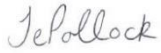
PROCEDURE NAME	CCTV Policy	**PROCEDURE NO.**	GDPR, 004
MANAGER RESPONSIBLE	Joanna Pollock	**VERSION NO.**	3.0
SIGNATURE		**APPROVALS DOCUMENT OWNER**	JP

VERSION HISTORY				
VERSION	**REVIEWED BY**	**ISSUE DATE**	**DESCRIPTION OF CHANGE**	**APPROVED BY**
2.0	Michéal O'Neill	13.06.2022	Updated format	MON
1.0	Máire Hussey, Úna Houlihan	18.08.2020	Initial release of document	MH, UH

1. INTRODUCTION

SouthDoc operates in a highly controlled and regulated environment.

To support this CCTV installation and operation is necessary for the following:

- To monitor the security of premises.
- To prevent, detect, and investigate a crime that may have occurred on SouthDoc property.
- To support and ensure the safety of staff.
- To protect and monitor property, including Medication stored on site.

2. PURPOSE

The purpose of this document is to ensure that the use of CCTV adheres to the principles of the GDPR and to provide guidance, information and transparency related to the use of CCTV and CCTV footage across the organisation.

3. SCOPE

This policy applies to all SouthDoc staff, students, contractors, sub-contractors, agency staff and any other persons who may, from time to time be present on any of its premises.

4. DEFINITIONS

A list of terms used throughout this policy are defined in Appendix 1.

5. INSTALLATION

The installation of all CCTV must be in accordance with this policy and should remain appropriate to its original identified and documented business purpose.

The positioning of cameras are near sensitive areas such as the entrance point of the Treatment Centre, and Medicine Stores. However, they will never be placed in private areas such as toilet facilities.

6. STORAGE AND RETENTION

The CCTV footage captured from SouthDoc cameras are securely stored as electronic data and is retained for a period of 30 days.

It is deleted following this 30-day period unless a request is made for particular footage.

As guided by Section 8 of the Civil Liability Act, a 30-day retention period has been selected as a reasonable and proportionate timeframe for the purposes of defending a potential personal injury claim.

7. ACCESS

Access to and disclosure of CCTV footage to third parties is strictly controlled and documented. This is to ensure that the rights of the individual (s) are maintained and that the chain of evidence remains intact should the CCTV images be required for evidential purposes.

In relevant circumstances, CCTV footage recorded by SouthDoc may be accessed by:

- An Garda Síochána, 'and other competent bodies for law enforcement purposes, ('Competent authority' is defined at Section 69 of the Data Protection Act 2018), where SouthDoc is required by law or following a written request to make a report regarding a suspected crime or incident.
- Individuals whose images have been recorded by SouthDoc CCTV and who have submitted a valid SAR or FOI.
- In exceptional circumstances, CCTV footage may be used in the context of a formal internal investigation or disciplinary procedure concerning staff member.

When CCTV footage is being provided to an approved third party, a record of the request is documented on the secure disclosure logging database ('log').

Within the 'log' the following information is recorded:

- Reason for disclosure
- Details of the image disclosed (i.e. the date, time, and location of the image.)
- Identity of the person who released the CCTV image (s).

Subject Access Request for CCTV Footage

Any individual who is identifiable from the image which has been recorded by a SouthDoc CCTV camera is provided the right of access to their personal data under GDPR.

Upon receipt of a data access request for CCTV footage, the DPO must process them within one month. If they require additional time, the data subject must be notified.

If the SAR is made after the 30-day retention period and the footage has been erased, the data subject should be advised of this. If the request is made within the 30-day retention period, the footage should not be erased until the data access request has been processed.

The format in which the CCTV footage is provided is either on a disc or memory stick. If it is impossible to copy the footage from the CCTV system to another device for whatever reason, it is acceptable to provide pictures for the duration of the recording in order to comply with the SAR.

Where images of parties other than the requesting data subject appear on the CCTV footage, SouthDoc must pixelate or otherwise de-identify, as appropriate, the images of other identifiable parties before supplying a copy of the footage to the requester. Alternatively, SouthDoc may seek the consent of those other parties whose images appear in the footage to release an unedited copy containing their images to the requester.

8. COVERT SURVEILLANCE

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on an exceptional case-by-case basis where the data are kept for the purposes of preventing, detecting, or investigating offences, or apprehending or prosecuting offenders.

Covert surveillance must be focused and of short duration. A DPIA should be carried out prior to the installation of any covert systems, to clearly assess whether the measure can be justified on the basis of necessity and proportionality to achieve the intended purpose. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease.

9. FACIAL RECOGNITION AND BIOMETRIC DATA

Specific technical features of certain CCTV systems, such as the use of facial recognition software, may be a factor in determining the basis on which the data can be lawfully processed. Facial recognition processing involves a matching step where previously seen faces are registered and recorded on the system so that when and if they appear again, they are matched and can uniquely identify the individual in question. Facial recognition processing is considered biometric processing and accordingly the data processed is categorised as "special category" of personal data subject to the requirements of the GDPR, which, sets out further conditions to provide for the lawful processing of the data.

Any processing of biometric data should be considered as separate to the regular usage of the CCTV system and a data controller engaging in such processing must take all steps to ensure that it is compliant with the data protection legislative frameworks.

10. DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

For this reason, a DPIA must be carried out prior to installing any CCTV cameras.

11. RESPONSIBILITIES

SouthDoc Management are responsible for the enforcement of this policy.

12. ASSOCIATED DOCUMENTS

The following documents will provide additional information:

- Data Protection Policy
- Data Breach Incident Report
- Mobile Computing or Storage Device Incident Report
- Data Breach and Incident Log

13. POINTS OF CONTACT

The first point of contact for any queries or requests should be directed to the DPO at SouthDoc Head Office.

Email:	dpo@southdoc.ie
Phone:	064 6691974
Postal address:	Data Protection Officer, Floors 2&3 Hillard House, High Street, Killarney, Co. Kerry V93 K0DN

If one requires additional information on Data Protection, they should contact the Office of the Data Protection Commissioner (The supervisory authority).

Email:	dpo@dataprotection.ie
Lo call number:	1800 437 737
Postal address:	Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28

APPENDIX 1: DEFINITIONS

CCTV
Closed Circuit Television is a technology that uses video cameras to transmit signals to a specific place but does not transmit publicly.

Data Controller
A person or organisation who determines the purposes and methods of processing personal data.

Data Processor
A person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.

Data Protection Impact Assessment (DPIA)
A data protection impact assessment is a risk assessment audit designed to assist organisations in identifying, analysing, and minimising the privacy risks that come with collecting, processing, using, storing, and sharing user data. It is one of the key components required to comply with GDPR.

Data Protection Officer (DPO)
The role within a company whose responsibility is to ensure that the company or organisation is correctly protecting individuals' personal data according to current legislation.

Data Subject
A living individual to whom personal data held relates, including: employees, patients, suppliers. It should be noted that GDPR do not apply to deceased persons and to their data.

Freedom of Information (FOI)
Freedom of Information applies only to public bodies such as Government Departments, State Agencies and other public bodies receiving state funding in Ireland.

Freedom of Information Requests provides access to copies of original records and these records can include material across a broad range including statistics, reports, emails, or records that do not contain any personal information.

GDPR
General Data Protection Regulations.

Personal Data
Personal data is any information relating to an identified or identifiable living person (data subject) who could be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location, DOB, or to one or more factors specific to the physical, physiological, genetic, economic, cultural, or social identity of that individual.

Subject Access Request (SAR)
A written request made to the data controller by any individual about whom a data controller keeps personal data on computer on in a relevant filling system. Response must be provided to the data subject under the terms outlined by GDPR and/ or local requirements.

Special Category Data
GDPR provides extra protection for certain categories of personal data, called 'special category data' – referring to data which reveals:
"Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

These categories of personal data shall not be processed unless a controller can avail of one of the exceptions under Article 9 (2) of the GDPR.