CYBER SECURITY POLICY

Overview:

Policy	Cyber Security
Version	Version 1
Date of Approval	TBA
Effective date	30/06/2023
Date for Review	2023 Revised annually
Policy Officer	Executive Director

The purpose of this Cyber Security Policy is to establish guidelines and procedures to ensure the safety and security of students, staff, visitors, and the overall school landscape to maintain a conducive learning, leading and living environment. This policy outlines (a) Information and Technology assets that require protection; (b) Threats to those assets; (c) Principles and procedures for protecting those assets and Kildare Ministries and (d) processes for detecting and responding to a cyber security incident.

Kildare Ministries are committed to providing a secure environment that is caring, nurturing and safe for the children, young people, vulnerable adults and staff participating in our ministries and all its programs. To enable this, Kildare Ministries has introduced Cyber Security Principles, Procedures and Control Guidelines to assist the organisation in providing physical and logical security.

Content:

Policy	The purpose of this policy is to set out Kildare Ministries approach to implementing a culture of cyber security across all areas of the organisation providing services to children, young people, vulnerable adults and staff, to ensure the safety, security and wellbeing of all within Kildare Ministries. Each person involved in Kildare Ministries work has a duty to know, understand and comply with this policy, to be able to recognise, manage and respond to cyber security threats.
Scope	The cyber safety and protection of children, young persons and vulnerable adults in Kildare Ministries is the responsibility of everyone involved with the organisation including Trustees, staff, volunteers, board members and contractors, whether or not they work in direct contact with children, young people or adults at risk. The following information and technology assets are in scope for this policy and require protection from unintentional and / or unauthorised access, use, disclosure, disruption, modification, or destruction: • **Information Assets:** ○ Student information (name, DOB, address, email address, contact number, report information, parent details incl

	names addresses, passport details for travel purposes, medicare, medical conditions, alumni, psychologist reporting / court orders, health centre visits etc) ○ Employee Information (name, DOB, address, email address, contact number, payroll / salary details, work related injuries, general applicant information, disciplinary meetings and file notes, emergency contact details, qualifications, medical leave) ○ Financial information (bank records, account numbers, financial results, debt information) ○ Examination details (Exam questions, answers) ○ Contractors (including contract information Ts and Cs), working with children requirements ○ Community (profiling, campaigns, projects, ex-students / relatives) contacts including names, contact details, email addresses, volunteers ○ Vulnerable adults (name, date of birth, address, health records) • **Technology Assets:** ○ Student: Laptops, desktops, mobile devices ○ Staff: Laptops, desktops, mobile devices ○ Network Access Storage ○ Servers (domain controller, email, routers) ○ Printers ○ Surveillance systems (cameras, alarms, sensors) ○ Network (Wifi, physical) ○ Phone systems ○ Clous based solutions ○ Finance Management System ○ Learning Management System. • **Cyber Security Threats:** ○ Internal ▪ Unintentional • User discloses data by mistake e.g. incorrect email of student data ▪ Unauthorised • Student endeavours to access information on the network without approval • Malicious user leverages existing access credentials to access data without approval. ○ External ▪ Unauthorised • Malicious user leverages external access ports / channels to access data without approval (e.g. wifi hack)
PRINCIPLES	**THE PRINCIPLES, PROCEDURES AND CONTROL GUIDELINES ARE**

	CLOSELY ALIGNED TO INDUSTRY STANDARDS, DESIGNED TO MANAGE THE EVOLVING CYBER SECURITY THREAT LANDSCAPE WHICH KILDARE MINISTRIES FACES.
PRINCIPLE 1	COMMITTED LEADERSHIP, GOVERNANCE AND CULTURE *Promoting a culture of cybersecurity awareness among students and staff through training programs, workshops, and ongoing education. Students and staff should be aware of good practice, potential threats, and their roles in maintaining security.*
PRINCIPLE 2	RISK ASSESSMENT *Conducting regular risk assessments to identify and evaluate potential cybersecurity risks and vulnerabilities. This helps in prioritising resources and efforts based on the level of risk.*
PRINCIPLE 3	ACCESS CONTROL *Implementing effective physical and logical access controls to ensure that only authorised individuals have access to Kildare Ministries systems, data, and resources. This includes user authentication, strong passwords, access privileges, and regular reviews of access rights.*
PRINCIPLE 4	INCIDENT RESPONSE AND MANAGEMENT *Establishing procedures for detecting, reporting, and responding to security incidents promptly. This includes incident response plans, escalation processes, and coordination with relevant stakeholders.*
PRINCIPLE 5	DATA PROTECTION *Defining guidelines for the protection of sensitive information, such as personally identifiable information (PII), financial data, and intellectual property. Encryption, data classification, data retention standards, and secure disposal practices are examples of data protection measures.*
PRINCIPLE 6	NETWORK AND SYSTEM SECURITY *Implementing technical controls to safeguard networks and systems. This includes firewall configurations, intrusion detection and prevention systems, regular patching, and secure network architecture.*
PRINCIPLE 7	PHYSICAL SECURITY *Addressing physical security measures to protect facilities, equipment, and assets. This includes access controls, surveillance systems, environmental controls, and proper disposal of physical media.*
PRINCIPLE 8	THIRD-PARTY SECURITY *Defining security requirements for third-party vendors and contractors who have access to Kildare Ministries systems or data. This includes due diligence in selecting trustworthy partners and contractual agreements specifying security responsibilities.*
PRINCIPLE 9	REGULAR AUDITING AND MONITORING *Conducting regular audits, vulnerability assessments, and security monitoring to ensure compliance with policies and detect any potential security breaches or weaknesses.*
PRINCIPLE 10	REGULATORY COMPLIANCE *Adhering to relevant legal and regulatory requirements specific to the*

	Kildare Ministries. This includes data protection regulations (e.g., Australian Privacy Principles), industry-specific standards (e.g., PCI DSS), or government regulations.
Procedures	**1. Physical Access Control** 1.1 All entrances and exits to the school premises will be monitored and controlled. 1.2 Visitors must sign in at the main office, provide identification, and wear a visitor badge while on the premises. 1.3 Student release procedures will be strictly enforced, requiring authorised individuals to present proper identification and follow designated protocols. 1.4 Any changes to student custody arrangements must be accompanied by official documentation. **2. Cyber Emergency Preparedness** 2.1 The school will maintain an up-to-date emergency response plan that includes procedures for various incidents such as fire, medical emergencies, natural disasters, and lockdowns. 2.2 Regular drills and training sessions will be conducted to ensure students and staff are familiar with emergency procedures. 2.3 Emergency contact information for students and staff will be collected and kept up to date. 2.4 Communication systems (e.g., public address systems, emergency notification systems) will be in place to relay important information during emergencies. **3. Surveillance and Monitoring** 3.1 Closed-circuit television (CCTV) cameras may be installed in strategic locations within the school premises to monitor and deter unauthorised activities. 3.2 Any surveillance systems will be used in compliance with applicable privacy laws and regulations. 3.3 Monitoring systems will be regularly maintained, and recordings will be retained for a specified period as per legal requirements.

4. Information Security

4.1 Physical access to information and technology assets, will be restricted to authorised personnel only.

4.2 Network security measures will be implemented to safeguard against unauthorised access, malware, and other cyber threats.

4.3 Regular data backups will be performed to ensure the availability and integrity of critical information assets. Access to backups will be restricted to authorised personnel.

5. Incident Reporting and Response

5.1 All security incidents, accidents, or breaches must be promptly reported to the designated authority.

5.2 An incident response plan will be in place to address security breaches, including appropriate notification and escalation procedures.

5.3 Investigation procedures will be conducted to identify the cause of security incidents and implement corrective actions.

6. Cyber Safety

6.1 All staff members will receive commensurate training on identifying and reporting potential safety concerns, including cyber abuse or neglect.

6.2 Adequate supervision will be provided during school hours, including in common areas, playgrounds, and during transportation.

6.3 Students will be educated on personal safety and encouraged to report any suspicious cyber activities or concerns to school authorities.

7. Collaboration with Law Enforcement and External Agencies

7.1 The school will maintain a positive working relationship with local law enforcement agencies and emergency responders.

7.2 Regular communication and collaboration will occur to address security concerns and share relevant information.

7.3 School administrators and designated personnel will

cooperate with law enforcement in conducting investigations related to security incidents.

8. Third Parties

8.1 **Contractual Agreements:** Clearly define the security expectations and requirements in contractual agreements with vendors. This should include clauses related to data protection, confidentiality, access controls, data breach notification, and compliance with applicable laws and regulations.

8.2 **Security Assessments:** Conduct regular security assessments of vendors to evaluate their cybersecurity practices and ensure compliance with your organisation's standards. This can involve questionnaire-based assessments, on-site audits, or independent third-party assessments, depending on the criticality of the vendor and the sensitivity of the services they provide.

8.3 **Incident Response and Notification:** Define the expectations and procedures for vendor incident response and notification in case of security breaches or incidents. This should include requirements for timely reporting, information sharing, and collaboration with your organisation to mitigate the impact and prevent future incidents.

8.4 **Subcontractor Management**: If vendors engage subcontractors or third parties to perform services on their behalf, Kildare Ministries requires vendors to ensure that these parties adhere to the same security standards and obligations of this policy. Vendors must specify the need for sub-contractor oversight and approval of subcontractor engagements.

8.5 **Monitoring and Compliance:** Establish mechanisms to monitor vendor compliance with security requirements. This can include regular audits, security assessments, vulnerability scans, penetration testing, or ongoing monitoring of vendor systems and networks.

8.6 **Termination and Transition**: Include provisions for termination of vendor contracts and the secure transition of services to alternate vendors or back in-house. Specify the requirements for data transfer, data deletion, and removal

	of vendor access rights upon contract termination. 8.7 **Continuous Improvement:** Encourage vendors to continually improve their security practices by outlining the need for ongoing risk assessments, security training, and awareness programs for their employees. **9. Policy Review and Updates** 9.1 A regular audit of the implementation of this Policy by Kildare Ministries is undertaken by the relevant committee and/or a person or organisation duly appointed to do so. 9.2 All policies and procedures are reviewed at least once every three years and revised where necessary. 9.3 Any necessary updates or changes to the policy will be communicated to all KM stakeholders and implemented accordingly.
Control Guidelines	**1. Logical Security (passwords)** • Enforce password complexity, requiring a combination of uppercase and lowercase letters, numbers, and special characters. • Implement a password expiration policy to ensure regular password updates. • Discourage the use of common passwords and encourage unique, complex passwords. • Suggested password requirements are as follows: ○ At least 12 characters long. ○ A combination of uppercase letters, lowercase letters, numbers, and symbols. ○ Not a word that can be found in a dictionary or the name of a person, character, product, or organization. ○ Significantly different from previous passwords.
	2. Role Based Access Control • Role-based access control (RBAC) is a method of restricting system access based on the roles of users (e.g. Teacher vs Principle). RBAC provides a simple and manageable way of access management that is more secure and efficient than individually assigning permissions. • RBAC must assign permissions and privileges to users according to their role within the organisation based on least privilege principles across components such as role-permissions, user-role and role-role relationships.

	3. Email Security • **Spam and Phishing Filters:** Utilise spam and phishing filters to automatically detect and block malicious emails. Regularly update and maintain the filtering system to stay current with the latest threats. • **Encryption**: Enable encryption for email communications containing sensitive information, such as student records or staff personal details. Implement Transport Layer Security (TLS) to secure email transmissions between servers. Utilise secure email encryption protocols, such as S/MIME or PGP, to protect the confidentiality and integrity of email content. • **Email Filtering and Content Control:** Implement content filtering to identify and block emails containing malicious attachments, viruses, or malware. Configure email filters to block or flag suspicious email attachments, such as executable files or certain file extensions. • **Employee Awareness and Training:** Conduct regular training sessions to educate employees about email security best practices, including recognizing phishing attempts and avoiding suspicious email attachments or links. Encourage employees to report any suspicious emails or security incidents promptly. • **Regular Software Updates:** Keep email client software, email servers, and security software up to date with the latest patches and updates to mitigate known vulnerabilities. • **Data Loss Prevention (DLP):** Implement DLP measures to prevent the unauthorised transmission of sensitive or confidential information through email. Define policies to automatically detect and block the sending of sensitive data, such as social security numbers or credit card information. • **Email Backup and Recovery:** Regularly backup email data to ensure availability in case of accidental deletion, hardware failure, or a security incident. Test the backup and recovery process periodically to ensure its effectiveness.
	4. Data Encryption • **Full Disk Encryption (FDE):** Implement full disk encryption on all school-owned computers and laptops, including the operating system and all data stored on the devices. Ensure that strong encryption algorithms, such as AES-256, are used for FDE. • **Removable Media Encryption:** Require encryption for any portable storage devices, such as USB drives or external hard drives, used to store or transfer sensitive school data. Encourage the use of encrypted USB drives that automatically encrypt data stored on the device. • **File and Folder Encryption:** Implement file and folder

	encryption for sensitive data stored on network drives or shared folders. Utilise encryption technologies that provide access controls and encryption at the file level to protect sensitive information. • **Wireless Network Encryption:** Secure the school's wireless network with encryption protocols, such as WPA2 or WPA3, to protect wireless communications from unauthorized access. Implement strong passwords or pre-shared keys (PSK) for wireless network access. • **Web Traffic Encryption:** Encourage the use of secure HTTPS connections for school websites and online services. Ensure that websites and web applications used by the school employ SSL/TLS encryption to protect data transmitted over the internet. • **Database Encryption**: Encrypt sensitive data stored in school databases, such as student records, staff information, or financial data. Utilise database encryption solutions that provide transparent encryption and access controls to protect data at rest. • **Mobile Device Encryption:** Implement encryption for mobile devices used by the school, such as smartphones and tablets. Enable device-level encryption and enforce passcode or biometric authentication for mobile device access. • **Backup Data Encryption:** Encrypt all backup data, whether stored on physical media or in cloud-based backup solutions, to protect against unauthorised access to sensitive information. Use encryption solutions that support secure backup and recovery processes. • **Password and Key Management:** Implement strong password policies and encourage the use of password management tools to securely store and manage encryption keys and passwords. Regularly update and rotate encryption keys to maintain a strong security posture.
	5. Social Media and Internet Controls • **Acceptable Use Statement (AUS):** Develop and enforce an AUS that outlines guidelines and rules for appropriate use of social media and the internet within the organisation. Clearly define prohibited activities, such as accessing explicit content, sharing confidential information, or engaging in cyberbullying. Communicate the AUS to all employees and regularly provide training and reminders about its importance. • **Web Content Filtering:** Implement web content filtering tools or services to restrict access to certain websites or

	categories of websites. Configure filters to block access to malicious websites, adult content, gambling sites, or other categories based on organisational policies. Regularly update and maintain the filtering system to stay current with emerging threats and changing content. • **URL Filtering:** Utilise URL filtering mechanisms to block or allow specific websites based on their reputation or security risk. Maintain a regularly updated list of approved and blocked URLs, taking into account legitimate sites required for business purposes and known malicious websites. • **Social Media Access Controls:** Implement controls to restrict or monitor access to social media platforms during work / school hours or for specific user groups. Utilise firewalls, proxy servers, or access control lists (ACLs) to manage and control social media access at the network level. • **Employee Training and Awareness:** Conduct regular training sessions to educate employees about the responsible use of social media and the potential risks associated with it. Provide guidance on identifying and avoiding social engineering attacks, phishing attempts, and scams that can originate from social media platforms. • **Monitoring and Logging:** Implement network monitoring and logging tools to track and record internet usage, including social media activities, within the organisation. • **Patch Management and Security Updates:** Keep social media and internet-related applications, plugins, and browser software up to date with the latest security patches to mitigate known vulnerabilities. Implement controls to protect the privacy of personal data shared through social media platforms or collected during internet usage.
	6. Logging and monitoring • **Log Collection and Centralised Storage:** Configure systems, applications, network devices, and security appliances to generate logs. Collect and store logs centrally in a secure and protected environment, such as a log management system. • **Event and Log Retention:** Define a log retention standard that specifies the duration logs should be retained based on legal, regulatory, and operational requirements. Ensure logs are retained for an appropriate period to facilitate incident investigation and compliance audits. • **Security Event Logging**: Enable logging of security-related events, such as failed login attempts, changes to access privileges, or suspicious activities. Include logs from network devices, firewalls, intrusion detection systems, and other

security infrastructure components.

- **Network Traffic Monitoring:** Deploy network traffic monitoring tools to capture and analyse network traffic patterns, anomalies, and security-related activities. Monitor for unusual network behaviours, such as large data transfers, multiple failed login attempts, or communication with known malicious IP addresses.
- **User Activity Monitoring:** Implement user activity monitoring tools to track and log user actions within the school's systems and applications. Monitor user access, file activity, and application usage to identify any suspicious or unauthorised activities.
- **Intrusion Detection and Prevention System (IDPS):** Deploy IDPS solutions to monitor network traffic and detect potential intrusion attempts or malicious activities. Configure IDPS to generate alerts and log relevant information for further analysis and response.
- **Regular Log Analysis and Review:** Conduct regular log analysis and review to identify security events, trends, and potential security gaps. Perform log correlation and analysis to detect patterns of suspicious activities or potential security incidents.

7. Multifactor Authentication (MFA)

- Enable MFA for all accounts where possible, requiring users to provide an additional verification factor, such as a one-time password or biometric authentication.
- Implement a strong MFA solution that supports multiple authentication methods for added security.

8. Anti-malware

- **Deploy and Configure Endpoint Protection Software:** Install the selected endpoint protection software on endpoints, including desktops, laptops, and mobile devices. Configure the software to enable real-time scanning of files, email attachments, and web content. Customise the settings to suit your organization's needs, such as defining scan schedules, quarantine actions, and exclusions for trusted applications or files.
- **Enable Malware Signature and Behaviour-based Detection:** Activate malware signature-based detection, which compares file signatures against known malware definitions to identify and block threats. Utilise behaviour-based detection mechanisms that analyse system activities and behaviours to identify suspicious or malicious activities. Ensure that the endpoint protection software receives regular updates for the latest malware signatures and detection algorithms.

	• **Implement Heuristic Analysis and Machine Learning:** Enable heuristic analysis, which identifies potential malware based on suspicious characteristics and behaviour patterns, even without specific signatures. Leverage machine learning algorithms to continuously improve detection capabilities by learning from past malware behaviours and patterns. • **Enable Real-time Protection and Web Filtering:** Activate real-time protection to monitor and block malware in real-time as files are accessed or executed. Implement web filtering mechanisms to block access to malicious websites or URLs known for distributing malware. Configure the endpoint protection software to scan downloaded files and email attachments before they are accessed by end-users. • **Centralised Management and Monitoring**: Utilise a centralised management console or software to centrally manage and monitor endpoint protection across the organisation. Ensure the console provides visibility into the security status of endpoints, including malware detection, threat alerts, and system health. Regularly review security logs, reports, and alerts to identify potential malware incidents and take appropriate actions. • **Regular Updates and Patching:** Ensure the endpoint protection software is kept up to date with the latest
	software patches, bug fixes, and security updates. Configure the software to automatically fetch updates from trusted sources to minimise the risk of vulnerabilities. Regularly apply security patches and updates to the organisation's internet gateway devices, such as firewalls, routers, and proxy servers.
	• **User Education and Awareness:** Educate end-users about safe computing practices, such as avoiding suspicious downloads, clicking on unknown links, or opening email attachments from unknown sources. Promote awareness about the dangers of social engineering and phishing attacks, which often deliver malware payloads. Encourage users to report any suspicious activities or potential malware incidents promptly. • **Periodic Assessments and Penetration Testing:** Conduct regular assessments and penetration testing of endpoint protection solutions to evaluate their effectiveness. • **Incident Response and Remediation:** Develop an incident response plan specifically for malware incidents, outlining procedures to detect, contain, and remediate infections. Define roles and responsibilities for responding to malware incidents promptly and effectively. Regularly test the incident response plan through tabletop exercises or simulations to ensure preparedness.

	9. Cyber Incident Response • Develop an incident response plan specifically for cyber incidents, outlining procedures to detect, contain, and remediate. Define roles and responsibilities for responding to cyber incidents promptly and effectively. • Regularly test the cyber response plan through tabletop exercises or simulations to ensure preparedness. • Assign roles and responsibilities to designated individuals who will handle security incidents. • Encourage employees to promptly report any suspicious activities, policy violations, or security incidents.