	John McGivney School Authority Administration	P2010
	Information Technology Security Policy	

## TERMINOLOGY:

**Data:** Includes but is not limited to John McGivney School Authority student records, employee records, confidential, personal, or professional information, communications, and usage or monitoring logs.

**Information Technology Resources:** Include but are not limited to computers, phones, tablets, interactive displays, cellular/mobile technology, peripheral devices, computer applications, email, servers, networks, internet/cloud services, internet access, social media, data, and any other electronic or communication technology provided by the John McGivney School Authority that exist today or may be developed or procured in the future regardless of whether it is hosted by JMCCSA or a third party.

**Cloud Services:** Include any service provided by the School Authority that is hosted on the internet. Examples include but not limited to Gmail/Meet/Classroom, the school IEP engine, Software as a Service (SaaS) applications.


**User:** Any individual authorized to access the JMCCSA's Information Technology Resources through any electronic or communication activity using any device, whether or not such device is personally owned or has been provided by the JMCCSA and regardless of the user's physical location. Users include but are not limited to employees, students, parents, volunteers, visitors, contractors, Trustees, or any other authorized individuals.

**Administrator:** Any individual user that has been granted privileges used to manage or administer JMCCSA Information Technology Resources (system administrators).

**Personal Information:** Recorded information about an identifiable individual, including:

- I. information relating to race, national or ethnic origin, colour, religion, age, sex, sexual orientation, or marital or family status of the individual;
- II. information relating to the education, medical, psychiatric, psychological, criminal, or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- III. any identifying number, symbol, or other particular assigned to the individual;
- IV. the address, telephone number, or other personal contact information of the individual;
- V. the personal opinions or views of the individual except where they relate to another individual;

**Printed copies are for reference only. Please refer to the electronic copy for the latest version.**


	<p style="text-align: center;">John McGivney School Authority Administration</p>	<p style="text-align: center;">P2010</p>
	<p style="text-align: center;">Information Technology Security Policy</p>	

- VI. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- VII. the views or opinions of another individual about the individual; and
- VIII. the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual. (Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c.M.56).

**Portable/Removable Media:** Any data storage medium (USB drives, CDs, DVDs, etc.) that can be easily removed or inserted by a standard user into an end-point device such as a laptop or desktop computer.

**POLICY:**

The John McGivney School Authority acknowledges that safe access to its computing network will enhance and encourage more effective overall technology use at the JMCCSA, and thus improve the effectiveness and efficiency of its staff in developing and maintaining an exceptional learning environment. The goal of this policy is to protect the JMCCSA's computing resources such as student and administrative data, computer systems, communications networks, etc. from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to the School Authority's public image. All students, Board trustees, employees, School Council Chairpersons, contractors, vendors and guests accessing the Board's computing resources must adhere to this policy and its corresponding procedure. Violations of this policy and its corresponding procedure may result in the temporary or permanent termination of computing resource access privileges and other appropriate disciplinary action

	John McGivney School Authority Administration	P2010
	Information Technology Security Policy	

**APPLICABLE DOCUMENTS**

Document/Form Nbr.	Title
PR2010	<a href="#">Information Technology Security Resources Procedure</a>
Mission & Vision	<a href="#">JMCCSA Mission and Vision Statement</a>
	<u>Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c.M.56</u>

---

EFFECTIVE DATE: February, 2024

LAST REVISION DATE: February, 2024

NEXT REVIEW YEAR: 2026-2027

**Printed copies are for reference only. Please refer to the electronic copy for the latest version.**