CHALCOT LODGE PRIMARY SCHOOL

POLICY: Information Security

Ratified

22/03/22

Information Security — Info Safe

Policy

The purpose of this policy is to make sure that schools manage and share information appropriately and securely in order to meet information security obligations and to appropriately protect staff, students and their families.

Summary

- Information security aims to protect the confidentiality, integrity and availability of school information. This includes the consideration of privacy compliance when dealing with personal information. Refer to Privacy and Information Sharing Policy for more information about privacy and information sharing.
- Principals must establish appropriate practices to protect critical and sensitive information. All staff should consider:
    - what information they have
    - how sensitive the information is
    - where it is stored
    - who has access to it
- Principals are to make sure that information security risks and issues are appropriately managed by seeking advice from the InfoSafe team.

Details

The following information provides an overview of the key practices schools must implement to protect the confidentiality, integrity and availability of school information.

For more detailed information on implementing these information security practices, refer to: Information Security (InfoSafe): Guidance for Victorian Government Schools (login required).

Behaviours — Being InfoSafe

Schools must make sure that the protection of information is embedded in all aspects of school operations as outlined in this policy and accompanying Information Security Standards and guidance materials. The consequences of an information security breach can be far reaching, potentially affecting staff, students and families.

Priority Actions:

1. Ensure that priority actions from this policy are considered in appropriate local school practices and IT Committees.
2. Staff are encouraged to complete the Information Security for School Staff eLearning module (login required) on an annual basis.
3. Establish and maintain an InfoSafe culture by promoting this policy and through ongoing conversations.

Risks — Understanding your information risks

Schools must adopt a risk-based approach to information security by periodically assessing themselves against a set of common, published risks and associated treatment plans. This will enable school treatment plans to be prioritised and actioned based on the extent of the risk.

Priority Actions:

1. Consider the IT environment, online tools and the nature of the information at your school.
2. Consider the most common school information security and privacy risks and their relevance at your school.
3. Refer to the Pre-populated InfoSafe School Risk Document.

Access — Identify the appropriate access for the information at your school

Schools must make sure that access to information is authorised for individuals based upon their role and function within the school environment. Failure to assign the right level of access to information to the right role may result in an information security or privacy breach.

Priority Actions:

1. Identify who has access to sensitive information and who has privileged accounts at your school. Refer to Privacy and Information Sharing Policy for more information.
2. Establish a process to capture and regularly review school and Department staff, and third-party access, including parents, volunteers and contractors.
3. Establish a process to enforce need-to-know access to sensitive information (revoke access in a timely manner).

Incidents — Reporting incidents

Schools must report any potential or confirmed information security incidents as soon as possible to the IT Service Desk 1800 641 943 or email servicedesk@edumail.vic.gov.au (or via their Specialist Technician) as soon as they are identified.

Problems that are not reported immediately can grow bigger and more difficult to contain, and early detection helps to mitigate any potential harms resulting from the incident. Some cyber-security incidents may also reveal a risk (such as a virus) that other schools can then prepare against.

Priority Actions:

1. Make sure all staff know what constitutes an information security incident – refer to Definitions below.
2. Reinforce the importance to all staff of reporting incidents.
3. The principal must ensure that the incident is reported and then respond to the incident as advised by the Department.

Networks — Securing ICT networks

Schools must maintain a secure ICT network by following Departmental requirements and adopting appropriate technical controls. Without these controls the school information and systems will be vulnerable to cyber-attacks.

Priority Actions:

1. IT Technicians in schools (whether engaged through the Technical Support to Schools Program or directly by the school) need to regularly review network configuration and anti-virus and patching arrangements as set out in the Tech Campus (login required, access limited to Department engaged technicians).
2. Technicians need to confirm the school's Internet Service Provider (ISP) arrangement meets the requirements of the DET standards.

Storage — Identifying and storing your information appropriately

Schools must identify their critical and sensitive information and store it in approved and trusted locations.

Priority Actions:

1. Identify and document assets holding sensitive and critical information. Refer to School Administration Systems Policy (previously called CASES21 Policy) for all mandated DET ICT school administration systems. Refer to the Pre-populated Risk Document to assist with documenting assets.

2. For systems holding personal information, ensure you have completed a Privacy Impact Assessment. Refer to the Privacy and Information Sharing Policy for information about Privacy Impact Assessments.
3. Review school processes to identify where data is held long-term.

Physical — Physical protection

Schools must protect information and ICT equipment by housing all ICT infrastructure (servers and network equipment) and personal computers, when not in use, in a locked and secured location with restricted access. Schools should also monitor visitor entry to the school premises and authorise entry into infrastructure and records storage locations.

Priority Actions:

1. Ensure the school follows both their local visitors policy and the Department's Visitors in Schools Policy.
2. Make sure that sensitive information (digital and hard copy) and ICT equipment is housed in physically secured locations. Refer also to Records Management — School Records.

Awareness — Training and awareness

Schools must encourage staff to be vigilant and aware of the ongoing need to protect sensitive school information and systems. Staff should complete the Information Security for School Staff e-learning module (login required). Schools should act on Department information and directions about emerging cyber security threats.

Priority Actions:

1. Continue to drive the completion rate of the Information Security for School Staff eLearning module and encourage all staff to complete the module annually.
2. Ensure the induction process for new staff, including contractors and casuals, includes the Information Security for School Staff eLearning module.
3. Regularly communicate, affirm and review security obligations for staff (and target specific roles that have access to sensitive information).

Sharing — Sharing information safely

Schools must follow Department policies for sharing personal or sensitive information with other schools or anyone external to the school.

Priority Actions:

1. Identify which personal and sensitive information is regularly shared or likely to be shared (typically personal data of staff or students, but potentially other categories of information e.g. financial, commercial). Refer to Requests for Information about Students and Privacy and Information Sharing.

2. Make sure staff are aware of Department policies and local procedures for sharing information. Refer to Privacy and Information Sharing and Requests for Information about Students.
3. Use only approved tools to transmit sensitive data, closely manage distribution lists.

Suppliers — Externally sourced systems security

Schools and the Department must ensure the security of new systems and the suppliers who provide them.

Priority Actions:

1. Seek advice from the InfoSafe team to ensure all new systems meet Information Security and ICT security requirements.
2. For those systems holding personal information, conduct a Privacy Impact Assessment (PIA) which includes a security assessment for that system.

Definitions

Information security incident
Indicators of a potential or actual information security incident are:

- emails from unexpected or unidentifiable senders
- unexpected emails from people that you do know
- requests for information from unknown sources
- inability to access systems
- inability to access files or documents
- unusually slow systems or unexpected and strange behaviour of PCs and devices

Personal information
Personal information is recorded information or opinion about an identifiable individual. It can be almost any information linked to an individual, including name, address, sex, age, financial details, marital status, education or employment history. De-identified information about individuals can also be personal information if it has the potential to be re-identified.

Sensitive information
For the purpose of this policy and associated guidance material, sensitive information in schools includes but is not limited to the following:

- student information including name address and date of birth
- student academic records, progress reports, assignments and assessments
- student health and medication information
- student information pertaining to family circumstances including Intervention Orders and Family Court decisions
- student class photographs and individual images
- parents' names, address, phone number, email address and custody instructions
- teachers personal information

- parents’ banking and credit card information and hard-copy records
- school financial information
- tendering and procurement documents
- vendor invoices, contacts and accounts payable and receivables