Premises Security – CCTV Policy

Descriptor	Changes made	Date	Version
Policy first implemented	Policy published		1.0
Review no.1			
Review no.2			
Review no.3			

Name of policy being superseded (if applicable)	N/A
Related policies	Data Protection Policy
	Premises Security Policy
	Clear Desk Policy
	Complaints Policy
Related SOPs/process	N/A
Related Guidance	Data Protection Impact Assessment
	EIS Monitoring Guidance
	Employee Privacy Notice
	Early Concerns and Grievance Procedure
	SDS Data Request form
Equality Impact Assessment completed	No
Island Community Impact Assessment completed	No
Intended Audience	All colleagues
For publication	Internally and externally
Team responsible for policy	Property and Facilities
Policy owner contact details (email)	Derek.Cairns1@sds.co.uk
Policy due for review (date)	September 2025

Policies should have a clear purpose and perform at least one of the following functions. Please identify all the functions this policy performs.	If statement applies, please mark with an X below
Outline how we allocate limited resources to deliver services or outcomes	
Outline how SDS adheres to legislation	X
Ensure fair and consistent allocation of benefits	
Protect organisational assets, including data	X
Define expectations around the employee/employer relationship	
Other (please specify)	

Skills Development Scotland

Contents

Skills Development Scotland

1. Policy summary

Surveillance Camera Systems also known as ‘CCTV’ have a legitimate role to play in helping to maintain a safe and secure environment for all SDS colleagues, customers, and visitors. However, this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by CCTV systems are personal data which must be processed in accordance with UK Data Protection legislation and SDS’s Data Protection policy. This policy is designed to help SDS comply with its legal obligations; it is also intended to assist colleagues to comply with their own legal obligations when working with personal data. In certain circumstances, misuse of data generated by CCTV could constitute a criminal offence.

2. Policy purpose and objectives

SDS makes use of CCTV to help maintain a safe and secure environment for all SDS colleagues, customers, and visitors. This policy is intended to give a clear and transparent description of how CCTV will be used by SDS and what controls and parameters must be applied so that its use is legally compliant, appropriate, and proportionate. It is designed to help SDS comply with its legal obligations, particularly regarding privacy and data protection, and to help colleagues to comply with their own individual legal and policy obligations when working with personal data. Further information is set out in the SDS Data Protection Policy.

3. Strategic context

SDS currently uses CCTV cameras to routinely view and record individuals on and around its premises. This policy outlines the use of CCTV and the processing of data recorded by CCTV cameras to ensure that SDS is compliant with data protection law and best practice.

SDS recognises that images of individuals recorded by CCTV cameras in the workplace constitute personal data and are therefore subject to Data Protection Legislation. SDS is the data controller for any personal data processed by CCTV cameras on SDS premises.

SDS uses CCTV around its site for the following legitimate business purposes:

- To assist in day-to-day management, including ensuring the health and safety of SDS colleagues, customers, visitors and other members of the public and to act as a deterrent against crime.
- To monitor the security of buildings.
- To prevent crime and protect buildings and assets from damage, disruption, vandalism, and other crime.
- To support law enforcement bodies in the prevention, detection, and prosecution of crime.
- To assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.
- To assist in the defence of any civil litigation, including employment tribunal proceedings.

4. Definitions

Closed circuit television (CCTV) – is a surveillance system designed to capture and record images of individuals, or information relating to individuals and property. Primarily this is a system of fixed cameras.

Data Controller – a person or organisation that determines the purposes and means of processing personal data.

Data Protection Impact Assessment (DPIA) – a risk assessment process which helps to identify and reduce the data protection risks of processing personal data (in this case, the use of CCTV).

Data Protection Legislation – the legislation relating to the processing of personal data current in force in the United Kingdom, which includes the Data Protection Act (2018) and the UK GDPR.

Data Protection Team – the team which ensures SDS's compliance with Data Protection Legislation, including the management of Subject Access Requests, Data Breaches, and generally provides advice and guidance in relation to this subject matter (contactable at **DPO@sds.co.uk**).

Subject Access Request – a request made by a person (e.g., individual member of public, customer, and/or SDS employee) to access their own personal information. In the context of this policy, which would include a person requesting to access specific CCTV footage that includes images of themselves. SDS has a calendar month to provide a response to these requests upon receiving them, and the Data Protection Team (**DPO@sds.co.uk**) should be immediately notified of any such requests that are received.

5. Scope

This policy is applicable to all SDS colleagues, including contractors and agency workers based in SDS premises, who have a duty to familiarise themselves with this policy. For sites that are in the control of other organisations (including schools and partner organisations), SDS colleagues should familiarise themselves with, and follow, the CCTV policy of the controlling organisation.

6. Policy detail

6.1 CCTV Operation

- CCTV systems operate 24 hours a day, seven days a week.
- CCTV camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras are not focussed on private homes, gardens, or other areas of private property.
- As far as practically possible CCTV cameras are not focussed in areas where there is a reasonable expectation of privacy, such as meeting rooms or private interview rooms (see Section 6.5).
- CCTV camera systems are not configured to record sound. This will only change in the event that an updated DPIA recommends that doing so is necessary and proportionate to achieve the business purposes listed in Section 3, and that following due consultation SDS senior management are in agreement with this recommendation. In this event, this section of the Policy will be updated to reflect any change.

- Authorised SDS colleagues, and contracted uniformed security guards, may use body worn cameras in response to specific events. Where this is required, this will be implemented in line with the requirements set out in both the CCTV and Data Protection Policies.
- SDS colleagues must not use CCTV systems until they have completed appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.
- The Property & Facilities Manager is responsible for approving all existing and new use of CCTV. In considering such use, the Property & Facilities Manager seeks advice as appropriate from the SDS Data Protection team.
- Where CCTV cameras are placed in the workplace, SDS ensures that adequate signs are displayed to alert individuals that their image may be recorded.
- Only authorised colleagues monitor live feeds from CCTV cameras where it is deemed reasonably necessary, for example to protect health and safety or to ensure that the CCTV system is operational.
- Recorded images are viewed only by authorised and trained SDS colleagues.
- Recorded images are only viewed in designated, secure offices.

6.2 Management and access

- The CCTV system is managed by the Property & Facilities Manager and on a day-to-day basis the CCTV system is operated remotely by the Property & Facilities Team.
- The viewing of live CCTV images is restricted to the Property & Facilities Team and the system is password protected.
- Recorded images which are stored by the CCTV system will be restricted to access by the Property & Facilities Team or any colleague on site who has been granted temporary approval to access by the Property & Facilities Manager. A record of all temporary access approvals will be kept by the Property & Facilities Manager.
- No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy for the disclosure of images.
- The CCTV system is checked monthly by the Property and Facilities Team to ensure that it is operating effectively, with further access only permitted:
    - in the event that an incident is reported; or
    - where a SDS Data Request or Subject Access Request is submitted as outlined in sections 6.8 and 6.9.

6.3 Use of Data gathered by CCTV

- Data gathered from CCTV cameras is transmitted and stored in a way that maintains its confidentiality, integrity, and availability, in order to ensure that the rights of individuals whose images recorded by the CCTV systems are protected.
- Data is password protected and only accessible to identified members of the Property and Facilities team.
- No third parties have access to the SDS CCTV systems or data.

6.4 Storage and Retention of CCTV images

SDS ensures that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- Where possible CCTV recording systems are in restricted access areas.
- CCTV systems are password protected.
- Restriction of the ability to make copies to specified SDS colleagues.

Images are normally retained for 31 days, but can be held for longer in the following circumstances:

- Where compliance with a legal obligation requires an extended retention period; or
- In specific circumstances in which longer retention periods are required to establish patterns of behaviour or to retain evidence. For further information of covert CCTV monitoring, please refer to section 6.6.

Data and images recorded by the CCTV system are permanently and securely deleted once the purpose for which they were collected has expired. The Property & Facilities Team maintain a log of when data is deleted. Any physical material including tapes, discs, hard copy prints and still photographs, etc. are disposed of as confidential waste.

6.5 Additional Surveillance Camera Systems

- An update to the DPIA for CCTV will be considered, if necessary, e.g., prior to introducing a new surveillance camera system or placing a new CCTV camera in a workplace location.
- In very exceptional circumstances and only where it is judged to be strictly necessary and to deal with the most serious concerns or dangerous circumstances, will CCTV cameras be placed in areas where there is an expectation of privacy. This includes private interview rooms or meeting rooms. Where this is judged to be required, any needed signage will be installed and the DPIA will be reviewed to ensure the usage is necessary and appropriate.

6.6 Covert CCTV Monitoring

- SDS will only engage in covert CCTV monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) in highly exceptional circumstances. This includes where there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, SDS reasonably believes there is no less intrusive way to tackle the issue.
- The implementation of covert monitoring must be approved by the Property & Facilities Manager, the Data Protection Officer and a Senior Director. Where approved, a TU official will be notified upon each approval of covert CCTV use with the generalities, but not specifics, of the case.

- Covert monitoring must only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and must only relate to the specific suspected illegal or unauthorised activity.

6.7 Review of CCTV use

- The ongoing use of existing CCTV cameras in the workplace is reviewed every 6 months by the Facilities Manager. This will ensure that their use remains necessary and appropriate, and that any surveillance camera system is continuing to address the business needs that justified its introduction. A request can be made to introduce CCTV to an SDS premises or area of an SDS premises where no CCTV currently exists where the business believes there is sufficient justification. This can be made by an Area Manager or a Head of Service to **facilities@sds.co.uk**. The Facilities Manager will then conduct a security risk assessment and consult with the SDS Health & Safety Advisor to determine if CCTV is required.

6.8 Requests from law enforcement to access CCTV footage

- The release of, or access to, recorded footage to law enforcement in order to aid an investigation, will only be carried out on the approval of the Property & Facilities Manager and the Data Protection Team.
- Any such request must be valid and lawful, and the **SDS Data Request Form**, must be completed by the requesting party (e.g., Police Officer, Solicitor).
- For purposes of clarity, this type of request is **not** a Subject Access Request. This would be covered under Section 6.9 below.
- The completed SDS Data Request Form should be submitted to **DPO@sds.co.uk**.

6.9 Subject Access Requests (SARs)

- Under UK Data Protection legislation, individuals (referred to as 'data subjects') may make a request to access a copy of their personal information, which can include CCTV images. These are known as a Subject Access Requests (SAR), and the procedures are set out in the Data Protection Policy.
- Under law, SDS has one calendar month to respond to an individual that makes a SAR. As soon as a SAR is received by SDS, this must be forwarded as soon as possible to the SDS Data Protection Team (**DPO@sds.co.uk**) so that the response to the request can be managed within the legislative timeframes.

6.10 Other Requests for use of CCTV footage

- Images from CCTV cameras are not routinely disclosed to other third parties, without express permission being given by the Data Protection Team who must ensure that the disclosure observes the Data Protection Legislation.
- No images from the CCTV system or recordings in any format are posted online or disclosed to the media.

6.11 Misuse of CCTV

- The misuse of the CCTV system without proper authorisation is strictly prohibited. This includes attempting or gaining unauthorised access, tampering with CCTV equipment, including disconnecting from power or blocking or defacing the camera lenses, and attempting to delete/download or deleting/downloading data from the system. Carrying out such actions could constitute a criminal offence.
- Any employee who breaches this policy may be subject to disciplinary action, up to and including dismissal.

6.12 Complaints

- Any questions about this policy or any concerns about SDS's use of CCTV should be raised with the Property & Facilities Manager in the first instance. If the issue cannot be resolved, the complaint can be escalated in the following ways:
    - Member of the public complaints – in line with the Complaints Policy
    - Colleague complaints - by speaking with your line manager in the first instance and following the Early Concerns and Grievance Procedures

7. Monitoring and Review of Requirements

This policy will be reviewed annually, or following Lessons Learned reports from relevant security incidents, and will be updated as required by the Property & Facilities Manager with input from relevant colleagues across the organisation including:

- Information Governance, Resilience and Risk (Data Protection, Information Management and Business Continuity & Resilience)

Final approval will be by the Senior Director of Delivery.

8. Further guidance

Further guidance on Security and Data Protection policies and procedures is available on Connect.