A tool for

UNISA and BHC - Workbook 3 - Cyber Safety Awareness Policies and Procedures_V5.0

ACSI
STRONGER TOGETHER
SOUTHERN AFRICA

		Yes/No	NOTES
1.	All teachers submit termly assessment plans for control purposes.		
2.	All teachers create computer generated mark books.		
3.	Learners' books are regularly marked and given formative feedback.		
4.	Written evidence of marking memoranda or rubrics is available.		
5.	Assessment workshops, as part of professional development, are held.		
6.	School assessment plans in the High School are created to prevent bottlenecking.		
7.	'Assessment Accountability Triangle' of Learner-Teacher-Parent is maintained.		

NOTES FOR IMPROVEMENT PLAN:

_____ _____

SIGNED **DATE**



CYBER SAFETY AWARENESS POLICIES AND PROCEDURES

PART OF THE CYBER SAFETY AWARENESS TOOLKIT FOR LEARNERS

British High Commission Pretoria

UNISA | college of science, engineering and technology

For further information visit:
https://www.cybersecurityhub.gov.za/cyberawareness/
http://cyberaware.co.za

CYBERSECURITY HUB

Table of Contents

1. Introduction 1
2. Objectives of this Document 1
3. Aim of this Document 1
4. Responsibility of the School Leadership 2
5. Approach 2
6. Phase 1: Assess 3
   - 6.1. Cyber Governance 3
   - 6.2. Cyber Risk Management 4
   - 6.3. Cyber Safety Compliance in Schools 5
   - 6.4. Identifying the Current Cyber Safety Culture within the School 6
7. Phase 2: Build 6
   - 7.1. Building a Cyber Safety Environment/Culture 6
   - 7.1.1. Cyber Safety Policies 6
   - 7.1.2. Cyber Safety Standards 7
   - 7.1.3. Cyber Safety Procedures 7
   - 7.1.4. Cyber Safety Guidelines 7
8. Phase 3: Continuously Growing a Cyber Safety Culture 8
   - 8.1. What Is a Cyber Safety Awareness Programme? 9
   - 8.2. What belongs in a Cyber Safety Awareness Programme? 9
   - 8.2.1 Communication 9
   - 8.2.2 Checklist(s) 9
   - 8.2.3 Content 9
   - 8.3. How Frequently Should a School Conduct Cyber Safety Training? 10
   - 8.4. Cyber Safety Guidelines Specifically for Teachers 10
9. Phase 4: Defend 10
   - 9.1. Incident Management Plan 10
   - 9.2. Incident Management Roles and Responsibilities 11
   - 9.3. Developing an Incident Management Plan 11
   - 9.4. Review of the Incident Management Plan 12
10. Phase 5: Evaluate 13
11. Appendix A: Example of the Responsibility and Reporting of Teachers, Learners and Parents 14
    - 11.1. Cyber Safety Guidelines Specifically for Teachers 14
    - 11.2. Cyber Safety Guidelines for Learners 16
    - 11.3. Cyber Safety Guidelines for Parents / Caregivers 17
12. SA Compliance Summary 18
13. References 20

1. Introduction

Learners have incredible opportunities for entertainment and self-education in cyberspace, using an array of digital applications and devices. They spend a significant amount of time surfing the Internet and communicating online via social media or gaming platforms. Schools are also using more Information and Communication Technology (ICT) and ICT devices as part of their educational programme support and office-based functions. It is therefore vital that learners, teachers, administrative staff and parents (or caregivers) are forewarned about online dangers, trained to detect/avoid potential threats, and are empowered to better deal with any possible incidents should they occur. A cyber safety toolkit has been created to assist in achieving the goal of establishing a safer cyberspace for all.

2. Objectives of this document

This document provides governance, monitoring and incident response guidance to assist South African (SA) schools to better manage cyber safety and awareness requirements.

The key objectives of this document are:

a) To provide schools with recommendations on improving cyber safety awareness.

b) To identify the specific risk, threats, vulnerabilities, and recommended guidance applicable to learners, teachers, administrative staff and parents (or caregivers) in SA.

c) To equip users of this document with the understanding of how to better protect themselves and learners under their care.

d) To outline an approach in order to improve cyber risk management for the typical SA school environment and minimise the harm caused by incidents.

3. Aim of this document

This document aims to establish, grow, and cultivate a cyber safety culture in schools and will assist by:

a) Indicating the responsibility (according to law) of schools towards cyber safety among teachers and school learners.

b) Improving schools' understanding and responsibility of cyber safety towards learners.

c) Providing guidance in identifying key role players and the establishment of an oversight. Committee to better manage the rollout of a cyber safety plan.

d) Highlighting the key responsibilities of teachers, learners, and parents.

e) Enabling them to respond more effectively to any cyber-related incidents that may occur.

4. Responsibility of the school leadership

The opportunities and risks of using cyberspace are well documented. Schools face the same cyber threats as other organisations and may be targeted by a range of different cyber agents seeking to compromise their systems.

The education sector is extremely dependant on ICT, and increasingly cyber incidents result in devasting consequences such as:

- Financial – A motive for hackers carrying out an attack on an education institution is often for financial gain. Schools manage a large number of learner fees, and they are a prime target for cyber criminals.
- Data theft – All institutions hold learner and staff data, including sensitive details such as addresses and names. This type of information can be valuable to cyber criminals who could potentially exploit the information by releasing it to a third-party.
- Reputational damage – Disgruntled individuals or groups of people can cause significant harm to a school's reputation with the spreading of fake news or disclosing sensitive information on social media platforms.
- Psychological or physical harm – The misuse of social media can have a detrimental effect on both learners and teachers. Bullying or aggressive messaging may even spill over into actual scenarios where the physical safety of people is compromised.
- Financial loss – Cyber criminals are able to utilise a range of methods to defraud or extort money from schools or parents.
- Lawsuits – Schools are expected to comply with the laws and regulations of the country. Failure to do so may result in fines or even lawsuits from disgruntled community members.

There are sufficient reasons to improve cyber risk management for the typical SA school environment and minimise the harm caused by incidents.

5. Approach

It is essential that school leadership work in partnership with school administration, teachers, learners, parents (or caregivers) and local communities to adopt and implement a cyber safety approach. This document proposes an ABCDE cyber safety methodology. The ABCDE approach consists of 5 phases, as illustrated below.

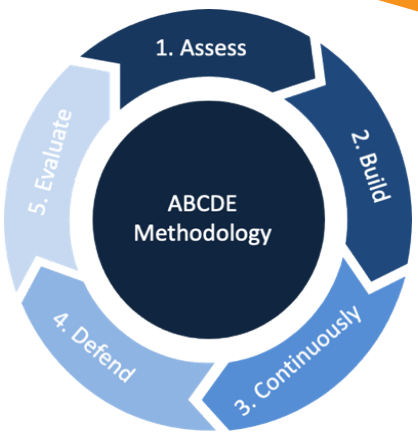
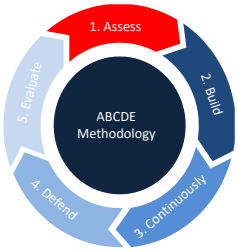


Figure 1: ABCDE school cyber safety methodology

Each of these phases will be outlined in more detail in the rest of this document.

6. Phase 1: Assess



This phase will focus on the assessment of the current cyber safety environment within the school. It will focus on determining the school's cyber governance (6.1), cyber risk management (6.2), cyber safety compliance (6.3) and identifying the current cyber safety culture within the school (6.4).

6.1. Cyber governance

Cyber governance is a component of corporate governance, which helps determine an information security strategy, how high-impact cyber business risks are managed, and which ensures that the correct level of resources is made available. It is recommended that schools form a Cyber Safety Committee, possibly under the School Safety Committee (if there is one). The function being to take reasonable steps to protect learners from any reasonably forseen harm, including those that may be encountered within the online learning environment, online social activities, and online communications.

Ideally, the role-players that should form part the Cyber Safety Committee are outlined below. It is realised, however, that schools might have limited personnel resources. However, it is important that a Cyber Safety Committee is established by school management consisting of:

- IT, Network Administrator or external IT Company Representative.
- IT Teacher or Head of Department.
- Librarian/Counsellor/Life Skills Teacher.
- School Governing Body Representative.
- A member of the local police service or private security firm.
- Learner Representative.
- Parent (or Caregiver) Representative.
- Other appropriate specialists as required (Legal Representatives).

The committee should be constituted according to all the required protocols for committees,

including an attendance register, agendas and minutes of meetings.

Source: Adapted from the Guidelines on e-Safety in Schools: SA Department of Basic Education

The Cyber Safety Committee responsibilities include:

- Developing, implementing and enforcing relevant policies and procedures with appropriate pre-determined penalties for any breach of such policies. These would need to be reviewed and updated on an annual basis.
- Meeting at least each quarter and documenting decisions and task allocations.
- Coordinating training and awareness workshops based on the identified risk and compliance environment.
- Communicating all policies to teachers, administrative staff, parents/caregivers and learners.
- Managing a consultation process between all role-players before the policy can be changed.
- Ensuring that teachers, parents/caregivers and learners understand the content of the policy, their role and responsibility, as well as the consequences if the policy is not adhered to.
- Allocating a budget to meet the objectives of the Cyber Safety Committee.

6.2. Cyber risk management

The committee should take reasonable steps to protect learners from any harm that should have reasonably been foreseen, including those that may be encountered within the online learning environment, online social activities and online communications.

The Cyber Safety Committee should investigate and determine:

1. Who are the cyber threat agents the school needs to consider? (these could be either external or internal people with harmful intentions)
2. What are the cyber threats the school faces? (dangers)
3. What cyber vulnerabilities does the school need to address? (weaknesses that may be exploited)
4. What cyber risks is the school concerned about? (that will significantly impact the organisation)
5. What controls does the school need to implement? (to reduce unacceptable risks)
6. How to ensure that the school's assets (tangible and intangible) have sufficient levels of protection?

Relevant examples for each section above are outlined in the figure below:

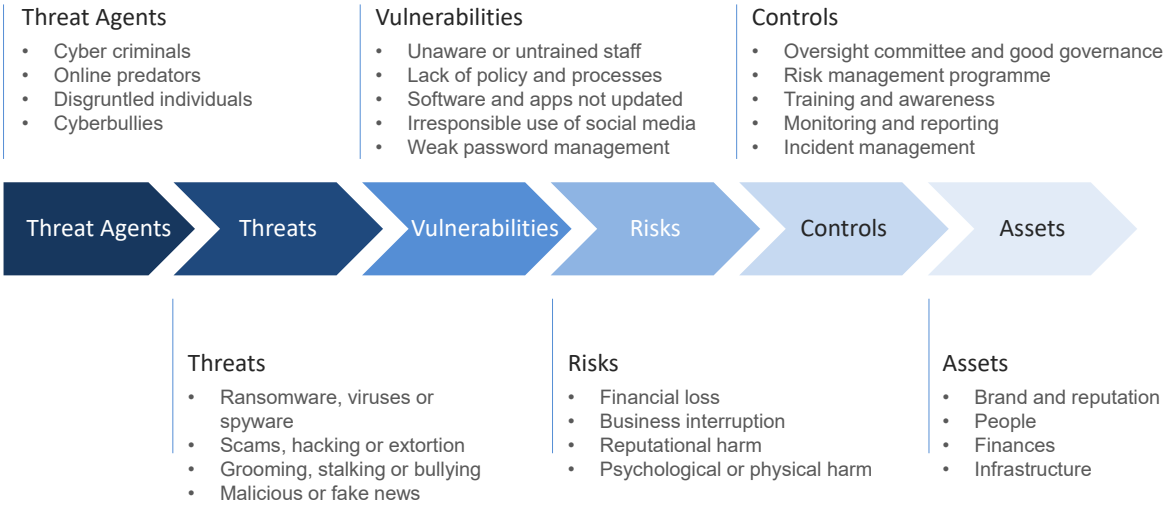


Figure 2: Scope of school cyber safety risk review

The Cyber Safety Committee should then consider this information to help prioritise which areas require focus, to ensure that risks to the school's reputation, operations and the safety of staff and learners are prioritised and managed within adherence to policy.

The school must have a Risk Register to indicate all the risks identified above, the plan to mitigate the risks and the indicators to determine if the risks were addressed.

6.3. Cyber safety compliance in schools

In South Africa, there are a number of legal frameworks and regulatory requirements in terms of cyber safety and data protection that organisations, such as schools, are required to comply with. The Cyber Safety Committee will need to adhere to existing documents and guidelines to ensure compliance in schools. Some of the key legislative frameworks in SA, as well as additional compliance areas that are relevant to cyber safety, include:



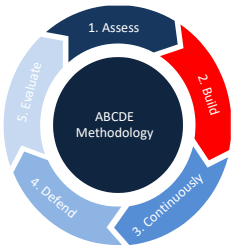
Figure 3: Key legislative frameworks and relevant compliance requirements in SA

Schools are therefore required to ensure the safety of the school learners. This includes to establish, grow and cultivate a cyber safety awareness culture. It is highly advisable that the school appoint a legal representative on the Cyber Safety Committee to assist with all legal aspects.

6.4. Identifying the current cyber safety culture within the school

This step is to identify prior knowledge of teachers and learners to find out what is the current need for cyber safety for teachers and learners. Schools should also do an analysis regarding existing and available funding and resources within the school that can be used to improve the cyber safety culture.

7. Phase 2: Build



This phase focuses on assisting the schools to build holistic cyber safety policies, standards, procedures and guidelines.

7.1. Building a cyber safety environment/culture

The Cyber Safety Committee is encouraged to establish, communicate and enforce a set of governance documents that define how cyber risks are to be managed within a school. An overview of each type of document and a brief outline of the document's use is explained below.

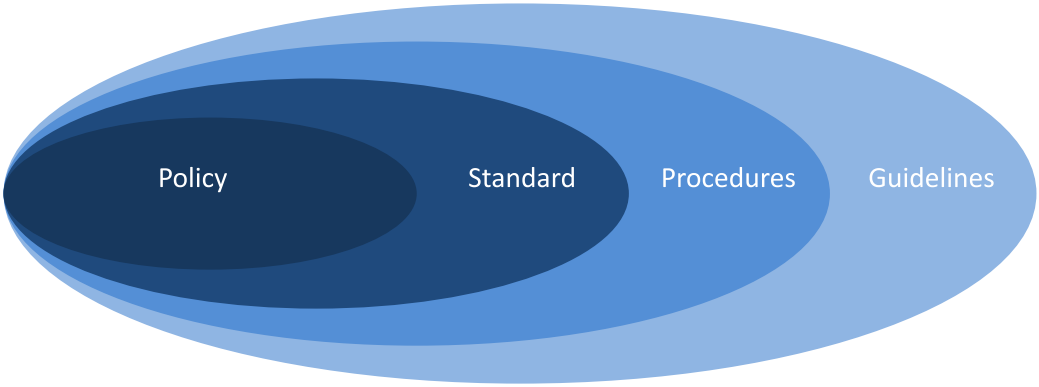


Figure 4: Cyber governance documentation

7.1.1. Cyber safety policies

- Consist of a high-level statement of leadership intent that formally establishes requirements to guide decisions and achieve rational outcomes.
- Are simple, easy to understand, and do not require training only awareness.
- Are statements of expectation, enforced by standards, and further implemented by procedures.
- Decided by external influencers, such as statutory, regulatory, or contractual obligations. These are commonly the root causes of a policy's existence.

- Examples of policies the school must have in place include a:
    - Cyber Safety Awareness Policy – Aims to inform all users of the result of their actions regarding security and privacy.
    - Acceptable Use Policy (AUP) - Ensures all employees and learners know the acceptable use of technology.

7.1.2. Cyber safety standards

- Standards are formally-established requirements with regard to processes, actions, and configurations.
- Exceptions are always to standards and never to policies. If a standard cannot be met, it is usually necessary to implement a compensating control to mitigate the risk associated with that deficiency.
- Can have a level of complexity and technical understanding – requires training and awareness.
- Examples of standards the school must have in place include networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.

7.1.3. Cyber safety procedures

- Procedures are a formal method of completing something based on a series of actions conducted in a certain manner or way.
- Procedures are the responsibility of the asset custodian (typically owner of the application or process) to build and maintain in support of standards and policies.
- Cyber Safety Procedures can be complex and technical – requires training from the service provider.
- An example of procedures the school must have in place includes:
    - Incident management procedures that direct members of the incident response team on how to detect an incident and how to respond accordingly. Specific examples, such as phishing or ransomware, may be covered.

7.1.4. Cyber safety guidelines

- Unlike standards, guidelines allow users to apply discretion or flexibility in their understanding, implementation, or use.
- Guidelines are generally recommended practices based on industry recognised practices or cultural norms within an organisation.
- Cyber Safety Guidelines can be complex and technical – require training from the service

provider.

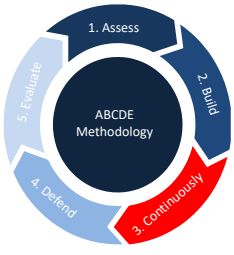
- An example of a guideline the school could have in place includes password management conventions, as decided by the school, for example, that:
    - User passwords must adhere to a minimum length and format as defined by current password guidelines.
    - User chosen passwords must include at least one upper case letter, one lower case letter, and one number.
    - User chosen passwords must be at least 8 characters in length.
    - User chosen passwords must not have consecutive duplicate characters such as 99 or ABC.

The following areas may be addressed in creating policies, standards, procedures and guidelines:

- Establishing prior cyber safety awareness, knowledge and skills.
- Improving awareness among learners.
- Informing parents (or caregivers)and obtaining their written consent.
- Skills and development training of teachers.
- Skills and development training of administrative staff.
- Measuring and Monitoring.
- Evaluation.
- Incident reporting systems.
- Involvement of external role players.

These cybersecurity policies, standards, procedures and guidelines may apply to any person, staff, volunteer, or visitor, who has access to a school's personally identifiable information (PII) whether in electronic or paper format.

8. Phase 3: Continuously growing a cyber safety culture



The purpose of this phase is to continuously educate relevant stakeholders, namely teachers, administrative staff, learners and parents (or caregivers). Schools have a duty of care (in loco parentis) to take reasonable steps to protect learners from any harm that should have reasonably been foreseen.

These steps must be:

- Planned, implemented, monitored and communicated to all involved.
- Supported by obtaining buy-in from all stakeholders (administrative staff, teachers, learners and parents (or caregivers).

- Focussed on improving cyber safety awareness for all stakeholders.

The school should consider establishing a cyber safety awareness programme to achieve these goals.

8.1. What is a cyber safety awareness programme?

Cyber safety is not just a technical problem. It is also a people problem. Keeping the people side of the security equation strong requires that all people in the school are aware of the risks. A cyber safety awareness programme ensures that everyone at the school has an appropriate level of know-how about cyber safety, along with an appropriate sense of responsibility.

8.2. What belongs in a cyber safety awareness programme?

A good cyber safety awareness programme should have these key components.

8.2.1. Communication

- Security and cyber safety need to become a regular part of the conversation at the school. The key is to ensure that communication is clear for the various stakeholders, regular, relevant, and interactive.
- This can take the form of emails, presentations, workshops, learner-led initiatives, or some combination of the above.

8.2.2. Checklist(s)

- Checklist (or a series of checklists) — that can be used to ensure that cyber safety awareness practices are being actively spread throughout the school, in a systematic manner. This checklist could include:
    - What to do when a new person starts (and when they leave).
    - When and how often to remind people of security protocols.
    - What to do when an incident takes place.
    - How to communicate with parents in the event of a breach.

8.2.3. Content

- A selection of relevant content about cyber safety is also needed. The purpose of this is so that the awareness team can refer to it when needed and that it can be utilised when training and communicating.
- Depending on the school's plan and unique security requirements, these could include:
    - A security handbook (this can be a PDF sent to everyone or part of an intranet).
    - Training programmes (both for new hires and ongoing employee education).

- Relevant animated videos, posters, games either purchased from a service provider or developed by learners, either formally in class or as part of a Cyber Security Club.

8.3. How frequently should a school conduct cyber safety training?

Below is a list of key times when it is vital for a school to offer cyber safety training to staff and learners:

- At planned / regular intervals throughout the year - either yearly or quarterly.
- When there are new-joiners.
- After an incident occurs.

Each of these moments provides a different opportunity to train people on specific aspects or to offer them real-world examples of what to do and what not to do

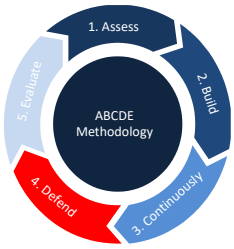
8.4. Cyber safety guidelines specifically for teachers

Digital technology and cyberspace have become an integral part of teaching and learning; however, it does not come without challenges. Staff members are guided by professional conduct outlined in the Department of Basic Education policies, as well as standards set by the leadership teams of each school.

As role-models for learners, staff have a responsibility to uphold school values and ensure the online environment is a positive place to connect, learn and enjoy. This implies modelling safe, responsible and ethical use of digital technology and online spaces, including social media.

The school is responsible for and directly oversees the use of devices, systems and principles in place designed to support learning and teaching.

9. Phase 4: Defend



The purpose of this phase is to empower schools to respond effectively to any cyber safety incidents that may arise. The nature and scope of the duty in these circumstances will vary according to several factors, for example, the role and responsibility of the teacher, and whether the incident occurred inside or outside of school hours.

9.1. Incident management plan

The purpose of an Incident Management Plan is to enable the school to manage cyber safety risks by streamlining the response during an incident. The plan defines:

- What constitutes a cyber safety incident.
- The various categories of incidents.

- Structured approaches to prioritising and managing security incidents.
- Roles and responsibilities for incident responders and those they interface with.
- Developing a Risk Register of cyber safety risks.

9.2. Incident management roles and responsibilities

The table below outlines the typical people within an incident response team, as well as their associated roles and responsibilities when it comes to incident management.

Team	Description
End User	The end user will report suspicious behaviour or incidents. This could be a teacher, learner or external stakeholder.
Nominated Contact Personnel	Contact personnel will receive information about potential cybersecurity incidents from channels such as telephones, email, monitoring systems, and assign them to relevant personnel.
Incident Team Leader	Takes a lead role in the incident management process. Responsible for confirming, analysing, containing, eradicating and recovering from incidents. Could be a distributed team augmented with specialist service providers.
IT Teacher or External Provider	Will perform technical assistance during an incident. Monitor operational systems and flag any suspicious events.
Principal or Nominated Senior Manager	Ultimately accountable for incident management. Responsible for decision-making.
Legal, HR, PR	Involved in communication activities during the incident response process. Assisting with disciplinary processes where security policies have been flouted by employees or learners. Provide legal advice as appropriate.

Table 1: Cybersecurity Incident management roles and responsibilities

An Incident Response Team ("IRT") is defined as the group of individuals in charge of executing the school's Incident Response Plan – reporting into the Cyber Safety Committee. IRT members are responsible for the detection, containment and eradication of cyber incidents as well as for the restoration of any affected IT systems.

9.3. Developing an incident management plan

A documented Incident Management Plan helps schools respond quickly by streamlining decisions, outlining processes, and defining appropriate use of the technologies available.

There are six phases, as defined by best-practice, of incident response that schools should plan for:

1. **Preparation** - Preparing the incident response team to handle potential incidents. This includes training, equipping, and practising.
2. **Identification** - Detecting and deciding if an incident fulfils the conditions to be considered a security incident by the school and its severity.
3. **Containment** - Containing the incident by isolating compromised systems to prevent future damage.

4. **Eradication** - Detecting the cause of the incident and eliminating the threats from affected systems.
5. **Recovery** - Restoring affected systems and making sure no threat remains.
6. **Lessons learned** - Analysing the incident, updating the response plan, and completing incident documentation.

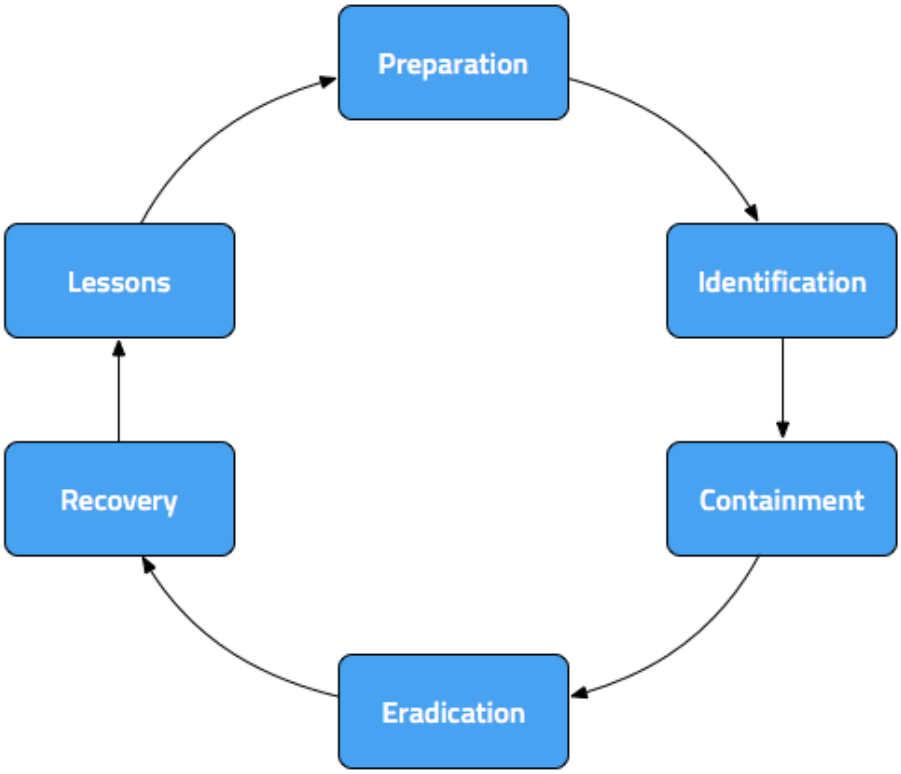


Figure 5: Incident management steps

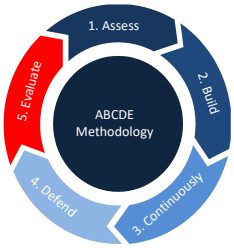
9.4. Review of the incident management plan

This Incident Management Plan is intended to be a 'living' document and as such, should be reviewed regularly. The plan should be formally reviewed annually and, where practicable, rehearsed at least once a year in the form of a drill. The drill may be in the form of a walk-through or mock disaster.

Formal review should take place as follows (whichever occurs first):

- At least every twelve months.
- Whenever the plan is invoked, and updates and corrections are identified.
- In the event of substantial changes to the school environment.

10. Phase 5: Evaluate



The school should have a Monitoring, Reporting, Evaluation and Learning Plan (MREL plan) to evaluate the overall cyber safety programme's sufficiency and transfer of skills across time.

The MREL plan outlines the following:

1. **Stakeholder** - Individuals or entities with whom the school should communicate, both internally and externally.
2. **Objective** - Goals or requirements the school wants to meet.
3. **Message** - Information the school wants to deliver, specific to the role-players and objectives.
4. **Medium** - Available communication vehicles to deliver the message to target stakeholders.
5. **Frequency** - Timeline/due dates for the delivery of each message.
6. **Communicator** - Person or team responsible for communicating the cyber safety messages.
7. **Results** – Was the school successful? Did the school achieve the desired results? How can the school improve the process?
8. **Metrics** – Measurement, reported findings and improvements.

An example MREL may outline the following:

Stakeholder	Objective	Message	Medium	Frequency	Communicator	Results
Individuals or entities with whom the school should communicate, both internally & externally	Goals or requirements the school wants to meet	Information the school wants to deliver, specific to the stakeholder and objective	Available communication vehicles to deliver the message to target stakeholders	Timeline/due dates for the delivery of each message	Person or team responsible for communicating the message	Was the school? Did the school achieve the desired results? How can the school improve the process?
Learners	Cyber safety awareness aligned aimed at learners. Increase awareness on risks, threats and trends as well as increase knowledge.	Personal implications of not keeping cyber safety in mind. **Awareness Themes** Introduction to Cyber Safety.	**Introduction Theme:** Video Poster Cartoon Word Search	Suggest dividing into the 4 school terms.	Teachers / Parents (or caregivers).	Increase in cybersecurity awareness and incident reporting. A decrease in cybersecurity Incidents.
Principals	Provide guidance on how to establish and create a cyber safety culture within the school.	Guidance on how to establish and create a cyber safety culture within the school.	Workbook 3	Annually	Principals.	Successful implementation of knowledge gained from workbook 3.

11. Appendix A: Example of the responsibility and reporting of teachers, learners and parents

This section focuses on the aspect of cyber safety awareness requirements for each stakeholder in two steps – namely the responsibilities required, and what is required to report an incident.

11.1. Cyber safety guidelines specifically for teachers

Step 1: Device and App Responsibilities:

- **Password security:** Keep your passwords private and ensure that they are strong. Do not use others' login details or share your login details.
- **Log out when leaving your computer:** This is an important security measure for keeping content and sites safe.
- **New software:** Always ask for permission from the school IT manager/team before downloading software to the school network, or devices that connect to the network to make sure that they do not interfere with the school's equipment/network or the online security of another person.
- **Personal device security:** Staff members are responsible for the security settings of their own devices. Staff should aim to ensure any device used within the school has suitable security software, that all software is up to date – and that the devices are free from any harmful content which may accidentally be exposed during use.
- **Offensive content:** Do not bring to school, or add to school systems, content that is deemed inappropriate for the learners.
- **Recognise copyright and intellectual property:** Follow copyright and intellectual property obligations by accrediting references, images, text, audio and video appropriately.

Step 2: Communication Responsibilities:

- **Protect your reputation:** Social media may reveal our private lives to our professional communities. Be careful of how and where you post personal content that could compromise your reputation as a teacher.
- **Share with care:** our right to share our views is protected by freedom of expression. However, it does not protect people against the harm expressing those views may cause. Be careful of creating or forwarding content that could be considered harmful, inappropriate or hurtful to any member of the school community.
- **Protect privacy:** Do not share another person's sensitive personal information in any digital communication. Also, be sure to evaluate what information you share about yourself online. Messages you send in private may be made public by others.
- **Keep it offline:** Do not participate in school community disputes online. Disputes will arise between parents or learners, from time to time, within the school community and may take

place online. The school has processes and channels in place for complaints and disputes to be handled.

- **Get consent for content:** Only share and record photo, video or audio content if the people in it are aware of it and have provided their consent.

Step 3: Incident Reporting

Incident Responsibilities:

Despite people's best intentions when it comes to the advantages technology offers, sometimes there will be challenges or harm will occur within an online community. Staff members are required to action incidents regardless of whether they were purposeful or accidental. Even incidents that occur outside of the school or outside of school hours are required to be actioned if they are negatively impacting learner learning.

- **Receiving reports:** Incidents of cyberbullying or harm are not tolerated at the school, and learners are required to report them to any staff member. Staff are required to obtain these reports and to take appropriate steps.
- **Responsibility to report:** If you become aware of or suspect an online incident with the potential to cause harm to a member of the school community, you must act upon it. Incidents impacting learners within your care must be recorded and the appropriate action must be taken. Risk to other members of the school community should be escalated appropriately.
- **Supporting learners:** Staff members are expected to prioritise learner safety and to escalate reports appropriately. Learners should be encouraged and, if necessary, helped to preserve evidence of what is happening so that an investigation can occur. Learners should be discouraged from engaging with the person(s) in order to protect themselves from further risks.
- **Abuse of staff:** Online harassment and abuse of staff is not tolerated by the school. Any staff member who is subjected to online harassment or abuse must be urged to seek support from school management. The school must report or mediate disputes to external authorities as appropriate.
- **Incidents involving staff:** When a staff member becomes aware of any online incident or breach of these guidelines that have the potential to cause harm to a member of the school community, they are responsible for reporting it to school management.

11.2. Cyber safety guidelines for learners

This section outlines the responsibilities of learners as members of our online community. It can also be used to support discipline processes when necessary.

The school should directly oversee and is responsible for, the use of devices, systems and principles in place designed to support learning. This section outlines what the school considers as appropriate professional conduct.

Step 1: Learner Responsibilities:

- **Remain positive:** Always respect others online and communicate constructively. Do not publish or create indecent, threatening or offensive content.
- **Protect privacy:** Do not divulge sensitive personal information about another person or yourself in any communication. This includes sharing passwords, accessing online sites or devices belonging to others, without consent, as well as taking screenshots and sharing this without consent.
- **Act cautiously:** Anything you do or post online can impact other people's thoughts of you. Similarly, always carefully analyse whether the information you see online is true. If you are not sure of something, talk to an adult.
- **Avoid online bullying:** Forwarding or creating content that is harmful, inappropriate or hurtful is never okay at any time, and may breach legislation. If you are harassing others by sending multiple messages, this too is considered cyberbullying and is unacceptable.
- **Be security smart:** Keep personal information safe and secure by utilising strong passwords and not sharing them with others.
- **Check consent:** Before downloading software onto devices or the school network, ask for permission. Interfering with the school systems, equipment/network, digital technologies, or the online security of another person is never appropriate.
- **Recognise the work of others:** Follow copyright and intellectual property requirements by accrediting references, images, text, audio and videos appropriately.
- **Respect the rights of others:** Only share and record photo, video or audio content if the people in it are aware of it and have provided consent.
- **Use personal devices sensibly:** Keep your device(s) on silent during school hours and only use it as indicated by the school, unless you have been given permission by a school staff member to use it during lessons.
- **Seek help:** At times, you or someone you know will come across inappropriate or hurtful online content and behaviours, or feel unsafe. If this happens, talk to a trusted adult about what can be done.

Step 2: Incident Responsibilities

- **Online bullying:** Incidents of online bullying (cyberbullying) or harm will not be tolerated at the school. If you or somebody else is being harmed or bullied online, it is never okay at any time. It is important to keep the evidence of what happened to you or someone so that this can be investigated. Do not place yourself at further risk by continuing contact with the person(s) who are bullying online, or creating hurtful or harmful content.
- **Report a problem:** You should report suspicious behaviour or an online incident as soon as you can to the nominated school contact or a trusted adult. Once the school is made aware of a problem, the problem will be assessed, and the school will work to resolve it.

11.3. Cyber safety guidelines for parents / caregivers

The Internet, digital technologies and social media tools present learning spaces that are present both inside and outside of the school's physical environment. Spaces such as recommended websites, a school Intranet, some blogs and wikis, must be available to learners in their homes, inside and outside of school hours. Schools have a responsibility to inform parents (or caregivers) of any learning spaces that they make available to learners, as well as the expected behaviours and protocols surrounding their use.

Parents (or caregivers) play an important role in assisting their children with using digital technologies safely and responsibly. Schools may assist parents by providing them with useful information about emerging and existing technologies, including them in the development and review of policies and inviting them to information sessions or distributing cyber safety guidelines for learners.

Parents (or caregivers) are, however, a learner's first and primary role model when it comes to behaviour – in the real world or online. Times have changed – parents are urged to embrace their children's world.

Step 1: Parent (or Caregiver) Responsibilities:

- **Manage social media:** Be a positive role model by demonstrating respectful and responsible behaviours when communicating about your child's school online.
- **Think before you type:** Avoid posting negative comments online that identify the school or individuals. Consider these points:
    - Am I being a good role model for my child?
    - Will this information reflect badly on me?
    - Does the school community or individual really need to know this information?
    - Is this information relevant, helpful and positive?
    - Will this information upset or embarrass the school community or an individual?
    - Am I making the situation worse?

- Use parental controls on computers and devices: Teach children to respect their devices and have 'screen free' time.
- Encourage cleanliness: You encourage your children to maintain good hygiene or clean their rooms – ensure they also maintain a clean digital footprint which increasingly may become just as important as a clean credit score for future job applications.
- Adhere to the school's cyber safety awareness policies and procedures.
- Ensure that learners understand and adhere to the school's cyber safety awareness policies and procedures.

Step 2: Incident Responsibilities:

- Report all cyber-related incidents to the school within as short a time as possible to allow the school leadership or the Cyber Safety Awareness Committee to respond as per defined procedures.

12. SA compliance summary

Department of Social Development
National Cybersecurity Policy Framework Promotion of a Cybersecurity Culture 1 4. 1 To effectively deal with Cybersecurity, it is prudent that civil society, government and the private sector play their part in ensuring South Africa has a culture of Cybersecurity. Critical to this is the development of a culture of Cybersecurity, in which role players understand the risks of surfing in cyberspace. To facilitate the building of a Cybersecurity culture, the NCPF provides for inter alia: 14.1.1 Implementing Cybersecurity awareness programs for private sector, public sector and civil society users; 14.1.2 Encouraging business to develop a positive culture for Cybersecurity; 14.1.3 Supporting outreach to civil society, children and individual users; 1 4.1.4 Promoting a comprehensive national awareness program and guidelines; for the protection and welfare of children
Child Care Act, 1983 For the protection and welfare of children Terms: "care", in relation to a child, includes, where appropriate - (b) safeguarding and promoting the well-being of the child; (c) protecting the child from maltreatment, abuse, neglect, degradation, discrimination, exploitation and any other physical, emotional or moral harm or hazards;
Department of Communication
The Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002 ("RICA") Regulates the interception and monitoring of direct and indirect communications. RICA contains exceptions relating to where interception and monitoring takes place with the consent of the parties involved or where it is carried out by law enforcement personnel.
Electronic Communications Act of 2006 Regulates electronic communications and transactions and is the primary legislation currently in force which criminalises cyber-related offences.

The Cybercrimes Bill

Aims to provide for the criminalisation of a broad range of cyber-related crimes.

a) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which is harmful, is guilty of an offence.

b) Intimidates, encourages or harasses a person to harm himself or herself or any other person

c) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not give his or her consent to the making available, broadcasting or distribution of the data message, is guilty of an offence.

Protection of Personal Information Act (PoPIA)

PoPIA is data protection legislation primarily modelled on the EU general data protection laws. Importantly, it establishes the Information Regulator and confers various powers, duties and functions including monitoring and enforcing compliance by public and private bodies and handling complaints in respect of contraventions of PoPIA.

It also establishes a comprehensive compliance framework and places cybersecurity obligations on responsible parties to secure the integrity and confidentiality of personal information in its possession or control by taking appropriate, reasonable technical and organisational measures to prevent unlawful access.

Films and Publications Act, 1996 (Act 65 of 1996)

Section 24B of the Act, which deals with child pornography and the sexual exploitation of children, is repealed.

Department of Education

Child Justice Act, 2008 (Act 75 of 2008)

Schedules 2 and 3 are amended to provide for the sentencing of child offenders who commit cyber offences.

32 OF 2007

Compelling or causing persons 18 years or older to witness sexual offences, sexual acts or self-masturbation, exposure or display of or causing exposure or display of genital organs, anus or female breasts (‘flashing’), child pornography to persons 18 years or older or engaging sexual services of persons 18 years or older

Constitution of South Africa, 1996

The right to privacy is enshrined in section 14 of the states that “everyone has the right to privacy, which includes the right not to have their privacy of their communications infringed”.

13. References

Department of Basic Education. 2018. Guidelines on e-Safety in Schools: Educating towards responsible. and ethical use of ICT in education. https://www.education.gov.za/

International Organization for Standardization.2012. First Edition: Information technology - Security techniques - Guidelines for cybersecurity. ISO/IEC 27032:2012. Multiple. Distributed through American National Standards Institute (ANSI). Washington, DC. Headquarters. Available at:httpsat: https://www.iso.org/about-us.html

Kritzinger, Elmarie, 2017. Cultivating a Cyber-Safety Culture among School Learners in South Africa. Available at: <https://www.tandfonline.com/doi/abs/10.1080/18146627.2016.1224561>

[Accessed 31 March 2020]

South African Department of Communications, Films and Publications Act (65/1996). Classification guidelines for the Classification of Films, Interactive Computer Games and certain publications. Available at <http://www.gpwonline.co.za/Pages/default.aspx> [Accessed 2 April 2020]

Victoria State Government, June 2020,

https://www.education.vic.gov.au/about/programs/bullystoppers/Pages/princyber.aspx

[Last accessed 30 June 2020]

Netsafe Schools, June 2020,

https://www.netsafe.org.nz/the-kit/policy-user-agreements/online-safety-policy/

[Last accessed 30 June 2020]

Fuse Education & Training, June 2020,

https://fuse.education.vic.gov.au/pages/View.aspx?id=8edd3b8f-512e-48e7-9027-6c4e7877496b&Source=%252fpages%252fResults.aspx%253fs%253dgo%252bfigure

[Last accessed 30 June 2020]

Threatstack, July 2020

https://www.threatstack.com/blog/how-to-implement-a-security-awareness-program-at-your-organization

TechRadar, July 2020

https://www.techradar.com/news/improving-cybersecurity-in-education-systems

Infocyte, July 2020

https://www.infocyte.com/blog/2019/09/04/a-practical-guide-to-building-a-cyber-incident-response-team/

JOIN US ON A
CYBER SAFETY AWARENESS JOURNEY

Taking a trip into cyberspace? Decline social media invitations you are not sure about.

No to cyberbullying.

Using the Internet is fun. Enjoy it most by keeping yourself safe. Be smart, responsible, and safe online!

Secure your profile on social networking sites. Secure your smart device.

Be alert behind your screen. Always protect your personal information.



CYBER CADETS

Guiding You Through Cyberspace

British High Commission Pretoria

UNISA | college of science, engineering and technology

For further information visit:
https://www.cybersecurityhub.gov.za/cyberawareness/
http://cyberaware.co.za

CYBERSECURITY HUB

British
High Commission
Pretoria

UNISA | college of science, engineering and technology

For further information visit:
https://www.cybersecurityhub.gov.za/cyberawareness/
http://cyberaware.co.za

CYBERSECURITY HUB