Albion Neighbourhood Services

Privacy and Confidentiality Policy

Albion Neighbourhood Services (ANS) is committed to protecting the privacy, confidentiality, and security of all personal, organizational, and stakeholder information. This policy outlines expectations for employees, contractors, Board members, and volunteers in handling sensitive information, safeguarding digital systems and equipment, and complying with relevant privacy legislation. This policy applies to:

- All employees (full-time, part-time, temporary)
- Independent contractors and consultants
- Members of the Board of Directors
- Volunteers and interns

Legal Compliance – PIPEDA: ANS adheres to the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which governs how personal information is collected, used, and disclosed. All personnel must ensure that their handling of personal information is consistent with PIPEDA's ten privacy principles, which include accountability, consent, limiting use, safeguarding, accuracy, openness, and individual access. Further details on PIPEDA can be found at www.priv.gc.ca.

Confidential Information Includes (but is not limited to):

- Client information (e.g., name, address, SIN, financial, medical, housing, employment)
- Staff and Board member personal or employment details
- Donor and funder information
- Organizational financial records and reports
- Payroll, pension, and benefits information
- Internal policies, strategies, meeting minutes, and confidential reports
- Login credentials, internal communications, and IT system data
- Any other non-public information disclosed during work or service

Privacy & Confidentiality Expectations

All representatives of ANS are expected to:

1. Treat all confidential information with care and access it only when required for their role.
2. Protect both physical and digital data by following ANS procedures.
3. Never disclose confidential information to unauthorized persons inside or outside the organization.

4. Immediately report any suspected data breaches or loss of information to a supervisor or the Executive Director.
5. Return or securely destroy all confidential material upon ending their relationship with ANS.

Digital Data and Equipment Care

To ensure data protection and responsible use of ANS equipment, all individuals must:

- Use strong passwords and keep login credentials secure.
- Lock or log off devices when unattended.
- Only use ANS-approved and secured devices to access sensitive data.
- Avoid storing confidential data on personal devices unless authorized.
- Report any lost, stolen, or damaged equipment immediately.
- Refrain from installing unauthorized software or accessing unsafe websites.
- Use ANS-approved cloud services for document storage and sharing.
- Return all devices and digital records upon departure from the organization.

Use of Information Systems

All users accessing ANS systems (email, cloud storage, accounting, payroll, communications, etc.) must:

- Use systems solely for ANS-related work.
- Store documents in designated secure platforms (e.g., Microsoft 365, SharePoint).
- Avoid sharing sensitive data through unsecured channels.
- Follow all ANS digital security protocols, including MFA and access restrictions.

Disclosure Requirements

Any confidential information disclosure must be approved by the Executive Director. Confidential information may only be disclosed:

- When legally required (e.g.,police, court order, subpoena); or
- With the explicit, informed consent of the individual concerned.

Breach of Policy

Violation of this policy may result in:

- Disciplinary action up to and including termination
- Legal liability for damages
- Reporting to relevant authorities, if warranted under privacy legislation