	John McGivney School Authority Administration	PR2011
	User Access and Management 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. General Access Principles

2.1.1. JMCCSA will provide access privileges to IT Resources based on the following principles:

- Need to know – users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.
- Least privilege – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

2.1.2. Requests for users’ accounts and access privileges must be appropriately approved by the principal or designate.

2.1.3. Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared/generic accounts, test accounts and remote access) must be formally documented and approved by the JMCCSA Principal or the JMCCSA Business Manager.

2.1.4. All user accounts must be password protected at all times.

2.1.5. All user accounts with privileged access and/or access to Personal Information must use Multi-Factor Authentication.

2.1.6. Access rights will be disabled or removed when JMCCSA IT staff receives notification that a user is terminated or ceases to have a legitimate reason to access JMCCSA systems.

2.1.7. A verification of the user's identity must be performed by JMCCSA IT staff before granting a new password.

2.1.8. Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

- An active account assigned to external contractors, vendors or employees that no longer work for JMCCSA.
- An active account with access rights for which the User's role and responsibilities do not require access. For example, Users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.
- System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
- Unknown active accounts.

2.1.9. All Users acknowledge that access and activity through User accounts may be monitored. Such activity may be logged and accessed by JMCCSA Administrators, and includes but is not limited to dates, times, and duration of access, data uploads and downloads, digital communications, and document creation/changes.

- User accounts for Cloud systems may be accessed on Personal Electronic Devices (PEDs) with the understanding that JMCCSA reserves the right to monitor activity related to these accounts to detect and respond to issues of confidentiality/data loss by wiping school-owned data from PEDs and/or revoking User access on specific devices.

2.2. Administrator Access

2.2.1. Administrator accounts must have appropriate usernames that clearly identify the individual the account is assigned to.

2.2.2. Administrator accounts must be password protected and utilize Multi-Factor Authentication to acquire access.

2.2.3. Active Directory Administrator accounts are not to be used for standard daily activities and should only be actively logged into as needed to complete Administrator tasks and promptly logged out of immediately upon the completion of such tasks. Users who are granted Active Directory Administrator access are to use their standard Active Directory User account for all other functions related to their duties.

2.2.4. Administrator accounts can only be granted upon approval by the School Principal, the JMCCSA Business Manager, or the Third-Party Managed Service Provider for the sole purpose of managing JMCCSA IT Resources.

2.3. Shared/Unassigned User Accounts

2.3.1. Where possible, individual user accounts should always be preferred over shared or unassigned User accounts.

2.3.2. Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as “guest” and “functional” accounts.

2.3.3. User credentials for shared accounts will be stored and handled in accordance with the Password Policy. School Administrators will be responsible for storing, managing, and providing access to these credentials.

2.4. Test Accounts

2.4.1. Test accounts are to be created and maintained as needed at the discretion of JMCCSA Administrators.

2.4.2. Test accounts are to be deactivated/deleted when they are no longer necessary.

2.5. Contractors and Vendors

2.5.1. In accordance with the Contract Management Policy, contracts with contractors/vendors will include specific requirements for the protection of data. In addition, contractor / vendor representatives will be required to sign a Confidentiality Agreement prior to obtaining approval to access Institution systems and applications.

2.5.2. JMCCSA will maintain a current list of external contractors or vendors having access to JMCCSA IT Resources.

2.5.3. JMCCSA Administrators will be responsible to review the status of User accounts assigned to third-party contractors/vendors regularly (annually as a minimum). Unused User accounts or User accounts that are no longer necessary are to be deactivated/deleted.

2.6. Visitors

2.6.1. Visitors may access JMCCSA IT Resources in accordance with the JMCCSA Bring-Your-Own-Device (BYOD) Policy and Procedure.

2.6.2. Visitors should only be granted User accounts on an exception basis with appropriate approval from the School Principal or Business Manager.

APPLICABLE DOCUMENTS

Document/ Form Nbr.	Title
P2011	User Access and Management Policy
P2008	Bring Your Own Device (BYOD) Policy
PR2008	Bring Your Own Device (BYOD) Procedure
Mission & Vision	JMCCSA Mission and Vision Statement

EFFECTIVE DATE: February, 2024

LAST REVISION DATE: February, 2024

NEXT REVIEW YEAR: 2026-2027