	<p style="text-align: center;">John McGivney School Authority Administration</p>	<p style="text-align: center;">P2009</p>
	<p style="text-align: center;">Acceptable Use of Information Technology Resources Procedure</p>	

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. Personal Safety Rules

- 2.1.1. Never reveal user-credentials (username or password) whether they are unique to your user account or a general school account.
- 2.1.2. Never send a picture of yourself, another person or a group over an electronic network without prior informed permission of all the individuals involved and, in the case of minors, their parents or guardians.
- 2.1.3. Report immediately to an Administrator any suspected instances of malicious activities, messages, or unauthorized attempts to access Information Technology Resources you encounter. This includes but is not limited to phishing emails, instances of Business Email Compromise (BEC), automated notices of suspicious activity sent by Cloud Services, and navigation to a website that is different from the URL you intended to enter.

2.2. Unacceptable Sites and Materials

- 2.2.1. Despite JMCCSA-controlled measures and supervision, on occasion, users of Information Technology Resources may encounter material that is controversial and which other users, parents, or staff might consider inappropriate or offensive. It is the responsibility of the individual user not to intentionally access such material and if inadvertently accessed, should report to an Administrator.
- 2.2.2. The JMCCSA is committed to meeting obligations under the Canadian Charter of Rights and Freedoms and the Ontario Human Rights Code

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;">P2009</p>
	<p style="text-align: center;">Acceptable Use of Information Technology Resources Procedure</p>	

by providing a safe school and workplace that respects the rights of every individual. Discrimination, bullying, and harassment will not be tolerated. It is not acceptable to use Information Technology Resources to knowingly access sites which contain material of a discriminatory or harassing nature.

2.2.3. Users of the JMCCSA's Information Technology Resources will **not** knowingly access, upload, download, store, display, distribute, or publish any information that:

- a. is illegal or that advocates illegal acts or facilitates unlawful activity;
- b. threatens or intimidates any person or suggests violence, hatred, or discrimination toward other people;
- c. uses inappropriate and/or abusive language or conduct;
- d. contains inappropriate religious or political messages;
- e. violates or infringes the rights of any other person according to the John McGivney School Authority policies, Ministry of Education policies, the Ontario Human Rights Code, or the Canadian Charter of Rights and Freedoms;
- f. is racially, culturally, or religiously offensive;
- g. encourages the use of controlled substances, participation in an illegal act, or uses JMCCSA Information Technology Resources to incite criminal actions;
- h. is of a defamatory, abusive, obscene, profane, pornographic, or sexually explicit nature;
- i. contains personal information, images, or signatures of individuals without their prior informed consent;
- j. constitutes messages of sexual harassment or which contains inappropriate romantic overtones;
- k. solicits any users on behalf of any business or commercial organization without appropriate authorization;
- l. supports bulk mail, junk mail, phishing, or spamming, with exceptions to pre-approved activities that aim to support school operations, strategic goals, or staff training;
- m. propagates chain letters, or other email debris;
- n. attempts to hide, disguise, or misrepresent the identity of the sender, except for pre-approved activities that aim to support staff training (e.g. phishing simulations);
- o. interrupts or disrupts student learning and/or affects the moral tone of the environment.

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;">P2009</p>
	<p style="text-align: center;">Acceptable Use of Information Technology Resources Procedure</p>	

2.3. User Obligations and Acknowledgement

All users of JMCCSA Information Technology Resources will do the following:


- 2.3.1. Keep use of online services within reasonable limits in terms of time and volume of information transferred through the system. Excessive use of the system may disrupt services for all users (e.g. sending mass mailing of large documents, transferring large files, or movie streaming at times of peak system usage).
- 2.3.2. Report to an Administrator any known or suspected instances of data loss or exfiltration and/or any known or suspected harm to the system or to information on the system, whether such instances have been caused accidentally or intentionally.
- 2.3.3. Use email only to further the School Authority's objectives, and recognize that the JMCCSA email system and its associated data is the School Authority's property. As part of regular, day-to-day business operations, the School Authority does not monitor email. Should a specific need arise, an Administrator can request that specific School Authority email be monitored.
- 2.3.4. Take reasonable measures to maintain the security of JMCCSA Information Technology Resources. This includes but is not limited to adhering to guidance on email security, reporting any suspected phishing emails or malicious links, and locking computer accounts when not in use.
- 2.3.5. Users acknowledge that JMCCSA is the proprietary owner of any content created for use within the JMCCSA setting throughout the course of a user's employment or association with the JMCCSA.

2.4. Prohibited Uses and Activities

All users of JMCCSA online systems will **not** do the following:

- 2.4.1. copy, download, install, or run viruses or other inappropriate, malicious, or unauthorized materials such as games, files, or scripts from any source;
- 2.4.2. cause damage to any computer(s) and/or equipment including, but not limited to computer hardware, furniture, projectors, connectors,

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;">P2009</p>
	<p style="text-align: center;">Acceptable Use of Information Technology Resources Procedure</p>	


keyboards, storage devices (e.g. disk drives, jump drives, etc.), and pointing devices (e.g. mice);

- 2.4.3. damage or erase files or information belonging to any person without authorization;
- 2.4.4. cause any user to lose access to the system - for example, by disabling accounts or changing passwords without authorization;
- 2.4.5. open a computer case or tamper with internal computer components without authorization;
- 2.4.6. attach unauthorized devices to a computer or network. If an unknown storage device (e.g. usb jump drive) is found on school premises, it should never be plugged into a computer and should instead be immediately turned in to the School Office for investigation. Such devices may contain malware or other harmful applications;
- 2.4.7. compromise themselves or others by unauthorized copying of information, work, or software belonging to others, encouraging others to abuse the computers or network, displaying, transferring, or sharing inappropriate materials. Software pirating and unauthorized copying of material belonging to others is regarded as theft;
- 2.4.8. access data or Information Technology Resources that are not required for job functions or the education of JMCCSA students;
- 2.4.9. copy, transfer, or use files, programs, or any other information belonging to JMCCSA without prior authorization by Administrators;
- 2.4.10. Attempt to subvert or disrupt the JMCCSA networks by breaching or attempting to breach security measures, accessing records without authorization, or any other type of disruption.
- 2.4.11. Leave computer user accounts unlocked while unattended.

2.5. Consequences

Inappropriate use of Information Technology Resources by students and staff could result in disciplinary action by the principal or designate that may include legal action and/or involvement of police.

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;">P2009</p>
	<p style="text-align: center;">Acceptable Use of Information Technology Resources Procedure</p>	

2.6. Cloud Services

The internet provides a wealth of resources for educational purposes. Some Cloud Services require accounts to access the resource while others do not. Google Workspace for Education is an example of a JMCCSA approved Cloud Service. JMCCSA supports the use of approved Cloud Services for educational and business purposes dedicated to improving student success, achievement, and well-being.


- 2.6.1. Access and privileges to Cloud Services are provided on an as-needed basis. If a user no longer requires access to specific data or privileges, they must inform an Administrator.

2.7. Online Publishing

Information published on the internet can reach millions of people who are mostly unknown to the original publishers. For this reason, it is important to regulate information that is published through JMCCSA Information Technology Resources.

- 2.7.1. The electronic publication of information using the facilities of the JMCCSA is subject to all JMCCSA policies, procedures, and guidelines.
- 2.7.2. Links from a JMCCSA site to outside sites must be carefully selected and are subject to the same standards of content quality as JMCCSA sites.
- 2.7.3. The information published online must be kept current and accurate with no conscious attempt to mislead the reader.
- 2.7.4. Personal information such as personal addresses, phone numbers, individual or group pictures, or signatures cannot be published without express informed permission according to JMCCSA procedures.
- 2.7.5. All JMCCSA staff are responsible for ensuring that all work published is original or has been cleared for copyright with the originator and ownership of the copyright is clearly indicated.
- 2.7.6. All web pages hosted on the JMCCSA website or paid for by the JMCCSA are considered property of the JMCCSA.

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

	John McGivney School Authority Administration	P2009
	Acceptable Use of Information Technology Resources Procedure	

APPLICABLE DOCUMENTS

Document/Form Nbr.	Title
P2009	Acceptable Use of Information Technology Resources Policy
P2008	Bring-Your-Own-Device (BYOD) Policy
PR2008	Bring-Your-Own-Device (BYOD) Procedure
P2010	IT Security Policy
PR2010	IT Security Procedure
P3003	Code of Conduct
Mission & Vision	JMCCSA Mission and Vision Statement
	Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c.M.56

EFFECTIVE DATE: February, 2024

LAST REVISION DATE: February, 2024

NEXT REVIEW YEAR: 2028-2029

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