POLICY:	**Cyber Security & Acceptable Use Policy**
POLICY NUMBER:	**1.10**
ISSUING AUTHORITY:	**Community Foundation of Portage and District Inc.**
APPROVED:	**Month, day, year**
LAST REVIEWED:	
NEXT REVIEW:	**Month, day, year**

Purpose:
The purpose of this policy is to outline how the Community Foundation of Portage and District Inc (CFPD) will protect the integrity, confidentiality, and availability of CFPD's data and systems, ensuring the privacy and security of our donors, staff, volunteers, and beneficiaries. This policy will also ensure that all users of CFPD's technology systems act responsibly, ethically, and in compliance with cybersecurity and organizational standards.

A comprehensive listing of technology access points used by CFPD has been developed and is considered a procedural document. It will be updated on a regular basis as these points are amended. This document is available to employees; board members and volunteers through the CFPD web site "Board Portal".

Scope:
This policy applies to all volunteers, board members, contractors, and third-party partners (herein referred to as "users"), who access CFPD's information systems, network infrastructure, internet, email, any internal network and/or digital resources.

1. **Data Protection and Privacy:**
    - Confidential data must not be shared outside of the organization without authorization. Auto-forwarding of electronic messages outside of CFPD internal systems is prohibited.
    - Users must store data only on approved, secure platforms (e.g. internal servers, authorized cloud storage, CFPD USB devices).
    - Users are prohibited from sharing personal authentication information including account passwords, Multi-Factor Identification etc. with anyone not specifically authorized to receive such information.
    - Personal and sensitive information of fund holders, staff and volunteers will be stored in cabinets that are locked at end of business day and accessed only by authorized personnel.
    - Access to donor and beneficiary data is restricted to authorized users only.

- Yearly audits are conducted by the IT service provider to ensure compliance with online data protection and recommendations are made in accordance with industry standards.

2. **Access Control and Security:**
    - Access to technology resources is intended for business-related purposes only. Personal cell phones are the exception.
    - All hardware and software must be connected and installed by the IT service provider on all CFPD equipment. All assets taken off-site should be physically secured at all times. Users are prohibited from allowing unauthorized individuals access to CFPD resources.
    - Users are responsible for safeguarding their login credentials and are prohibited from sharing them with others. Whenever possible, use unique passwords for each system or platform to reduce the risk of unauthorized access. Use strong authentication methods, including two-step verification (2SV) or multi-factor authentication (MFA), for accessing systems, whenever supported.
    - Passwords are not to be saved directly to browsers or devices. All passwords are to be recorded on a central document, which is password protected, to support business continuity.
    - Users must report lost, stolen or compromised devices immediately and follow the Incident Response Policy.
    - Users must log off from any applications or network services when they are leaving their workspace unattended.
3. **Email, Internet and Social Media Use:**
    - Users should not engage in activities that may harass, threaten, impersonate or abuse others.
    - Phishing, spam and suspicious messages must be reported immediately as per the Incident Response Policy.
    - Users are responsible for the content they publish online. Publishing content needs to align with CFPD's mission, vision and values. It is prohibited to post confidential information or offensive, discriminatory or harassing language. Users should take every effort to verify information for accuracy before posting.
    - Users are expected to ensure that their personal social media activities do not conflict with the values, mission or reputation of CFPD. While personal accounts are not managed by CFPD, individuals should refrain from posting content that could reasonably be viewed as offensive, discriminatory or damaging to the organization's credibility.
4. **Prohibited Activities:**
    - The following are strictly prohibited:

- Bypassing security controls or tampering with system settings
- Installing unapproved software or hardware
- Downloading or distributing pirated or illegal materials/software
- Using organizational resources for personal business ventures, political activity or any other unauthorized use
- Engaging in malicious activities
- Accessing, viewing or sharing inappropriate content, including but not limited to:
    - Sexually explicit content
    - Content that promotes hatred or discrimination based on race, religion, gender, etc.
    - Material that bullies, intimidates, or threatens others
    - Content that is generally considered vulgar, offensive, or disturbing
    - Confidential or proprietary information

5. **Incident Response:**
    - Adhere to incident response plan to identify, respond to, and recover from cybersecurity incidents.
    - Immediate actions will be taken to contain threats, recover data, and notify affected parties.
6. **Regular Audits and Assessments:**
    - Conduct annual security assessments and audits with IT professionals to identify vulnerabilities and ensure policy adherence. This annual report is reviewed by the Executive Director and provided to the Executive Committee.
7. **Training and Awareness:**
    - Provide cybersecurity training/phishing training sessions for staff.
    - Educate on best practices, including recognizing phishing attempts and using secure communication channels.
8. **Compliance, Monitoring and Enforcement:**
    - Ensure compliance with relevant local, provincial, and federal regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and Manitoba's privacy laws.
    - CFPD reserves the right to monitor usage of its systems to ensure compliance. Information created, sent, received or stored on CFPD devices are not private and may be accessed at the discretion or under the direction of the Executive Director, Board of Directors Executive Committee, or the IT service provider at any time, without the knowledge or consent of the User.
    - Violations of this policy with be dealt with in accordance with the Human Resources Policy 5.0.

Responsibilities:

- **Users:** Responsible for implementing, following and maintaining cybersecurity measures. Report any suspicious activities.
- **Executive Director/Board of Directors:** Ensure resources are allocated for cybersecurity initiatives and training and oversight of policy adherence.

Responsibility:

Review, and revision of this policy annually or more frequently as required, with subsequent recommendation to the Board for approval.