed without their knowledge or consent. Children and young people may also disclose personal information unintentionally or intentionally.

Examples include:

- personal information is accessed without permission by other people (eg spyware)
- personal information is disclosed unintentionally (eg through meta-data, geo-location and phishing scams)
- personal information is disclosed intentionally, without an awareness of the risks associated (eg identifying material contained within photographs or text).

Consumer related risks

Children and young people may become financially active online before they have developed an understanding of money, budgeting and credit. This may expose them or their family to financial and security risks.

Examples include:

- fraudulent transactions
- unintentional spending online, including through in-app purchases and subscriptions
- excessive use and overspending on internet content or services
- down-loading viruses and malware.

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 connection exists, staff have a duty of care to ensure the physical and psychological safety of the child or young person.

Some online safety incidents will be more serious and complex than others. The response to an online safety incident should be proportionate to the incident. Principals must consider a number of factors to determine the most appropriate response. Those factors include:

Nature of the child or young person's behaviour

Children and young people's behaviour spans a continuum. Indicators of increased seriousness may include:

- the child or young person has engaged in complex and challenging behaviours. These behaviours raise greater concern due to their severity, frequency or duration and require more persistent guidance and support to minimise.
- the child or young person has engaged in unsafe behaviours. These behaviours:
  - are severe, of high frequency or extended duration
  - or are unsafe for the child or young person and, those around them.

Complex, challenging and unsafe behaviours may also be illegal behaviours.

Child protection concerns

Online incidents may be more serious if the incident requires a mandatory notification to child protection authorities because it causes educators to suspect on reasonable grounds that a child or young person is, or may be, at risk and the suspicion was formed in the course of the educators' employment – Children and Young People (Safety) Act 2017 (SA).

The behaviour may be illegal

Incidents that involve suspected illegal behaviour are more serious. These incidents may involve illegal behaviour by a child or young person, or by an adult acting illegally towards the child or young person.

Scale of the incident

The number of children, schools and other organisations involved should be considered. Indicators of increased seriousness include:

- a significant number of children and young people are involved
- multiple schools are involved and negatively impacted (or there is a high likelihood for involvement of multiple schools). This includes the involvement of schools across education sectors
- the incident involves others in the community. For example, sporting clubs, religious organisations, Out of School Hours Care programs
- the incident is highly visible through media attention or through online sharing.

Prior efforts made by the school to address the behaviour

Indicators of increased seriousness include where:

- the school has previously addressed the same or similar behaviour, and those efforts have not changed the child or young person's behaviours
- the behaviours have escalated or become more covert after adult intervention.

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, bullying, child abuse and neglect).

Some children and young people may require a faster and escalated response to online safety incidents. This includes escalating the response for minor and one-off incidents.

For Aboriginal children and young people, unresolved online safety incidents can result in the school being seen as a culturally unsafe place. Unresolved issues for one Aboriginal student may have significant implications for all Aboriginal students and families within the school community. This may result in non-attendance or disengagement from learning for multiple students across the school.

Involves targeted behaviour towards particular cohorts

Incidents may be more serious where the behaviour is targeted at specific groups based on race, religious beliefs, gender or sexual identity, and cultural backgrounds. This includes online content that:

- involves racism, homophobia, extremism, radicalisation and other forms of hate-based intolerance
- targets children and young people of particular racial and cultural backgrounds, religious beliefs, gender and sexual identities
- is being done by groups or organisations that promote racism, homophobia, extremism, radicalisation and other forms of hate-based intolerance.

Anonymity and use of overseas servers

Individuals may target a child or young person using fake accounts, false identities or under false pretences. The use of an overseas server can increase the risks to children and young people. Personal data and digital activity contained on off-shore servers may not be protected under Australian law. Data and digital activity stored in Australia may result in better protections for children and young person.

Impact and extent of support needed for resolution

The degree of impact on the children and young people involved and the extent of additional support that is needed to address an incident should be considered. Indicators of increased seriousness may include:

- significant impact on the children or young people involved, especially where it affects their daily functioning
- support to children and young people is likely to be high, protracted or complex
- high level of monitoring is required to ensure the safety and wellbeing of the children and young people involved
- specialist or multi-disciplinary services may be required to restore relationships between the children and young people who are involved
- there is insufficient expertise or capacity at the school to respond to the incident and behaviours.

APPENDIX 3: COMMUNICATING WITH THE SCHOOL COMMUNITY

A school may wish to communicate with the school community about an online safety incident. When making a determination on the appropriateness of communication, principals should consider the factors for assessing an online safety incident. For example, the behaviour may be illegal, scale of the incident, involves targeted behaviour towards particular cohorts.

When communicating, consider:

- the form of communication (ie social media, website, school app, paper based letter)
- timing
- advice received from the South Australia Police for suspected illegal behaviours
- sector specific legal and media advice
- sector specific protocols for school community wide communication on critical incidents
- that all communication will be made available to the general public
- the requirement for some children, young people and their families to have additional or different communication (ie language, content, method of communication).

The following draft letter should be modified according to the online safety incident and needs of the school community, with legal, media and leadership advice sought according to sector protocols.

Letter guide

Introduction

- Reflect the positive attributes and culture of the school community.
- Establish tone:
  - language is respectful, professional, simple and direct
  - be calm and measured.

Explanation

- Provide a brief and clear explanation of the broad issues the school is managing.
- Information disclosed must be factual.
- Do not reveal details of the incident or names of students involved.

Schools response

- Acknowledge the impact on the school community.
- Briefly outline what the school has done in response.
- Briefly outline what the plan of action is going forward. This may be a general and brief statement for those involved and for the school community.
- Discuss any wellbeing supports for students.

Closing

- Provide reassurance.
- Nominate a contact person and encourage parents and carers to make contact.
- Circle back to the school values.

Optional

- Provide options for what parents and carers may do with their child.
- Provide parents and carers with resources so that they can then provide emotional and educational support to their child.
- Encourage parents and carers to review local school polices and provide link or copy.

Sign off

- Determine who the letter should be from (ie principal or sector representative).

SAMPLE

Dear school community

As educators at Toll Primary School we strive for our school to be a place of inclusion.

Our school values are: be respectful, be responsible, be learners and be safe. We are grateful for our wonderful students, parents, carers, volunteers and school staff who strive to uphold these values.

Recently, some students in our school community have acted in ways that do not reflect our school's values. A serious incident of cyberbullying has occurred among our students.

The school has addressed this situation. The leadership team will continue to work with those who are directly involved to prevent similar incidents in the future.

Toll Primary School is committed to supporting students to be safe and responsible users of digital technology.

I invite you to contact the School Student Wellbeing Leader ..... if you have any concerns about this matter. Together, we can work to create a healthy environment for our students both at home and at school.

We encourage you to speak with your child about cyberbullying and online safety. Some trusted resources are:

- Department for Education SA – cyberbullying and online safety guides
  www.education.sa.gov.au
- eSafety Commissioner
  www.esafety.gov.au
- Kids Help Line 1800 55 1800
  www.kidshelpline.com.au
- headspace – national youth mental health foundation
  www.headspace.org.au

Yours sincerely

..... Principal

Record history

Published date: August 2021

Approvals

OP number: 298

File number: DE19/34234

Status: approved

Version: 1.0

Policy officer: Policy Officer, Engagement and Wellbeing Directorate

Policy sponsor: Director, Engagement and Wellbeing Directorate

Responsible executive director: Executive Director, Early Years and Child Development Division

Approved by: Executive Director, Early Years and Child Development Division

Approval date: 10 August 2021

Next review date: 10 August 2024

This guideline is a collaboration between the SA government and non-government education sectors. Education sectors will continue to work together with a shared commitment to the wellbeing and safety of children and young people in South Australia.

Revision record

Version: 1.0

Approved by: Executive Director, Early Years and Child Development Division

Approval date: 10 August 2021

Next review date: 10 August 2024

Amendment(s): new guideline implemented.

Keywords

Online safety, cyberbullying, critical incident, cyber safety, police, bullying, behaviour, behaviours of concern, digital technology, mobile phone, device, behaviour support, online abuse, cyber abuse.

Contacts

Business unit: Engagement and Wellbeing Directorate

Email: Education.EngagementAndWellbeing@sa.gov.au

Government of South Australia
Department for Education

Association of
Independent Schools
of South Australia