John McGivney Children's Centre School Authority	John McGivney School Authority Administration	PR2010
	Information Technology Security Procedure	

1. GUIDELINES:

1.1. All policies, procedures, codes of behaviour, and rules of the JMCCSA apply to all users who access Information Technology Resources provided by or on behalf of the School Authority.

1.2. The JMCCSA reserves the right to monitor the use of Information Technology Resources by all who access the systems and will take appropriate measures to ensure security of the facilities, infrastructure, data, and compliance with policies, procedures, and code of behaviour.

2. PROCEDURE:

2.1. Roles and Responsibilities

2.1.1. School Authority Administrative Team

- Promote an appropriate cyber security risk management culture across the School Authority.
- Manage cyber security resources to enable effective cyber security risk management.
- Oversee the security risk acceptance and tolerance levels.
- Monitor and assess cyber security risk management issues relevant to and/or affecting School Authority IT infrastructure and services.
- Raise cyber security risk management issues with the School Principal and/or School Authority Board of Trustees where appropriate.
- Communicate cyber security risk management issues with all staff, as appropriate.
- Oversee the design and implementation of the School Authority's cyber security plan, controls and capabilities.
- Review and report on the management of cyber security risks.
- Determine cyber security related services required to support:
  - The School Authority's cyber security strategy;
  - the School Authority's strategic priorities, legal and contractual obligations, policies and procedures.

2.1.2. Users

- Follow School Authority policies at all times while using IT resources.

- Be aware of the security requirements of the IT resources they use.
- Take every precaution to safeguard their access to these systems against unauthorized use (e.g. do not share passwords, do not leave workstation unlocked).
- Immediately report any known or suspected cyber security incidents or breaches to the School Authority Administrative Team.

2.2. Email Security

JMCCSA employees, personnel, or third party contractors using JMCCSA facilities should not modify the security parameters within the JMCCSA email system. Users making unauthorized changes to the email security parameters are in violation of this policy.

2.2.1. User Authentication

- All school email user accounts must be secured using a strong password with a minimum number of characters.
- All school staff must remember their passwords and keep them private and secure from compromise.
- School email user accounts assigned to individuals (staff, volunteers, trustees, students) must have multi-factor authentication (MFA) enabled.
  - School email user accounts may have MFA disabled at the discretion of JMCCSA administrative team. User accounts with MFA disabled must have appropriate safeguards applied to compensate for the lack of this feature (eg. restrictions on data that is accessible to account).

2.2.2. Phishing and Malware

- All school staff are to be provided training annually by the School Authority on how to identify malicious emails containing phishing and malware attempts.
  - School staff are to adhere to the training and guidance they receive regarding phishing and malware. Staff are expected to remain diligent to identify emails that carry malware or phishing attempts. We instruct employees to:
    - Avoid opening attachments and clicking on links when content is not adequately explained (e.g. “Watch this video, it’s amazing.”);
    - Be suspicious of clickbait headlines and subject lines;

        - Check email addresses and names of unknown and known senders;
        - Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks, excessive number of common words, or prose that does not align with known sender's typical voice or tone);
        - Be suspicious of any emails requesting urgent action.
    - School staff are to report any suspected malicious emails they receive to the school office immediately upon identification.

2.3. Removable/Portable Media

2.3.1. Users are permitted to use and access removable/portable media as needed for the completion of their job.

2.3.2. If personal identifiable information (PII) is stored on removable/portable media, the files containing such PII must be password encrypted.

2.3.3. Users must delete any sensitive data from removable/portable media immediately after its use on such media is no longer required.

2.3.4. Users are not permitted to use removable/portable media that they are unfamiliar with, does not belong to them, or has not been permitted for use by the owner.

2.3.5. Staff are expected to report to IT/office staff any instances in which they find removable/portable media on school premises that is unattended or appears to have been lost.

2.4. Response to Suspected and Confirmed IT Security Breaches

2.4.1. School IT/office staff should be notified immediately by users if the user suspects an unauthorized breach of IT systems by individuals, malware, or any other means.

APPLICABLE DOCUMENTS

Document/Form Nbr.	Title
P2010	Information Technology Security Policy
Mission & Vision	JMCCSA Mission and Vision Statement
	Municipal Freedom of Information and Protection of Privacy Act, R 1990, c.M.56
	Government of Ontario Information Technology Standards

EFFECTIVE DATE: February, 2024

LAST REVISION DATE: February, 2024

NEXT REVIEW YEAR: 2024-2025