Document Control

Policy Title	CCTV Policy
Policy Number	84
Owner	Information & Communication Technology Manager
Contributors	Information & Communication Technology Team
Version	1.0
Date of Production	01 September 2014
Review date	01 September 2016
Post holder responsible for review	Information & Communication Technology Manager
Primary Circulation List	Shared Drive
Web address	n/a
Restrictions	None

Version Control

Version Number	Owner	Description	Circulation
1.0	Information & Communication Technology Manager	Review	SMT

1.0 POLICY STATEMENT:

The purpose of this policy is to define the acceptable use and management of closed circuit TV (CCTV) throughout Sunbeam House Services (SHS).

In the interest of the safety and security of staff, clients, and the general public CCTV footage is recorded. This footage is only used for security purposes, NOT for supervision.

CCTV images come under *SHS Data Protection Policy*.

2.0 TRANSPARENCY

Section 2D of the Data Protection Acts requires that certain essential information is supplied to a data subject before any personal data is recorded. This information includes:

- the identity of the data controller;
- the purposes for which data are processed;
- any third parties to whom the data may be supplied.

This can usually be achieved by placing easily-read and well-lit signs in prominent positions. A sign at all entrances will normally suffice.

If the identity of the data controller and the usual purpose for processing – security - is obvious, all that need be placed on the sign is a statement that CCTV is in operation. A contact number for persons wishing to discuss processing should also be available. This contact can be either the security company operating the cameras or the owner of the premises.

If the purpose or purposes is not obvious, there is a duty on the data controller to make this clear. If the purpose of CCTV is also for health and safety reasons, this should be clearly stated and made known.

3.0 STORAGE AND RETENTION

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which they were obtained. A data controller needs to be able to justify this retention period. For a normal security system, it would be difficult to justify retention beyond a month, except where the images identify an issue – such as a break-in or theft - and is retained specifically in the context of an investigation of that issue.

The storage medium should be stored in a secure environment with a log of access kept. Access should be restricted to authorised personnel which are the ICT Manager and the designated Systems Administrator and Developer.

4.0 SUPPLY OF CCTV IMAGES TO AN GARDA SÍOCHÁNA

If the Gardaí request CCTV images for a specific investigation, the only individual authorised to distribute the CCTV image to the Gardai is the ICT Manager or the designed Systems Network Administrator and Developer with responsibility for CCTV on receipt of a valid Police Using Leading Systems Effectively (PULSE) number.

For practical purposes, a phone call to the requesting Garda's station may be sufficient, provided that the ICT Manager or designated Systems Network Administrator and Developer speak to a member in the District Office, the station sergeant or a higher ranking officer. It may be assumed that these personell are acting with the authority of a District/Divisional officer in confirming that an investigation is authorised.

5.0 ACCESS REQUESTS

Any person whose image has been recorded has a right to be given a copy of the information recorded. To exercise that right, a person must make an application in writing to the Data Protection Officer. Sunbeam House Services may charge up to €6.35 for responding to such a request and must respond within 40 days.

Practically, a person should provide necessary information to Sunbeam House Services, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data.

In giving a person a copy of his/her data, the Sunbeam House Services may provide a still/series of still pictures, a tape or a disk with relevant images. However, other people's images should be obscured before the data is released.

6.0 RESPONSIBILITIES OF SECURITY COMPANIES

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors". As data processors, they operate under the instruction of data controllers (their clients). Sections 2(2) and 2C of the Data Protection Acts places a number of obligations on data processors.

These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted.

Staff of the security company must be made aware of their obligations relating to the security of data.

Clients of the security company should have a contract in place which details what the security company may do with the data; what security standards should be in place and what verification procedures may apply.

Furthermore, section 16 of the Data Protection Acts 1988 & 2003 requires that certain data processors must have an entry in the public register maintained by the Data Protection Commissioner. Those parties who are required to be registered and process data whilst not registered are committing a criminal offence and may face prosecution by this office. (This provision may only apply where the data controller can identify the persons whose images are captured.)

7.0 SCOPE:

This policy represents SHS's position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All SHS Information Technology (ICT) resources which include equipment, systems and applications including cloud based applications.
- All users, and uses of SHS Information Technology (ICT) resources;
- All connections to (locally or remotely) SHS network (Local Area Network (LAN)/Wide area network (WAN))

8.0 ROLES & RESPONSIBILITIES:

8.1 Users

Each user of SHS's ICT resources is responsible for:-

8.1.1 Complying with the terms of this policy and all other relevant SHS polciies, procedures, regulations and applicable legislation.
8.1.2 Respecting and protecting the privacy and confidentiality of the information they process at all times.
8.1.3 Complying with instructions issued by the ICT Manager on behalf of SHS.
8.1.4 Reporting all misuse and breaches of this policy to their Senior Manager.

8.2 Senior Managers

In addition to each user's responsibilites, Senior Managers are directly responsible for:-

8.2.1 The implementation of this policy and all other relevant SHS policies within the business areas for which they are responsible.
8.2.2 Ensuring that all SHS employees who report to themare made aware of and are instructed to comply with this policy and all other relevant SHS policies.
8.2.3 Consulting with the ICT Manager in relation to the appropriate procedures to follow when a breach of this policy has occurred.

8.3 ICT System Administrators& Developers

Each SHS System Administrator & Developer is responsible for:-

8.3.1 Complying with the terms of this policy and all other relevant SHS policies, procedures, regulations and applicable legislation.
8.3.2 Retrieval of CCTV footage only on instructions from ICT Manager
8.3.3 Complying with instructions issued by the ICT Manager on behalf of SHS.

8.4 ICT Manager

In addtion to the above responsiblities the ICT Manager is responsible for any retention of images retrieved from a recording CCTV system within SHS.

9.0 GUIDELINES:

9.1 CCTV retrievable footage can only be used for the security of clients, staff, general public and SHS property.

9.2 CCTV is used as an aid for supervision where it is a live system and the images are not recorded.

9.3 The only indivduals who can retrieve footage from CCTV's are ICT System Administrators & Developers, ICT Manager and the relevant CCTV contractor.

10.0 ENFORCEMENT:

10.1 SHS reserves the right to take such action as it deems appropirate against users who breach the guidelines of the policy

10.2 Breaches of this policy by a third party, may lead to the withdrawal of SHS information technology resources to that third party and/or the cancelleation of any contract(s) between SHS and the third party.

10.3 SHS will refer any user of its ICT resources for illegal activities to the appropriate law enforcement agencies.