Empowering Minds Information Management Policy

Version	V 2020.1
Date Approved by Board of Directors	**December 16, 2020**
Next Review Date	**1-Year from approval date.**
Authors	Alexis Paproski, Operations Manager and Rob Finot, Governance Director

Purpose of Information Management Policy

The purpose of this policy is to guide and direct the creation and management of information, and to clarify Empowering Minds team member's responsibilities. Empowering Minds is committed to establishing and maintaining information management practices that meet its business needs, accountability requirements and stakeholder expectations.

The benefit of complying with this policy will be trusted information that is well-described, stored in known locations and accessible to Empowering Minds team members when needed.

This policy is written within the context of Empowering Minds' information management framework, which is located in One-Drive. Complementary policies and additional guidelines and procedures support this policy and are also located in One-Drive.

Policy Statement

Empowering Minds information is a corporate asset. It is vital both for ongoing operations and also in providing valuable evidence of business decisions, activities and transactions.

Empowering Minds is committed to creating and keeping accurate and reliable information to meet this obligation.

Also, Empowering Minds is committed to the principles and practices set out in whole-of-government policies and best-practice standards.

Empowering Minds will implement fit-for-purpose information management practices and systems to ensure the creation, maintenance and protection of reliable information. All information management practices in Empowering Minds are to follow this policy and its supporting procedures.

Scope

This policy applies to Empowering Minds staff and contractors, to all aspects of the organization's business and all business information created and received. It covers information in all formats including documents, email, voice messages, memoranda, minutes, audio-visual materials and business system data.

The policy also covers all business applications used to create, manage and store information, including the official information management systems, email, websites, social media applications, databases and business information systems. This policy covers information created and managed in-house and off-site.

Maintenance of Information

Business information must be created and captured by everyone subject to this policy. Business information created should provide a reliable and accurate account of business decisions and actions. This includes all necessary information to support the business needs, including names, dates and time, and other key information needed to capture the business context.

All business information created and received can only be captured by Empowering Minds endorsed information systems.

Empowering Minds will provide training on titling information and when and where to capture information.

Systems Used to Maintain Information

Empowering Minds primary information management system is our CRM known as Infusionsoft. Where possible, all incoming paper correspondence the organization receives should be converted to digital format and saved into the CRM. In limited situations, paper correspondence the organization receives should be converted to digital format and saved into the organizations One-Drive.

The following business and administrative databases and software applications are endorsed for the capture and storage of specific information. These include:

Infusionsoft
Sage Accounting
One-Drive for Electronic Files

These endorsed systems appropriately support information management processes, such as creation and capture, storage, protection of integrity and authenticity, security, access and retention, destruction, and transfer.

Corporate information must not be maintained in email folders, shared folders, or personal drives as these lack the necessary functionality to protect business information over time.

Also reference Cyber Policy for more details on approved systems and applications.

Personal Device Systems to Maintain Information

Information created and distributed on social media applications or mobile devices are trusted to be done so in good faith by each individual, to protect Empowering Minds' positive work within the community. Access and storage of information provided by Empowering Minds, is permitted in accordance with the agreement as established by Empowering Minds and named recipient only.

Access to Information

Sharing corporate information within Empowering Minds:

Information is a corporate resource to which all staff and contractors may have access, except where the nature of the information requires restriction.

Access restrictions include:

- Access to individual staff or client files without authorization.
- Access to sensitive material, including but not limited to security classified material.

Release of publicly available information:

We will provide access to publicly available information on our website. This is the responsibility of the Operations Manager.

The public also have legislative rights to apply for access to information our organization holds under the Freedom of Information Policy (FOIP). This applies to all information held by the agency, whether in officially endorsed information management systems or in personal stores such as email folders or shared and personal drives. Responses to applications for access under FOIP are the responsibility of the Operations Manager at Empowering Minds.

Retention or Destruction of Information and Records

Information is destroyed when it reaches the end of its required retention period. Retention periods in records authorities take into account all business, legal and government requirements for the information. Empowering Minds uses a number of general and agency-specific authorities to determine retention, destruction and transfer actions for its information.

Some information can be destroyed in the normal course of business. This is information that is of a short-term, facilitative or transitory value, which is destroyed as a 'normal administrative practice'. Examples of such information include rough working notes, drafts not needed for future use, or copies of information held for reference.

Staff should not destroy information without the approval of the Operations Manager.

Also reference Cyber Policy for more details on digital file destruction.

Transfer of Information

At times, certain information may be required to be transferred out of the custody of Empowering Minds. This occurs when information of archival value is no longer being actively used. In this instance Empowering Minds transfers it to an Archived File. We will still able to access the information if a future need arises, by submitting a request to the Operations Manager. Information may also be transferred if administrative change affects Empowering Minds and transferred to the inheriting agency.

Roles and Responsibilities

All staff are responsible for the creation and management of information as defined by this policy.

Operations Manager: The Operations Manager is ultimately responsible for the management of information within Empowering Minds. The Operations Manager has authorized this policy. The Operations Manager promotes compliance with this policy and ensures Empowering Minds information management program is adequately resourced.

Senior Management/Board of Directors: Senior executive officers and managers are responsible for the visible support of, and adherence to, this policy by promoting a culture of compliant information management within the organization and contributing to the development of strategic documents. These include the information governance framework and information management strategy. (This includes but is not limited to the President, CEO, Executive Director.)

ICT Staff/Contractor: ICT staff or contractors are responsible for maintaining the technology for Empowering Minds business information systems, including maintaining appropriate system accessibility, security and backup. ICT staff or contractors should ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with this policy. ICT and information management staff or contractors have an important joint role in ensuring that systems support accountable and effective information management across the organization.

Agency Security Adviser: The security adviser provides advice on security policy and guidelines associated with the management of information.

Managers: Managers are responsible for ensuring staff, including contract staff, are aware of, and are supported to follow, the information management practices defined in this policy. They should advise the Operations Manager of any barriers to staff complying with this policy. They should also advise staff and contractor staff of any changes in the business environment that would impact on information management requirements, such as new areas of business that need to be covered by a records authority.

Staff and Contract Staff: Staff and Contract Staff are to create and manage information in accordance with this policy to the extent specified in their contract.

Communication and Training
This policy will be communicated to staff and training will be provided on aspects of the policy. Training will be done when individuals join the organization and as changes are made to the policy or systems to ensure everyone is up-to-date. Training will be tailored so that it is meaningful to different work groups at Empowering Minds.

Monitoring and Review of this Policy
This policy will be updated as needed if there are any changes in the business or regulatory environment. It is scheduled for a comprehensive review by **July 31, 2021**. The Operations Manager will initiate this review and will work with the Director of Compliance to complete it.

The Operations Manager, with the support of managers, will monitor compliance with this policy. Levels of compliance will be reported at least annually to senior management and the Board of Directors.

Resources
Contact details for the Operations Manager:
> **Name:** Alexis Paproski
> **Email:** alexis@empoweringminds.org
> **Phone:** 403.718.1264 Ex. 2

1. Access to Information Act
2. Canada Evidence Act
3. Copyright Act
4. Criminal Records Act
5. Emergency Preparedness Act
6. Library and Archives of Canada Act
7. Official Languages Act
8. Security of Information Act
9. Personal Information Protection and Electronic Documents Act (Part 2)
10. Privacy Act

11. Statistics Act
12. Shared Services Canada Act

Senior Management / Board of Directors Endorsement
The President and the Board of Directors endorsed and approved this policy on **December 16, 2020**.