



THE ISLE OF GIGHA HERITAGE TRUST

Surveillance Camera Policy

Author signature

S Bannatyne

Date

12.06.2020

Chair of IGHT Board signature

Ga Wata

Date

16-06-2020

Revision History

| Version | Section | Page | Detail Amended | Amended By | Date |
|---------|---------|------|--------------------------------|-------------|------------|
| 1 | All | All | New policy for GDPR compliance | S Bannatyne | April 2020 |

Contents

- i. Introduction
- ii. Surveillance Camera devices used by IGHT
- iii. Acceptable Use
- iv. Security
- v. Risks / Liabilities / Disclaimers
- vi. Appendix A: Checklist for users of limited CCTV systems

i. Introduction

This policy has been created for compliance with the General Data Protection Regulation 2018 and Data Protection Act 2018.

This policy outlines the responsibilities of users of surveillance camera devices.

ii. Surveillance Camera devices used by IGHT

- Close Circuit Television (CCTV) cameras are installed at the Isle of Gigha Heritage Trust office.
 - Two external cameras and two internal cameras operate 24 hours a day, 7 days a week.
 - The external areas covered are the courtyard and adjoining parking area in front of the IGHT office.
 - The internal areas covered are the downstairs and upstairs of the IGHT office.
 - CCTV signage is displayed in the areas where cameras are located to notify passers-by.
 - CCTV images are accessible for 30 days on a rolling deletion programme.
 - Playback images can be viewed by connecting a monitor to the CCTV hard drive.

iii. Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of IGHT.
- The purpose of the CCTV is to deter crime; deter anti-social behaviour; collect evidence of a crime or anti-social behaviour; monitor office security; protect office staff.
- CCTV cameras are positioned to capture images only relevant to the purposes outlined above.
- Except for law enforcement bodies, images will not be provided to / shared with third parties.
- Surveillance Camera devices may not be used at any time to:
 - View, store or transmit illicit materials
 - View, store or transmit proprietary information belonging another company
 - Harass others
 - Engage in outside business activities
 - Monitor personal activities of residents or visitors

iv. Security

- The CCTV hard drive is stored and accessed in the IGHT office only.
- An admin password is required for viewing playback CCTV images.
- Playback images are only to be viewed by IGHT staff; IGHT directors or the Police, if necessary.
- Playback images must only be viewed if unacceptable activities or behaviour have been reported and an investigation is warranted.
- There is no audio recorded with the CCTV images.
- IGHT is registered with Information Commissioners' Office.

v. Risks/Liabilities/Disclaimers

- It is IGHT's and employees' responsibility to take precautions to prevent images from being accessed by unauthorised users.
- IGHT reserves the right to disable services without notification.
- Lost or stolen devices must be reported to IGHT within 24 hours.
- Employees are expected to use surveillance camera devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- IGHT assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- IGHT reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.

vi. Appendix A

Checklist for users of limited CCTV systems

This CCTV system and the images produced by it are controlled by the Isle of Gigha Heritage Trust (IGHT) who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 2018).

IGHT have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of employees. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

| | Checked (date) | Checked By | Date of next Review |
|---|----------------|------------|---------------------|
| There is a named individual who is responsible for the operation of the system | | | |
| The problem we are trying to address has been clearly defined and installing cameras in the best solution. This decision is reviewed on a regular basis. | | | |
| A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required. | | | |
| Cameras have been sited so that they provide clear images. | | | |
| Cameras have been positioned to avoid capturing the images of persons not visiting the premises / vicinity. | | | |
| There are visible signs showing that CCTV is in operation. | | | |
| There are contact details for who is responsible for the system displayed. | | | |
| Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them. | | | |
| The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. | | | |
| Except for law enforcement bodies, images will not be provided to third parties | | | |
| The potential impact on individuals' privacy has been identified and taken into account in the use of the system. | | | |
| The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made. | | | |
| Regular checks are carried out to ensure that the system is working properly and produces high quality images. | | | |

