St Margaret's Berwick Grammar

Cyber Security Policy

Purpose

This Policy provides the basis for cyber security management at St Margaret's Berwick Grammar (**SMBG,** the **School**) and supports commitment to meet SMBG business needs and statutory, legal, audit and moral obligations. It further sets the baseline for management and protection of SMBG information, communication and technology **(ICT**) assets in cyber security context.

Scope

This Policy applies to all ICT within SMBG, that is used by SMBGs' staff, contractors, volunteers and students and other users (**"SMBG Users"**)

Principles

It is the responsibility of all SBMG Users to work together to protect and secure the information held by SMBG, which includes the personal information from our staff and the School community, and internal corporate information.

1. Our staff are educated on the responsible use of technology, the importance of digital wellbeing, how to engage with technology respectfully and protect ourselves and each other;
2. SMBG will be a system where we are supported by digital solutions that are safe, uphold confidentiality, and where sensitive information is protected against unauthorised access; we aim to uphold confidentiality, integrity, and availability.

Policy Statement

Security Governance Risk and Compliance

1. must comply with all applicable state, federal, regulatory requirements. Applicable regulatory and compliance requirements related to cyber security and data protection must be identified, and processes established to ensure requirements are understood and met
2. information security threats and risks to SMBG's assets must be identified, assessed, appropriately responded to, and monitored through formalised and organisation wide security risk management procedures.

Classification, Handling and Protection

1. IT assets and systems (for example, hardware, software and electronic data and information) must be recorded in an inventory or asset register with asset owners and data ownership clearly assigned. Inventory or asset registers must be maintained and updated as required on an ongoing basis
2. information assets must be classified, labelled (where applicable), and handled in accordance the School's records management and with consideration to asset sensitivity and criticality
3. all systems collecting, accessing, processing, storing, transmitting, and/or otherwise interfacing with personally identifiable information must have a data retention policy in place to ensure that data is retained only for the required period
4. a robust data backup and recovery process must be in place for all critical systems to support the integrity and availability of critical information assets

5. processes must be in place to securely dispose of data that is no longer required. All information must be retained in accordance with local regulatory or legislative requirements.

Identity and Access Management

1. User access requests (e.g. system access requests, requests to update access privileges, or requests to revoke user access rights) must be assessed and approved in accordance with defined relevant ICT Acceptable Use Policy
2. Privileged access rights must be authorised according to the principle of least privilege and authenticated via multi-factor authentication where available. Access is to be reviewed at least biannually, with immediate remediation (e.g. immediate access revocation) as required.
3. Access to SMBG's information systems and assets must be securely established and managed

End User Security

1. SMBG Users that have access to IT systems, assets and services including but not limited to computer, email, internet, School issued devices, must adhere to specific rules regarding the use of SMBG IT systems, assets and services and must be aware of and adhere to the control requirements defined in the relevant "ICT Acceptable Use Policy".
2. SMBG Users must undergo security awareness training upon induction and at regular intervals
3. SMBG Users must report any observed or suspected security incidents to ICT Services.

Vendor/Third Party Security

1. All third party services, including Cloud services must be consumed following a formalised risk assessment to identify the necessary security controls that must be implemented by the third party / Cloud Service Provider, and formally documented to manage security risks to an acceptable level. Third parties must be reviewed periodically to assess compliance to contractual cyber terms
2. Security risks associated with contracted third parties who maintain direct or indirect access to SMBG's systems and data, must be operationally and contractually controlled.

Vulnerability Management

1. IT systems are subject to defined security patch management processes to identify, prioritise, and remediate security weaknesses. Remediation must be prioritised based on system criticality, risk analysis, the potential School impact, and available mitigation options
2. vulnerability management processes must be documented and implemented to identify, prioritise, and remediate security weaknesses and decommissioning out-of-band legacy systems across its critical IT infrastructure.

Application Security

1. desktop computers, mobile computers (e.g. laptops, mobile phones), must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of data

Network Security

1. networks must have appropriate controls in place to protect the network, information, and assets in accordance with network security procedure.

Infrastructure Security

1. all devices must be securely protected in accordance with approved standards to adequately protect IT systems that support SMBG processes and services.
2. user desktop computers, mobile phones, mobile computers (for example laptops, tablets), must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification SMBG data.
3. IT facilities (e.g. computer room) that store and process critical information must be constructed, maintained, and monitored in a way that data is adequately protected from physical and environmental threats.

Incident Response Management

Security incidents must be reported ICT Services and the Principal or nominee.
Potential security incidents must be handled appropriately through formalised plans as applicable at School level.
Security incidents must be prioritised based on their impact, reported accurately, and handled appropriately in accordance with incident management processes, and used as future references for resilience against similar security incidents.

Related policies

ICT Acceptable Use Policy
Privacy Policy
Privacy Collection Notice
CCTV Privacy Collection Notice
Child Safety and Wellbeing
Recordkeeping
Workplace Surveillance Act 2005
Network Security Procedure
Infrastructure Security Procedure

Review

This policy is approved by the Senior Executive and reviewed every two years, and/or earlier where required.

Policy Owner	Executive Director ICT
Effective Date	March 2026
Review Date	March 2028
Published	Nexus