POLICY TITLE:
Camera Privacy Policy
POLICY #: BEA001
APPROVAL DATE: January 1,2025
PREPARED BY: Director of Operations

Administrative Policy and Procedural Manual
CATEGORY: Privacy
EFFECTIVE DATE: January 23, 2025
SUPERCEDED POLICY(S):
N/A

Introduction

The Building Blocks BEACON Program is a private-sector safety and security solution. Building Blocks was established as a for-profit corporation with a vision of a world-class downtown waterfront and prosperity for all. The BEACON Program provides proactive safety and security in North Bay's downtown waterfront area. The triage for any incident that Building Blocks responds to will include Coordinated Access Nipissing access points for non-enforcement responses.

The Building Blocks BEACON Program may also assist and inform the city, emergency services, and public transit of potential serious or emergency events as well as reports of other crime related. Camera footage is substantially intended to improve the health, wellbeing, and safety of the downtown waterfront community. In the same spirit, BEACON may also aid other agencies.

Code of Practice Statement

Building Blocks owns, installs, and operates the Building Blocks BEACON Program within the identified location areas in collaboration with partner businesses and organizations with access to the camera images through a centralized operations point. The Building Blocks BEACON Program QNAP storage devices are owned and operated by Building Blocks and integrated within existing camera networks of partner businesses or organizations. Camera feeds are locally stored on QNAP storage devices with customizable alerts and notifications.

It is the practice of the Building Blocks to utilize the Building Blocks BEACON Program for the safety, health, and wellbeing of the North Bay downtown waterfront community. The Building Blocks BEACON Program collects anonymous information on a transitory basis and does not store identifiable personal information or identifiable vehicle data.

It is not Building Block's intent to collect personal information through the monitoring of the North Bay downtown waterfront streets, sidewalks, or public space network. However, in a circumstance where collection of personal information does occur, such information will only be used or disclosed in accordance with this policy.

As a corporation, collection, use, and disclosure of personal information is not typically subject to the Office of the Information and Privacy Commissioner of Ontario's **Guidelines for the Use of Video Surveillance.** This

guideline informs public institutions of their key obligations under the *Municipal Freedom of Information and Protection of Privacy Act,* and its provincial counterpart, FIPPA. However, as a community organization responsible to the community it serves, Building Blocks will comply with the Office of the Privacy Commissioner of Canada's **Guidelines for Overt Video Surveillance in the Private Sector.**

Building Blocks Privacy Principles

Building Blocks values privacy and confidentiality as part of its efforts to promote dignity to all. Every person, no matter their position, status, or vulnerability, should be treated in a way that preserves and enhances – rather than undermines – their dignity and self- respect. Privacy and confidentiality are crucial elements of the work undertaken by the Building Blocks and the relationship-building efforts that support these efforts.

- Where circumstances present, collection of personal information will:
    - Have a clear purpose;
    - Consist of only the minimum amount necessary;
    - Be direct, informed, and done with consent whenever possible.

- Internal use will:
    - Have an Authorized Purpose (the purpose for which it was collected; or, where necessary, to protect the mental/physical health or the safety of any individual or group of individuals; for the purpose of determining or verifying an individual's suitability or eligibility for a program, service or benefit; or law enforcement/crime prevention);
    - Involve the minimum amount of information necessary; and
    - Be limited to those that need that information to do their authorized work.

- External use will:
    - Have an authorized purpose (the purpose for which it was collected, or health and safety of individual, or law enforcement/crime prevention);
    - Involve the minimum amount of information necessary; and
    - Be limited to those that need that information to do their authorized work.

- Storage – Security safeguards are implemented which are consistent with the sensitivity of information involved. Safeguards will include appropriate:
    - Technical Safeguards;
    - Administrative Safeguards; and
    - Physical Safeguards.

- Retention of personal information is clear and limited.
    - Written retention policies are developed for personal information collected, acquired, and used; and
    - Retention of personal information are limited to the minimum amount of time necessary for the authorized purposes for which it was collected.

- Access to Personal Information
    - Access to personal information is limited according to the principle of least privilege; and
    - Access to personal information is regularly audited/reviewed.

- Accountability
    - The Operations Team is appointed to ensure adherence to privacy principles and/or privacy policy.