POLICY FOR OPERATING A PASSIVE CLOSED CIRCUIT TELEVISION (CCTV)

TO COMPLY WITH THE DATA PROTECTION AND OTHER RELEVANT LEGISLATION AND CODES OF PRACTICE

Reference No:	**BSO-CS 1**
Version:	**2**
Ratified by:	**BSO Board**
Date Ratified:	**28/02/2019**
Date Equality Screened:	**January 2019**
Name of Originator/Author	**Bill Harvey**
Date of Creation	**March 2015**
Name of responsible committee/individual	**Business Development Committee / DHRCS**
Date Issued:	**03/05/2019**
Review date:	**30/04/2021**
Target Audience:	**All BSO Staff**
Distributed Via:	**Metacompliance, Intranet, Hard Copy**

Amended by:	
Date amendments approved:	

Contents

1. INTRODUCTION

This document sets out the appropriate actions and procedures to comply with data protection legislation in respect of the use of CCTV surveillance systems operated, managed or used by the Business Services Organisation (BSO). It does not relate to surveillance activities undertaken by the Counter Fraud and Probity Service within BSO as part of their duties.

1.1 In drawing up this policy, due account has been taken of the following: -

- The Data Protection Act 2018 (DPA)
- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- The CCTV Code of Practice produced by the Information Commissioners Office (ICO);
- The Human Rights Act 1998;
- The Regulation of Investigatory Powers Act 2000;
- The Protection of Freedoms Act 2012
- The Code of Practice on Protecting the Confidentiality of Service User Information"

For clarity, the term 'data protection legislation' hereafter incorporates both DPA and GDPR.

1.2 An important feature of the legislation is the ICO's CCTV Code of Practice which sets out the measures which must be adopted to comply with data protection legislation. This goes on to set out guidance on following good data protection practice. The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations as Data Controllers and also reassuring the Public about the safeguards that operators should have in place. It also permits those that's image has been captured by a CCTV system, to request access to those whose images.

2. SCOPE

This policy will apply to all current, and potentially past employees of the Business Services Organisation (BSO), persons acting as Agents of the BSO, individuals or Bodies Corporate acting as providers of services on behalf of the BSO, tenants occupying BSO managed facilities and all other persons whose image may be captured by the systems operated and managed by the BSO and who can be clearly identified from that image.

3. POLICY APPLICATION

3.1 Justification

The role of CCTV can be used for various reasons including:

- Prevention and detection of unauthorised access to BSO Property
- Prevention and detection of theft, violence and other crime.
- To contribute to the assurance that health and safety rules are being complied with and/or so that footage is available in the event of a specific breach.
- Protecting business interests: e.g. to prevent misconduct and providing security to staff and BSO assets

Prior to the installation of any camera on BSO premises, SMT will assure itself that the installation complies with this policy, data protection legislation and all relevant legislation. All proposals to install new CCTV systems, add to, or upgrade existing systems or to reposition existing cameras must be with the prior approval of the SMT.

3.2 Quality of the Images

It is essential that the images produced by the equipment are as clear as possible, to ensure that they are effective for the purpose(s) for which they are intended. For example, if the purpose is 'apprehension and detection of offenders', then the quality should be such that allows individuals to be identified from the captured image.

All camera installations and service contracts should be undertaken by approved security companies. Upon installation all equipment is to be tested to ensure that only the approved predetermined areas are monitored and that the images are of sufficient quality, and available for viewing in live and play back mode. All CCTV cameras and equipment should be serviced and maintained on a regular basis.

The Corporate Services Manager will ensure that the time and date metadata captured by the BSO CCTV systems is correct. This is critical in the event that an incident is either time sensitive or date specific, and will add weight to the image in the event that the image is used as evidence by either the BSO or others.

3.3 Processing of Images

Images, which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary in order to comply with the principles as set out in Article 5 of GDPR, and the provisions of paragraph 4.2 below . While images are being retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of individuals whose image may have been recorded (see principle 7, DPA 2018). It is critical that access to and security of the images is controlled in accordance with the requirements of the DPA 2018. This requirement will be monitored by the Corporate Services Manager on a regular basis.

The Corporate Services Manager will be responsible for ensuring recorded images are deleted in accordance with appropriate guidance from The Department of Health (Northern Ireland) (DoH), ICO and other relevant authorities

Access to images recorded on a BSO CCTV system will be granted by the appropriate director or designated deputy. No viewing of live feed images captured by a CCTV system is permitted other than for those staff tasked with monitoring live feed monitors as part of the facilities management arrangement. No access to stored images held on BSO hard drives is permitted without the prior approval of the appropriate director or designated deputy. Any access to BSO systems which contain personal information is restricted. CCTV systems should be seen as a system that holds personal information about employees, members of the public, visitors and tenants and will be protected accordingly.

All images will be recorded on a digital format, (where existing equipment permits) and stored on secure BSO servers or dedicated server space, taking advantage of existing HSC ICT security mechanisms (see BSO ICT Security Policy). As at 3.4 access and/or extraction of these images will be authorised by the appropriate director or designated deputy, and on their authorisation, be facilitated by the BSO IT Security Team. All live feed monitors located within the BSO's facilities should be positioned so as to prevent unauthorised viewing by any person other than those tasked with that particular role. Care should be taken when positioning existing monitors or prior to the installation of new monitors, which will require the prior approval of the SMT. Premises wishing to install, upgrade, add additional cameras to an existing system, or reposition existing cameras, must put their proposal to SMT for consideration before taking any action. No modification or changes to existing CCTV systems is permitted without this prior approval.

Where the images are required for evidential purposes in legal or BSO disciplinary proceeding, a digital recording of these will be made by BSO IT Security personnel acting at the direction of the appropriate director or designated deputy. These recordings will be viewed to ensure that the correct images are captured, and placed in a sealed envelope signed and dated by two Senior Officers or appropriate Counter Fraud staff unconnected with the actions and held by the Corporate Services Manager until completion of the investigation.

3.4 Access to and Disclosure of Images to third parties

It is critical that access to, and disclosure of the images recorded by CCTV and similar monitoring equipment is restricted and carefully controlled. This will ensure that the rights of individuals are protected and preserved, but also ensure that the continuity of the evidence trail remains intact should images be required for evidential purposes e.g. A Police enquiry or an investigation being undertaken as part of the BSO's disciplinary procedure.

Accessing images for any other purpose not listed at 3.1 is not permitted unless there is an overriding interest in doing so, or prior approval has been obtained from the appropriate director or designated deputy.

Access and disclosure of images is permitted only if it supports the purpose of this policy and is in line with the provisions of data protection and/or other legislation, some of which are listed at section 1.1.

Applications made by the Police Service of Northern Ireland (PSNI) or other body charged with investigating any infringement of law, for access to CCTV images, must be approved by, the appropriate director or designated deputy prior to disclosure to the requesting body. As with any agency, the PSNI or other regulatory body are required to provide justification to BSO before access to CCTV images will be provided, and then, only relevant images will be furnished once a request has been approved. No person or authority has the automatic right to unfettered access to images stored on a CCTV system.

3.5 Access to Images by Individuals (Subject Access Requests DPA 2018)

Applicants requesting access to their own recorded image from a BSO CCTV system, have the right to do so under Article 15 of GDPR, and to be supplied with relevant data within a calendar month once adequate proof of identity and/or authority has been established. All requests for access to personal information held on a CCTV system will be transferred to, and administrated by, the Corporate Services

Department. Once applications have been processed and permission granted, BSO IT colleagues will be tasked with retrieving the electronic data and copying this on to removable media such as a CD for transfer by the BSO to the applicant.

Note: Once an application has been approved by the appropriate director or designated deputy and images have been released to an applicant, BSO is no longer responsible for any further purpose that those images may be used for. All third party data, In this case, images of other persons captured by the CCTV equipment, will be irreversibly removed from the copy released to the applicant. Not to do so may be in breach of the third parties rights as afforded by one or more of those pieces of legislation and codes of practice listed at section 1.1.

3.6 CCTV systems and Facility Tenants

Organisations who use BSO facilities may seek access to images captured by CCTV. BSO will consider any legitimate request and, after approval by the appropriate director of HR and Corporate Services, will facilitate access to these images in accordance with appropriate legislation and BSO procedures.

4. INTERACTION WITH OTHER BSO POLICIES

This policy should be read in conjunction with the BSO's Data Protection & Confidentiality Policy, Freedom of Information Policy and ICT Security Policy, and at each of the local offices, the respective Building Security Policy.

4.1 Freedom of Information Act interaction

It should be noted that images captured on CCTV systems, that DO NOT identify individuals, may not be subject to the provisions of data protection legislation. However, these images may still be requested and released by virtue of the provisions of the Freedom of Information Act 2000. These matters will be processed via BSO's Freedom of Information Policy, and in line with Freedom of Information Legislation.

4.2 Retention and Disposal Schedule

All images captured by BSO operated CCTV systems will be retained for the requisite period identified in the DoH document 'Good Management Good Records' (GMGR). GMGR references the retention of electronic images captured through the use of CCTV systems and recommends that these images should normally be retained for a period of 28 days and then permanently destroyed. Only in the event that images are required for evidential purposes, or if they are the subject of a Freedom of Information request or Subject Access

Request under Data Protection Legislation, should images be retained for longer than the agreed retention period.

5. RESPONSIBILITIES

a. The Board of BSO has overall responsibility for ensuring the organisation has an effective policy to comply with the legal requirement related to the operation of CCTV cameras as set out in paragraph 1.1.

b. The Chief Executive, as the Accounting Officer, is legally responsible for all BSO CCTV systems and for the uses that they are employed.

c. The Director of Human Resources and Corporate Services (DHRCS) has corporate responsibility for the implementation of this policy, for monitoring its effectiveness and ensuring that all legal responsibilities are met.

d. The Corporate Services Manager will on behalf of the DHRCS carry out the day to day operational requirements of this policy and will also ensure that use of CCTV images is compliant with all legal requirements and Codes of Practice. The specific duties are to

   - Conduct an annual review of CCTV systems and usage
   - Ensure that CCTV images are being stored securely and handled in accordance with this policy, relevant legislation and the ICO 'CCTV' Code of Practice
   - Ensure that images are retained in line with GMGR, and that this electronic record is managed in accordance with BSO's Information Security Policy
   - Ensure that images are disposed of in a secure and irreversible manner
   - Ensure access protocols are in place and are being followed at each BSO site
   - Ensure that viewing and disclosure of images is in line with BSO policy and legal obligations
   - Ensure that staff using or maintaining CCTV systems are sufficiently trained and aware of their obligations under the Data Protection Act and their Contract of Employment
   - Ensure that each system is regularly maintained and advise the DHRCS if system upgrades are necessary
   - Ensure that each passive CCTV system has adequate signage advising members of the public and staff that they are being monitored.

Directors are required to ensure that the policies relating to the installation and maintenance of CCTV and any modification thereto are brought to the SMT for approval

All Staff are legally bound by data protection legislation, the Common Law Duty of Confidence and their Contract of Employment to protect personal information in their care or charge. This policy sets out to protect personal information in electronic format, gathered by the legitimate monitoring of CCTV systems at BSO locations.

6. DOCUMENTATION

The Corporate Services Manager will ensure copies of all documentation and records relating to the CCTV systems are kept securely.

7. REVIEW

This policy will be reviewed every two years, or earlier in the light of new guidance or legislation.

8. NON-COMPLIANCE

A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action and /or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach.

In relation to the use of CCTV equipment, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.