SURVEILLANCE CAMERA POLICY

We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.

Owner: SIRO
Document ID: ICT-PL-0115
Version: 1.2
Date: March 2021
Review date: March 2023

DOCUMENT MANAGEMENT

Version	Date	Summary of Changes
1.0	August 2018	First version
1.2	March 2021	Review and Updates

Accountable Owner		Approval date
Senior Information Risk Owner (SIRO)	Chris Bally	02/07/2021

Responsible Owner		Approval date
Head of Information Governance	Peter Knight	21/04/2021

Reviewers	Role	Approval date
Policies Review Group: Russell Armstrong Philip Barbrook Anna Stephenson (policy review lead) Joanne Withey Corporate Information Governance Board - ratification	 IT Security Manager Enterprise Architect DPO & Compliance Manager DP & Training Manager	18/05/2021 29/07/2021

Publication information		
	Published (if YES, enter document location)?	**Location**
All staff	Yes	mySCC
Public	Yes	SCC website

1. Introduction

a) The purpose of this policy is to set out what steps must be followed by all staff and business units where surveillance cameras are to be deployed in any context for SCC business to ensure that:

- Ensure that the business benefits of having such surveillance are realised.
- There is clear understanding of data/information asset ownership and responsibilities by SCC and its contractors/business partners.
- Privacy, and information security risks are adequately considered prior to deployment of cameras and are managed effectively once they are operational.[1]

b) SCC has deployed forms of surveillance cameras for many years, and they continue to fulfil the primary purpose of protecting the health and safety of SCC staff, partners and visitors within the footprint of SCC buildings. But it is increasingly important to be clearer on policy and process in this area because:

i. Changes in law – UK GDPR/Data Protection Act (2018) – require SCC to always apply extra rigour in how it balances any business need with the privacy of individuals. As technology improves, such as sharper picture quality and the ability to zoom, so too do the questions around how far more personal data is captured than is strictly necessary for the purpose.

ii. Surveillance camera infrastructure is relatively straightforward to procure for any business unit with a budget (i.e. not centralised entirely to IT or estates). This means that it is especially important to be clear on the ground rules, so there is consistency across SCC regardless of which business unit 'owns' the surveillance camera infrastructure.

iii. It is commonplace to engage one or more supplier to manage surveillance cameras on behalf of SCC. Where this is the case it is essential to be clear on respective responsibilities as data controller and data processor.

iv. Finally, as surveillance cameras become part of IT networks and potentially accessible via the public Internet, a set of cyber-risks emerge which can impact on information and services in other areas (i.e. the security risks to the entire IT network could outweigh the health and safety benefits of having the cameras if not properly assessed).

c) This policy should be read in conjunction with the following document:

[1] This policy follows The Surveillance Camera Code of Practice (2013) for England and Wales under the provisions of the Freedoms Act 2012 as well as GDPR/Data Protection Act (2018).

- Data Protection Policy.

2. Scope

'Surveillance camera'[2] is used to describe any device set up by SCC with the purposes of capturing images for a fixed period or on an ongoing basis for one or more lawful business purposes. 'Surveillance camera system' describes the entire IT infrastructure used to support one or more cameras which may have a relationship to the wider SCC IT network and/or the public Internet.

a) This policy covers the deployment of any type of surveillance camera inside or outside of buildings owned or managed wholly or partially by SCC. It also includes body-worn or mobile cameras (e.g. wirelessly operated cameras which may be moved from place to place for short periods), where they operate within the footprint of SCC buildings/sites, or are used for business surveillance purposes. In the case of shared buildings this policy will apply to where SCC business units are officially based.[3]

b) This policy does not include schools in Suffolk - regardless of how funded - as they operate as their own data controllers (solely or as groups) and have their own business requirements. Nor does it include any buildings or working environments which SCC staff may be permitted to use on occasions (e.g. Police, other councils, NHS etc.), but do not constitute SCC official buildings.

c) This policy does not include the use of surveillance cameras in public areas (i.e. where cameras are located to capture images from outside the footprint of SCC buildings/sites on public roads or Fire & Rescue Service aerial surveillance 'drones' etc.), or the taking of photographic images/video that are for business purposes other than surveillance.

d) This policy does not include the use of surveillance cameras by persons in domestic settings (e.g. homes of those providing foster care for children funded by SCC), nor does it cover the use of cameras owned by members of staff in their own vehicles (e.g. when parked in SCC premises).

3. Roles and responsibilities

a) **Information Governance Team**: is tasked with implementing this policy and monitoring its effectiveness.

[2] This term is used in preference to Closed-Circuit Television or CCTV which no longer accurately describes what is being deployed.
[3] The organisations which share buildings (e.g. other councils) may or may not sign up to the same policy as SCC depending on specific contractual arrangements.

b) **Managers**: are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided where they are owners of surveillance camera information.

c) **Users**: all users must complete all mandatory training modules. Line managers have a responsibility to support this training and must raise with HR if any staff member does not or cannot complete the training.

d) **Non-compliance with this policy**: non-compliance with this policy by staff may lead to further action and investigation under the Council's Disciplinary Procedures. In certain circumstances, non-compliance with this policy may be considered gross misconduct resulting in dismissal. Councillors found to be in breach of this policy may be deemed to have breached the Members' Code of Conduct which may lead to a referral to the Council's Monitoring Officer.

e) **Security incidents**: users must report all suspected security incidents via IT Self Service, *Report an Incident*.

4. Agreed purpose for surveillance at SCC

a) The lawful basis for processing personal data is for SCC to carry out its statutory and public task duties to safeguard the health and safety of its employees and members of the public who are visiting its sites.

b) The primary purpose of all surveillance cameras at SCC is to protect the health and safety of staff, suppliers, partners and members of the public visiting the site and the security of assets within the footprint of its buildings in the following ways:

i. Visual check that entry points to buildings that require passes or keys are working as intended.
ii. Visual check that car park and barriers are operating as intended.
iii. Visual check that unauthorised persons are not attempting to gain entry.
iv. Visual deterrent to non-authorised persons who may consider gaining entry
v. Visual check of any suspicious behaviour which could lead to damage to property or cause distress/harm to individuals.
vi. Visual check on persons and vehicles (including the recording of number-plates) to ensure that buildings and sites (such as waste disposal) are being used in accordance with the rules.
vii. Visual check to enable better business continuity management (e.g. how fire-drills were conducted).
viii. Image data that enables the Council and its contractors to operate services in such a way as to ensure compliance with contract specifications.

ix. Use image data to assist with a disciplinary or other investigation relating to a member of staff or members of the public where health/safety/security/fraud is relevant.

In the event of mobile or body-held cameras being deployed, they should still be used only for the above purposes.

c) It is possible that activities are recorded on images which could constitute criminal offences (and there is a process to follow in regard to sharing information from surveillance technology with law enforcement agencies, see below). It should be noted that the detection and prevention of crime is not the primary purpose of SCC cameras.

d) No one in SCC can procure surveillance cameras for any other purpose (e.g. monitoring staff behaviour/performance, profiling visitors etc.) or include audio (i.e. the ability to listen as well as gain images) without consulting the Council's Data Protection Officer and gaining approval from the SCC Buildings Security Committee.

5. Ownership

a) Where surveillance cameras are deployed in SCC buildings and are capable of capturing personal data, then SCC is a data controller (or in special circumstances joint data controller) as defined by the UK GDPR/Data Protection Act (2018). Additionally, dataset owners must be identified within SCC for any deployment of surveillance cameras.

b) The Corporate Property Team in SCC is responsible for most (but not all) camera systems and its head is a dataset owner. Any existing camera system outside the remit of Corporate Property must be clearly owned (i.e. responsibility for the personal data collected by camera systems must be allocated to an dataset owner and recorded in the relevant Directorate's Register of Datasets).

6. Governance for new surveillance

Any head of service in SCC can make a case for the deployment of new surveillance cameras. But the following steps must occur:

a) Seek advice from the Head of Corporate Buildings who will assess whether existing infrastructure could be used to meet the new requirement, and whether the use of surveillance cameras is the best approach to deal with the problem.

b) If new infrastructure is sought (i.e. cameras, systems) then it must be agreed in principle by the SCC Buildings Security Committee who will ask for evidence that the essential steps are undertaken (see paragraph 7 below).

c) If the cameras are to be used for a purpose other than to uphold the health and safety of staff and visitors to buildings/sites then the Data

Protection Officer must be consulted, and the new purpose approved by the SCC Buildings Security Committee with consultation with the Corporate Information Governance Board.

d) No individual member of staff is permitted to install any ad-hoc surveillance cameras (e.g. portable wireless camera in part of the office) in any SCC property. The use of unauthorised devices could lead to disciplinary action against the person(s) installing or operating them (and possible legal action e.g. voyeurism under Sexual Offences Act 2003).

e) No member of staff should attempt to interfere with SCC surveillance cameras. Any complaints about their usage should be made using the procedure outlined in paragraph 14 below.

f) All staff should report any information security concerns about surveillance cameras (e.g. obvious faults, vandalism) to facilities management in the first instance.

7. Essential first steps for deploying cameras

a) Ownership

It will need to be clear who the dataset owner is at SCC (i.e. head of service responsible for the information collected by cameras). It will also need to be clear which business unit is responsible for the payment and any contractual and service management review arrangements of surveillance camera systems with suppliers.

b) Personal data processing

It will need to be clear whether the use of surveillance cameras will mean that personal data will be captured intentionally or unintentionally. **Note**: some cameras can be configured just to observe and detect (i.e. no personal data required) or to identify and recognise (i.e. which does require personal data). Improvements in technology can mean that it is difficult not to identify people unless the right configuration is in place.

c) Data Protection Impact Assessment

Any deployment of new surveillance cameras that involves the processing of personal data will require a Data Protection Impact Assessment (DPIA). This will include – among other things - an assessment of:

i. Purpose and nature of data to be collected (including whether special category is processed).
ii. The type of technology deployed and whether this raises privacy or security risks.
iii. How data is to be managed and shared. And the use of any suppliers as data processors.
iv. Proposed retention, review and disposal of data.

8. Suppliers & contracts

It is highly likely that one or more supplier may be engaged to manage all or certain aspects of the surveillance camera operation on behalf of SCC (at the very least the provision of actual hardware/software). The following must be clear:

a) **Ownership of infrastructure**: SCC Corporate Property has to date owned the surveillance infrastructure (i.e. cameras, servers and other hardware and the network) operated in core buildings across Suffolk. Alternative models (e.g. where another business unit owns infrastructure or where equipment is leased from suppliers or where SCC IT network and infrastructure is used) are possible. However, advice must be taken from the Head of Corporate Buildings and Buildings Security Committee to assess whether there are any financial and non-financial risks to SCC as a whole by so doing.

b) **Management of service:** where day-to-day management is to be carried out by a supplier, it must be clear in the contract and/or other documentation what tasks it is carrying out and whether it is a data processor.

   It should be noted that although such suppliers are usually data processors, there are occasions when considerable latitude/discretion is given to a company which could make them responsible in part (i.e. a controller) for the purpose and/or means by which personal data is processed. This needs to be clear by all the parties and documented in the supplier's Data Processing Schedule (see Appendix B of the DPIA).

c) **Technical standards**: the SCC business owner of the surveillance camera must discuss with suppliers any relevant technical and quality standards (equipment and processes) that are relevant to the deployment using the list of standards provided by the UK Surveillance Camera Commissioner.

   It should be noted that a supplier meeting a particular technical standard should be viewed in positive terms, but this is not a substitute in any way for doing a data protection impact assessment and other information security assurance work.

d) **Shared services & SCC as a supplier**: where SCC is part of a shared service arrangement (e.g. with another party such as a council at a shared building), it needs to be clear whether SCC is:

   i. acting as a sole or joint data controller for all the personal data collected across the entire shared sites, or

ii. data controller for personal data collected in some sites/zones where SCC staff work and a data processor for the data relating to non-SCC staff, or
iii. is a data processor on behalf of other parties since no SCC staff work in a particular area/zone.

The most practicable option needs to be agreed by the parties and documented.

e) **GDPR clauses and standard contracts**: a contract must follow SCC standard templates. Particular attention should be given to:

i. Sub-contracting. Where the supplier of surveillance cameras wishes to engage another supplier other than that specified in the original contract (e.g. specialist maintenance tasks or because it needs extra capacity) then SCC must be informed and has the right to object.
ii. Supplier must inform SCC as data controller without undue delay and no later than 24 hours if there is an information security incident relating to its operations.
iii. Any data must be returned or securely destroyed at end of contract, and for this to be documented.
iv. Business continuity: to set out the service level required, the recovery time objective and maintenance arrangements (including warranty periods for equipment).

9. Risk management and operations

In addition to the data protection impact assessment, the following security and other controls need to be in place:

a) **External siting of cameras**: cameras need to be sited in locations which capture data within the footprint of SCC buildings (i.e. not on to public streets or other properties). Where it is not possible to do this with the siting and angle of cameras, then technology should be deployed which pixelate non-SCC buildings.

b) **Internal siting of cameras**: cameras can be sited within SCC buildings (for the same purposes specified above) in office spaces, adjacent to or in sensitive areas (e.g. where there is cross-working with Police) or sensitive assets (e.g. computer server rooms).

Such cameras are ‘overt’ and staff are informed via signage and mandatory security training that monitoring takes place in the work place that balances privacy with lawful business requirements.

Any request for more intrusive surveillance or covert cameras for a strictly limited period in the event of an investigation about an individual must be approved by the SCC Head of Human Resources with advice from SCC Data Protection Officer. Where the individual is a Councillor, the Head of

Scrutiny must be consulted to assess whether such action is proportionate.

c) **Signage**: A sign – which acts as privacy/fair processing notice – must be located in a prominent position where a person can view it prior to entering a building/site. It should state the name of the data controller (SCC or exceptionally jointly with another party), the purpose for data processing (health and safety of staff and visitors) and contact telephone number of team in SCC who can assist with privacy enquiry.

So as to prevent confusion, the data protection sign should be separate from any other signage (e.g. parking charges, disclaimers about property damage etc.).

d) **Data storage and network segregation**: The data which is captured on cameras can be stored locally (i.e. adjacent to the cameras) or remotely (i.e. another geographical location). In each case such data needs to be held in locked rooms/cabinets with strictly controlled access to nominated persons. If the intention is to store the camera data outside of the UK, then the Data Protection Officer must be informed.

Where data from cameras is networked (i.e. not stand-alone, but cameras linked together and potentially to wider SCC IT network) then they must be virtually or physically separated to the satisfaction of the SCC IT Security Manager.

e) **Cyber risk mitigation**: where a surveillance camera network is linked virtually or physically to SCC wider IT network and/or the public internet (i.e. IP- Internet Protocol cameras) then SCC as data controller must have evidence from the supplier(s) prior to implementation that such equipment and software is a) still technically supported by vendors, b) up to date patches/versions and c) regular penetration test of such camera network by supplier on its network, and penetration test/health check by SCC where the data is on its IT network.

f) **Real-time monitoring**: it is permissible for footage on any surveillance camera deployed at SCC to be monitored in real time by designated suitably screened SCC or supplier personnel from any location in the UK.

The dataset owner, with advice from the Council's Corporate Property Officer, will instruct the suppliers which cameras simply record image data, and which are also monitored on a real-time basis. The privacy aspects of this should have been considered at data protection impact risk assessment stage.

Any business requirement for remote access by SCC or supplier personnel to data to carry out live monitoring and/or access technical or stored data needs to be risk assessed prior to implementation and documented (i.e. Direct Access from an official SCC device to the camera service data, or via the public Internet using any device).

Note: there are many practical benefits from such remote access, such as the ability to detect faults and business continuity when normal monitoring room is inaccessible. But this needs to be balanced with the security risks of an unauthorised person being able to view images (which may be personal data) or close down/disrupt the surveillance camera operations.

g) **Data retention and compression**: the standard period for retaining image data on cameras at SCC is 30 days (from date the image is recorded). There must be a strong business reason for any period longer than this (and for it to be documented).

Where data is to be deleted it needs to use a method that means data cannot be reconstructed (e.g. degaussing in the case of tape).

It is acceptable for a form of compression to be used on stored data, so long as it can be easily reviewed, and picture quality is sufficient for business purposes (e.g. identification of persons where this is necessary).

h) **Transporting image data**: SCC surveillance camera systems should be designed so that data remains on a standalone server or is transferred via a network to another server on the surveillance network.

In special cases when image data needs to be transported, such as when shared with SCC/Police/Courts in the event of an investigation, then it must be downloaded onto an encrypted device.

10. **Reviewing data**

SCC surveillance camera systems should be designed so that data relating to a particular site/date can be reviewed using software in use at SCC. Preference should be for viewing data on-site. A log book or audit trail should be kept detailing a) who viewed the data. b) what data (e.g. x camera data for 1 to 3 Jan XXXX) and c) the business purpose (e.g. checking how a door entry system was damaged).

11. **Subject Access Request (SAR)**

a) Under the UK GDPR/Data Protection Act (2018) anyone has the right to request from a data controller confirmation that personal data about them is being processed and for a copy of such data to be provided free of charge within one month of a valid request.

b) Where such a request is received that relates to a person who believes that their personal data has been captured on SCC surveillance camera data, then it must be recorded centrally using the formal SCC subject access request (SAR) process.

c) Any part of SCC and its suppliers could receive such a request in writing (e.g. via email, letter) or orally. Regardless of how the request came into SCC the SAR process must be followed.

i. The business unit, and dataset owner, of the surveillance cameras needs to be clear at the outset. There also needs to be confirmation that SCC is the data controller for the potential camera data that is requested. Where the camera data relates to another data controller then the requestor should be informed that SCC is not a data controller and that it should write to the correct party.

ii. The requestor should specify which SCC buildings/cameras, and on which dates it believes personal data was captured. SCC will provide help and advice, but open-ended requests could be deemed as manifestly unfounded or excessive under the terms of the UK GDPR/Data Protection Act (2018).

iii. Prior to preparing data it must be ascertained whether the surveillance camera does contain personal data. If the data is used primarily to detect and observe (but not to identify or recognise) and no person can be identified from the images, then the person making the subject access request should be informed accordingly.

iv. Where personal data has been identified in line with the SAR, then images should be copied and put into an easily readable format for use in SCC office environment. Third party data (i.e. images on persons and/or other personal data that relates to other people) must be redacted on the digital copy sent to the requestor using a method which cannot be reversed.

v. The data should be sent to the requestor using an encrypted removable media device.

vi. Other data subject rights include the rectification or deletion of data. Such requests will be dealt with using the central process above.

vii. Given the cyber and other security risks outlined above, data subjects are not permitted to view their own personal data from surveillance cameras on SCC premises.

12. **Law enforcement requests for camera surveillance data**

a) Where a request is made to SCC from a third party for copies of surveillance camera data, the dataset owner must be informed.

b) SCC will abide by any valid Court Order, which includes suspending destruction of specified data until it can be reviewed.

c) SCC will also assist a police officer where evidence is seized under Police and Criminal Evidence Act (1984) where there are reasonable grounds for

investigating an offence and that is necessary to avoid evidence being concealed, lost, tampered with or destroyed.

d) Additionally, SCC will consider requests from the Police or other law enforcement agencies where the request is deemed to be proportionate and in the public interest. SCC will require law enforcement agencies to comply with its procedures for releasing information in relation to any such requests. The written requests must be signed by an officer of the rank of Inspector or above in such cases.

e) Data can be reviewed by the Police at SCC premises, or if transferred to removable media it must be encrypted (whichever is most practicable).

13. **Other requests for data**

Other than SARs and law enforcement requests, SCC will not provide camera surveillance data to any other party (including staff) regardless of whether it is identifiable or non-identifiable data. Requests for images of vehicles in car-parks (in the event of damage etc.) cannot be processed. Staff should report suspected criminality to SCC front of house security teams and/or Police who will use the process outlined above if they believe it is necessary.

14. **Concerns & complaints**

Any member of staff or visitor to SCC buildings has the right to report a concern or complain about SCC usage of surveillance cameras inside or outside of buildings.

In the first instance this should be made to the Council's Corporate Property Officer who will provide a copy of this SCC Surveillance Camera Policy (2018) and consider whether it is being adhered to. If this does not deal with the query/complaint satisfactorily then the Senior Information Risk Owner (SIRO) will decide on any further action.