Public Privacy Policy: Beacon Community Network

Organization: Beacon Community Network
Effective Date: February 1, 2026
Policy Owner: Operations Manager

1. Introduction & Authority

In alignment with our **Community Safety and Well-being (CSWB) Plan**, The Beacon Community Network operates a Closed-Circuit Television (CCTV) system in select public areas. This system is used to enhance public safety, deter criminal activity, and protect assets.
The collection of personal information via video surveillance is conducted under the authority of the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and **Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)**, R.S.O. 1990, c. M.56, s. 28(2).

2. Scope of Surveillance

Surveillance is limited to external public-facing spaces including public streets, parks and spaces..

- **Public Areas:** City streets, business districts, public parks and community spaces.
- **Privacy Protections:** Cameras are positioned to avoid capturing the interior of private residences. Where a camera's field of view unavoidably includes private property, **digital privacy masking** (blurring) is applied.
- **No Audio:** This system records video only. Audio recording is strictly prohibited.

3. Use of Recorded Information

Information collected through the CCTV network will be used exclusively for:

1. Monitoring safety in public spaces.
2. Assisting law enforcement in the investigation of specific criminal incidents.
3. Assisting social services with community outreach.

Information will not be used for general tracking of individuals, monitoring lawful protests, or identifying people based on protected characteristics (e.g., race, religion, or gender).

4. Retention and Security

We take the security of your data seriously.

- **Retention:** Recordings are kept for a maximum of **30 days**. If no incident is reported within that time, the data is automatically and permanently overwritten.
- **Storage:** Data is stored on secure, encrypted Network Adjacent Storage (NAS) devices and cloud storage provided by Solink Corp. in Canada.
- **Access:** Only authorized security personnel with a "need to know" can view footage. Every instance of access is logged and audited.

5. Disclosure to Third Parties

Footage will only be disclosed to third parties (such as the Ontario Provincial Police or local Police Services) in the following circumstances:

- To assist in a specific law enforcement investigation.
- In response to a court order or subpoena.
- In an emergency where the health or safety of an individual is at immediate risk.

6. Your Rights: Access and Correction
You have the right to request access to your own personal information, including CCTV footage where you are identifiable.

- To make a **Subject Access Request (SAR)** please contact the Operations Manager.
- Please note that we may redact the faces of other individuals in the footage to protect their privacy before releasing it to you.

7. Contact Information
For questions regarding this policy or the operation of the CCTV system, please contact our **Operations Manager**:
[Rod Bilz/Operations Manager] [r.bilz@beaconnetwork.ca] [705-493-7403]

Implementation Checklist for Ontario CSWB Plans:

- **Signage:** Ensure signs are posted *before* someone enters the camera's range.
- **Audit Trail:** Keep a logbook of every time a video is viewed, including the date, time, and reason.
- **IPC Review:** The IPC of Ontario recommends that institutions notify them of new surveillance programs—it's a "best practice" that builds public trust.