South Derbyshire District Council

Surveillance Policy

Author: Kevin Stackhouse

Service Area: Corporate Resources

Date: October 2018

Contents

Version Control

Version	Description of version	Effective Date
1.0	First Surveillance Policy	November 2018
1.1	Review, additional section on CCTV in the workplace, inclusion of Head of Service under responsibilities (Section 5) and revised surveillance inventory	June 2020

Approvals

Approved by	Date
H & CS Committee	22.11.2018
H&CS Committee	

Associated Documentation

Description of Documentation	
South Derbyshire District Council (SDDC) Policy and Procedure in Relation to Body Worn Video Cameras	(Ref 32SNW)
SDDC Environmental Health Data Retention Policy	
SDDC POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA	
SDDC Vehicle Location System Police (To be completed)	
Home Office Surveillance Camera Code of Practice 2013	
SDDC Regulation of Investigatory Powers Act Policy and Guidance	
SDDC ICT Security Policy	
Information Commissioner's CCTV Code of Practice	
SDDC Data Retention Policy	

1. Introduction and Scope

- This Policy sets out the necessary steps that should be taken to ensure South Derbyshire District Council's (the Council's) surveillance systems comply with the overarching legislation as referred to in paragraph 14 of this policy.

- It is one of several polices at the Council which are in place to inform and instruct officers (or customers) on expected behaviour and conduct and should be considered in conjunction with the policies referred to in paragraph 14.

- This Policy applies to all surveillance systems in use by the Council with the exception of Vehicle Location Systems and Noise Monitoring Machines; these are both governed by standalone policies and procedures. See paragraph 14.

- Surveillance systems – collectively refers to closed circuit television, mobile CCTV, motion activated cameras and body worn cameras.

- This Policy applies to the installation and operation of surveillance systems; access to and retention of recorded images; complaints, access requests and enquiries; deletion and disposal of recorded images.

- The Council's surveillance camera systems must operate in compliance with the 12 principles set out in the Home Office's Surveillance Camera Code of Practice.

- The Surveillance Camera Code of Practice states that surveillance camera use must have a clearly defined purpose, be in pursuit of a legitimate aim, and be necessary to address a pressing need.

  For the Council a legitimate aim is:

  - The Prevention of Disorder or Crime

  For information other statutory grounds are:

  - The Protection of Health or Morals
  - Public Safety
  - The Protection of the Rights and Freedoms of Others
  - National Security

2. Local Strategic Objectives

- For the Council's surveillance systems these are as follows:

  - To support delivery of the Council's vision and priorities by assisting in the prevention and detection of crime and anti-social behaviour; putting residents first.
  - To ensure that the Council's surveillance systems are operated in accordance with regulatory requirements in a transparent and cost efficient manner, taking account of appropriate technological developments.
  - To assist the Council, Derbyshire Police and other statutory and enforcement agencies in carrying out their regulatory, investigatory and enforcement duties within the District.
  - All services must record and report what surveillance systems are in place, their purpose, their form, who is trained to operate them and the justification for having surveillance systems in place to the Data Protection Officer before deploying a surveillance system. The Council will maintain a Surveillance Inventory (see Appendix 5).
  - Services must register any new, additional or replacement surveillance equipment and/or deployment within 30 days of introduction. This must be added to the Corporate Surveillance Inventory

3. Data Protection Impact Assessments

- After establishing a legitimate aim for seeking to use a surveillance system, services need to demonstrate that the objective is proportionate to the impact it has on prospective individual's privacy, both that of the subject of surveillance as well as those of third parties who may suffer unintended collateral intrusion, by completing a Data Protection Impact Assessment (DPIA).

- The purpose of the DPIA is to ensure compliance with privacy legislation and the Surveillance Camera Code of Practice Principle 2; i.e. the use of a surveillance camera system must consider its effect on individuals and that any privacy risks are acknowledged and minimised.

- A data protection impact assessment (DPIA) should be completed before any surveillance camera system is installed, whenever a new technology or functionality is being added on to an existing system, or whenever there are plans to process more sensitive data or capture images from a different location. This will assist in assessing and mitigating any privacy issues linked to the use of a

surveillance system

- Surveillance systems should not exceed the defined purpose; consideration should be afforded as to whether it is necessary to capture imagery beyond the boundaries of a defined area.

- You **must** carry out a DPIA for any processing of surveillance camera data that is likely to result in a high risk to individual privacy. The GDPR states that a DPIA "shall in particular be required in the case of ''systematic monitoring of publicly accessible places on a large scale" (Article 35).

- As a controller in relation to the processing of personal data, you must seek the advice of a designated Data Protection Officer when carrying out a DPIA.

- The Surveillance Camera Commissioner has produced a Data Protection Impact Assessment template which should be used when completing a DPI. This form can be found on the Council Intranet page and via the Surveillance Commissioner Website:https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras.

4. Surveillance Systems

- The locations of and number of surveillance systems should be recorded and proportionately measured against the recorded purpose and DPIA.

- The use of audio recording, including recording incoming phone calls, and visual recording needs to be justifiable; it will not typically be enabled and agreement to use it must be obtained from the Data Protection Officer.

- Viewing of live or recorded imagery should be restricted to the systems designated operator(s) and the Surveillance Administrator, although there may be occasions where other authorised person(s) are required to view footage as a matter of necessity. Please refer to paragraph 9 - 'Requests to Access Footage'.

- Recorded data must be stored securely and effectively to maintain confidentiality and integrity of the recorded data.

- Disks and memory sticks or any other data storage devices must be encrypted as an effective means to prevent unauthorised access. Please refer to the Council's ICT Security Policy for additional information regarding device security.

- Retention of recorded imagery and related data should reflect the purpose for which the information was recorded; this should be tailored in accordance with stated aim. It will vary due to the purpose of the system and how long the information needs to

be retained so as to serve its intended purpose. Retention times are stated within the Corporate Data Retention Policy or local departmental Data Retention Schedules. For CCTV and body camera footage this should not exceed a 30-day period; should this period need to be extended beyond 30 days, the Data Protection Officer must consent to this extension taking into account the reason for the extension request, for example, it is evidence in an insurance or criminal investigation.

- Where the recorded imagery and related data is required for formal employment matters the retention and destruction of any data will be dictated by the relevant employment procedure.

- A Surveillance Administrator may need to retain images for a longer period, for example where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.

- Systems which make use of wireless communication links (e.g. transmitting images between cameras and a receiver) should ensure that these signals are encrypted to prevent interception.

- Systems which can transmit images over the internet (e.g. to allow viewing from a remote location) should ensure that these signals are encrypted to prevent interception and also require some form of authentication for access (e.g. a username and secure password).

- Where encryption is not appropriate, e.g. if it may have an effect on the information being processed, then other appropriate methods should be employed to ensure the safety and security of information.

5. Responsibilities

Chief Executive

- The Acts referenced in paragraph 14 place a statutory duty upon the Council, as a public authority and a data controller.
- The Chief Executive is responsible for ensuring that the Corporate Surveillance Inventory includes detail of all applicable surveillance assets within that service and for confirming the Asset Owner and Surveillance Administrator responsible for each asset. The Corporate Surveillance Inventory can be found under Appendix 5.

Data Protection Officer

NB for the purposes of the policy reference to information, refers to imagery, footage and any other data collected via surveillance systems.

The Data Protection Officer is the individual designated as responsible for statuary compliance and advice to the organisation on Data Protection legislation. Responsibilities include:

- Understanding the Council's obligations for managing personal and sensitive information.
- Understanding and monitoring how information assets are held, and for what purpose.
- Understanding and monitoring how information is created, amended, added to and deleted over time.
- Understanding and monitoring who has access to the information and why.
- Understanding and monitoring how and why information is shared with external parties and ensuring that this process is properly documented and controlled.
- Understanding and monitoring how information assets are handled and managed and for ensuring that documented processes are in place for this to be done appropriately.
- Ensuring that policies and procedures are followed.
- Responding to and managing information security incidents and any other Information Governance (IG) issues.
- Confirming acceptance and executing their responsibilities via self-certification IG audits (See Appendix 3)

Heads of Service

Heads of Service are responsible for ensuing compliance with this Policy at all times when surveillance systems are used for any services provided directly, or in partnership with other bodies working on behalf of the Council which includes but is not limited to:

- Maintaining accurate records and reviewing any assets used
- Ensuring Data Retention Schedules are observed, and images securely destroyed
- Ensuring the adequate and appropriate level of training for employees in the exercising of their roles
- Supporting the Chief Executive with developing and reviewing the Policy and its provisions,

Surveillance Administrator

A Surveillance Administrator has operational responsibility for the surveillance asset; this includes but is not limited to:

- Ensuring the system is maintained.
- Ensuring technical and organisational security of the asset.

- Having responsibility for the scheme; checking footage; downloading footage; arranging appointments, and supervising viewing.
- Ensuring day-to-day compliance with the requirements of this Surveillance Policy and the Home Office Surveillance Code of Practice.
- Carrying out annual reviews of whether the use of the surveillance systems continues to be justified.
- Conducting and reviewing DPIAs.
- Ensuring the Data Protection Officer is informed of all designated operators.

6. Body Worn Cameras

This section focuses on body worn cameras and should be followed in conjunction with the entirety of this policy.

- Clothing should explicitly and prominently identify that body worn cameras are in use; the camera itself should be clearly visible.

- Body worn cameras must only be in use whilst employees are acting in their official capacity. Usage should not continue in breaks at work or free time.

- If there is a specified and legitimate purpose for body worn cameras to be used covertly, then the Regulation of Investigatory Powers Act Policy must be followed; there are very limited occasions where such usage will be justified.

- All information should be stored securely and be accurate.

7. Signs

- The public must be alerted that a surveillance system is in operation; this should be done through the use of clear prominent signs at the entrance of the surveillance zones and also enforced with signs inside the area (See Appendix 1).

- Signs should:

    - Be clearly visible, readable and maintained.
    - Contain contact details of the Surveillance Administrator or Data Protection Officer.
    - Identify the purpose for using the surveillance system.
    - Be an appropriate size depending on context; for example, whether they are to be viewed by pedestrians or road users.

- Appropriate signs must be provided to alert road users to the use of cameras on the road network or in areas that vehicles have access to, such as car parks.

8. Maintenance

- A confidentiality agreement should be in place for any external contractors carrying out maintenance on, or who manage, operational surveillance systems.

- The confidentiality agreement must restrict access to recorded images, and the use of them, to specified permitted purposes. They must specify that purpose or purposes. Consideration should be given to how long the confidentiality should last for, including where appropriate beyond the contracted period. Access to surveillance systems must not be granted prior to a confidentiality agreement being signed. Signatories to the agreement must have the authority to legally bind the contractor. Please contact the Data Protection Officer for further advice.

- All maintenance must be logged; Surveillance Administrators must keep their own records.

- Procurement advice should be sought by a Surveillance Administrator prior to specification and purchase of new surveillance equipment including software, to ensure that the equipment is both sufficient and technically fit for the required purpose. All surveillance equipment should be compliant with British Standard Institution (BSI) current standards detailed in the BSI codes of practice.

- The Communities Team Manager, relevant Head of Service and Data Protection Officer should also be informed of any new surveillance equipment in order for it to be logged on the Council's surveillance inventory.

9. Requests to Access Footage

- A Surveillance Administrator must ensure that requests are assessed before any personal information is given and all disclosures must be logged with the Data Protection Officer. Guidance can be found at Appendix 2. Further guidance can be sought from the Strategic Director (Corporate Resources).

- Where the requestor is also the data subject, the subject access request procedure will be followed.

  - Requests by the Police (pursuant to section 29 of the Data Protection Act 2018) must be approved by the Surveillance Administrator and logged with the Data Protection Officer. Requesting Officers will need to supply Derbyshire Police's prescribed 807 personal data request form. The Surveillance Administrator will be supplied with a copy and this should be logged and signed for (By the requesting

Officer); by signing they agree to be responsible for its retention and disposal.

- All access requests must be recorded by the Surveillance Administrator. Details of the requestor, data subject, nature of the request and the legislation which the request is being made under will need to be provided promptly, so that the Data Protection Officer can validate the request.
- Leadership Team and Heads of Service may request footage to investigate an incident that has occurred e.g. as part of an employment process (if a crime has been committed or public safety affected by a member of staff), abuse of a member of staff, vandalism, damage, anti-social behaviour, hate crime or other in related situations. Each request will be assessed on a case-by-case basis and advice should be sought from the Data Protection Officer, Legal Services and HR. Where footage is shared for any of these reasons, the original must always be retained.
- Copies may be made available for employees to see and respond to, as part of an ongoing employment investigation, where necessary. Where this applies the service should maintain a record of what has been shared, how many copies were provided and to whom, and in what format.
- Footage should only be accessed where there is an allegation or /a report received of wrongdoing and not used as a tool to actively seek out wrongdoing
- Recorded material or live footage must not be released to print, broadcast or online media outlets for commercial or entertainment purposes.
- Footage may be requested under the Freedom of Information Act 2000 or the Data Protection Act 2018; such requests should be referred to the Data Protection Officer for approval.
- The Council will ensure only subjects of the surveillance can be obtained and others' privacy rights can be protected by having their images obliterated by pixelating their images.
- Footage will be processed in accordance with the eight data protection principles of the Data Protection Act 2018; images should be pixelated where appropriate.
- In responding to subject access requests or other disclosures, officers should consider an appropriate format of the data to be disclosed, and appropriate security controls. Before releasing any data, advice and instruction must be provided by the Data Protection Officer and legal services. During procurement, the capability of the device or prospective system to export data securely to third parties should also be considered.

10. CCTV in the workplace

- The Council may wish to use surveillance equipment in the workplace for various reasons, the Data Protection Act does not prevent employers from monitoring the work place or its workers, but it recognises that employees are entitled to some privacy at work.
- The Council will ensure all monitoring is proportionate, justifiable, and not too intrusive.
- The Council will inform employees in advance about any monitoring taking place inside the workplace and the reason for it.
- Employees will be given the opportunity to make their views on this known. Any new members of staff should have it explained to them in their induction.
- If Surveillance equipment is installed within the workplace, signs will be displayed near to the cameras to inform staff and visitors that there are cameras monitoring, its purpose and the details of the Surveillance Administrator.
- The information gathered through monitoring should only be used for the aim it was intended for and other circumstances as detailed in this Policy under Section 1.
- Employees have the right to ask which data is held on them, why it is collected and processed.
- Any changes to the use, replacement or installation of new monitoring equipment will be communicated to employees in advance.

11. Requests for Surveillance to be Set-up

- Law enforcement agencies may request that covert surveillance is set up for a specified purpose; such requests should be dealt with under the Council's Regulation of Investigatory Powers Act Policy.
- Any over deployment requests will need to be approved by the Strategic Director (Corporate Resources). Such deployments will need to be compliant with the entirety of this Policy.
- The Council's Regulation of Investigatory Powers Act (RIPA) Policy will cover any occasions where the Council would consider carrying out any covert surveillance.

12. Surveillance Evidence from Third Parties

The Council is regularly provided with surveillance evidence from third parties to

assist with investigations. It is the duty of the Investigating Officer to establish whether the evidence was obtained in accordance with the Data Protection Act if it was obtained from a public body (e.g. a Parish Council).

If a third party offers surveillance evidence that is required for a Council investigation, the investigating officer should acquire the evidence by downloading onto a Council owned storage device. The footage should be stored securely and should only be retained for the duration of the investigation. Once the investigation is complete the footage should be deleted or disposed of accordingly (see section 13).

13. Disposal of Confidential Waste

- Storage devices such as disks and memory sticks may be recycled where possible; secure data destruction must occur before devices are reused.

- Where storage devices cannot be reused, these devices need to be disposed of as confidential waste. Disposal must comply with the Council's disposal process, as detailed in the Council's ICT Security Policy. This requires secure destruction of all data to the standard prescribed by government legislation. Secure data destruction should occur in advance of devices being processed as waste and before being transported for disposal.

- It is essential for such devices to be treated securely and all staff need to maintain confidentiality up until the point of disposal. A record of any devices destroyed should be kept by the Surveillance Adminstrator.

14. Complaints

- Complaints should be promptly referred to the Data Protection Officer via DataprotectionOfficer@southderbyshire.gov.uk

- Where it is alleged that a data protection breach has occurred, the Data Protection Officer must be notified within 24 hours.

- The Data Protection Officer will respond in writing to any complaints within 20 working days.

- Further information can be found in the Council's Data Protection Policy.

15. Relevant Policies, Standards and Procedures

- Information Security Policy
- Data Protection Policy
- Council Data Retention Policies
- Regulation of Investigatory Powers Act (RIPA) Policy
- BSI British Standard - Closed Circuit Television - Management and Operation - Code of Practice. BS EN 7958:2009
- Crime and Disorder Act 1998
- Criminal Justice and Public Order Act 1994
- Criminal Procedures and Investigations Act 1996
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998 - Article 8 - The right to respect for private and family life, home and correspondence - infringement/invasion of privacy
- Information Commissioners Data Protection Code of Practice for Surveillance Cameras and Personal Information 2015
- Private Security Industry Act 2001
- Protection from Harassment Act 1997 - Offence of Harassment
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Surveillance Camera Commissioners Code of Practice for Surveillance Camera Systems 2013
- Data Protection Act 2018

16. Reviews

- In order to comply with the Surveillance Camera Code of Practice, the Data Protection Officer will conduct reviews of compliance with this policy across the Council.

- This policy will be reviewed bi-annually.

17. Compliance

- The Strategic Director (Corporate Resources) is responsible for monitoring compliance with this policy.

- If employees do not comply with Council policies, procedures or guidelines, the Council may take appropriate action in accordance with its employment procedures.

18. Contact Details

- Please contact the Council's Data Protection Officer with enquiries about this or any other referenced policy, procedure or law.

  Email to: DataprotectionOfficer@southderbyshire.gov.uk
  Telephone: 01283 595712

Appendix 1: Standard Signage for use with CCTV Systems

It is a legal requirement to notify the Information Commissioner's Office usage of Surveillance systems.

Signs **must** be displayed so that visitors, members of the public and employees are aware that they are entering a zone which is covered by surveillance equipment.

Signs must be clearly visible and legible. Size will vary according to circumstances:

- Signs displayed in a public area, for example a reception area, need only be **A4** if displayed at eye level.

- Signs displayed in a car park will need to be at least **A3** as they are likely to be viewed from further away, for example by a driver sitting in a car.

Signs must state and display:

- That the Council is responsible for the scheme
- The purpose of the scheme
- The details of whom to contact regarding the scheme.

Signs must be inspected on an annual basis to makes sure they remain visible and not obstructed in any way. There placement and any fixtures should also be included in the review with any maintenance/repair work carried out immediately where possible.

Template sign

Images are being recorded for the purpose of crime prevention and public safety.

This scheme is controlled by South Derbyshire District Council.

For more information please contact via email: dataprotectionofficer@southderbyshire.gov.uk

Appendix 2: Guidance on Key CCTV Statutory Provisions

S.7 Data Protection Act 1998 (Subject Access Requests)

Requests for CCTV can be made under section 7 of the Data Protection Act as a subject access request. Requests are commonly made under section 7 by individuals who wish to request their personal information or by those acting on their behalf with their consent. These requests can be validated with:

- The required proof of identity.
- Proof of vehicle ownership (if applicable).
- £10 fee.

However, as section 7 only entitles people to access their personal data, any other individuals/vehicles need to be pixelated.

If a solicitors or insurers is acting on the data subject's behalf, it is reasonable to take it in good faith that they have taken the appropriate due diligence checks in verifying their client's proof of identity and proof of vehicle ownership (if applicable). However, you will require the appropriate signed explicit consent from their client to enable you to release their personal information to them as a third party.

Section 29 Data Protection Act

Requests for CCTV can be made under section 29 of the Data Protection Act, for example if the request is in relation to the prevention and detection of crime. These requests are often submitted by Derbyshire Constabulary using their 807 form for personal data requests.

The 807 forms must be appropriately signed and completed, to give detail such as:

- To whom the personal data request relates.
- The purpose of the investigation.
- Details required to identify the footage.
- The purpose of requesting the footage (the legal justification to release the information).

When approving a request you should consider whether the disclosure is proportionate to the purpose of the investigation. You are entitled to ask the Police to refine their requests if you feel it is disproportionate.

Section 35 Data Protection Act

Requests for CCTV under section 35 of the Data Protection Act allows information to be disclosed if it is required by law or made in connection with legal proceedings. Requests can be identified as being under section 35 if the requestor indicates in their request that the request is being made specifically under section 35 or if the request is in connection with legal proceedings. If it is not clear what section of the Data Protection Act the request is being made under, then the requestor can clarify this.

If somebody is requesting footage in connection with legal proceedings they must verify that this is the case. It is reasonable to take it in good faith that solicitors and insurers have taken the appropriate due diligence checks in verifying their client's proof of identity and proof of vehicle ownership, although you will require the appropriate signed explicit consent from their client to enable you to release their personal information to them as a third party. This document is usually referenced as a 'form of authority.'

General Data Protection Regulation

The General Data Protection Regulation (EU) 2016/679 (GDPR) regulates the processing of personal data where the processing is carried out for non-Law Enforcement purposes.

<u>Disclosure for preventing and detecting crime or the apprehension or prosecution of offenders</u>

The UK Parliament used the Data Protection Action 2018 to set out certain exemptions from the GDPR which can be applied in some circumstances. They mean that some of the data protection principles and data subject rights within the GDPR need not be applied or can be restricted when personal data is used or disclosed for particular purposes in the public interest.

Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 (Crime & taxation: general) provides an exemption that can be applied to enable the disclosure of personal data by an organisation whose processing is subject to the GDPR, to the Police for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.

It permits the restriction or non-application of the GDPR data protection principles and data subject rights (as listed in the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 1) to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

In effect the exemption means that an organisation can provide personal data to the Police where it is necessary for the prevention or detection of crime or the apprehension

or prosecution of offenders without fear of breaching the GDPR or the Data Protection Act 2018.

Disclosure to protect the vital interest of individuals.

Article 6(1)(d) of the GDPR provides a lawful basis for organisations to disclose personal data to the Police where the disclosure is necessary in order to protect the vital interests of the data subject or of another natural person

Appendix 3: Surveillance Self-Certification Audit

Summary

This self-certification audit is designed to ensure Surveillance Administrators identify and accept their responsibilities in relation to any surveillance system that they operate.

This toolkit is based on the statutory requirements imposed by: Information Security Policy; Data Protection Policy – in process; Regulation of Investigatory Powers Act (RIPA) Policy; BSI British Standard - Closed Circuit Television - Management and Operation - Code of Practice. BS EN 7958:2009; Crime and Disorder Act 1998; Criminal Justice and Public Order Act 1994; Criminal Procedures and Investigations Act 1996; Data Protection Act 1998; Freedom of Information Act 2000; Human Rights Act 1998 - Article 8 - The right to respect for private and family life, home and correspondence - infringement/invasion of privacy; Information Commissioners Data Protection Code of Practice for Surveillance Cameras and Personal Information 2015; Private Security Industry Act 2001; Protection from Harassment Act 1997 - Offence of Harassment; Protection of Freedoms Act 2013; Regulation of Investigatory Powers Act 2000; Surveillance Camera Commissioners Code of Practice for Surveillance Camera Systems 2013; Data Protection Act 2018.

Name of surveillance system covered by this statement :
……..

Corporate reference number if known: :
……..

Full system inventory (*insert an embedded document)* :

Compliance Statement

I confirm that:

1. The surveillance is in place to address the pressing need of prevention of disorder or crime.
2. Annual reviews are carried out in accordance with the Council's Surveillance Policy to ensure continuing use remains justified. The review includes completion of a privacy impact assessment.
3. I am aware of their corporate and statutory responsibilities.
4. Appropriate technical, organisational and physical standards are adhered to.
5. Access is restricted to where there is justifiable necessity in accordance with the data protection legislation.
6. Relevant signage is in place, inspected and maintained.
7. Agreements with information processors or contractors for maintenance are compliant with the relevant legislation. Agreements restrict access to recorded images, and the use of them, to specified permitted purposes.
8. Requests to access personal data (other than Police requests) are sent to the Data Protection Officer via dataprotectionofficer@southderbyshire.gov.uk in a timely manner.
9. Requests for new cameras to be deployed are sent to the Data Protection Officer via dataprotectionofficer@southderbyshire.gov.uk in a timely manner.
10. I do not deploy or approve any covert surveillance without following the process outlined in the Council's RIPA policy.
11. Retention of surveillance material does not routinely exceed 30 calendar days.
12. Destruction or disposal of devices or information is carried out in a secure manner.
13. Surveillance complaints are promptly referred to the Data Protection Officer via email to dataprotectionofficer@southderbyshire.gov.uk

Surveillance Administrator Self Certification

I confirm that I am aware of my responsibilities as a Surveillance Administrator in conjunction with this Surveillance Policy and the relevant statutory provisions listed in Section 15

Signed……..

Name…….

Directorate……

Date……..……

Appendix 4 Police Form 807 Personal Data Request Form

OFFICIAL SENSITIVE (WHEN COMPLETE)

Form 807
R5/18

Request to external organisation for the disclosure of personal data to the Police

Under Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 and GDPR Article 6(1)(d)

To:

Position (where known):

Organisation: South Derbyshire District Council

Address: Civic Way, Swadlincote

I am making enquiries which are concerned with:

- ☒ The prevention or detection of crime*
- ☒ The prosecution or apprehension of offenders*
- ☐ Protecting the vital interests of a person*

☒ I confirm that the personal data requested below is needed for the purposes indicated above and a failure to provide that information will be likely to prejudice those matters. *

☒ I confirm that the individual(s) whose personal data is sought should not be informed of this request as to do so would be likely to prejudice the matters described above. *

*Check mark as is appropriate

Information required:

Police Reference:

Version 2.0 29th May 2018

OFFICIAL SENSITIVE (WHEN COMPLETE)

Form 807
R5/18

From:

Rank/Number/Name:

Station:

Date/Time:

Telephone Number(s):

Email address:

Signature*:

Counter Signature:*

Rank/Number/Name:

**as required by recipient, please see Completion Guidance below*

If your organisation receives a request for a copy of this document or this information, (e.g. under the Data Protection Act, EU General Data Protection Regulation or the Freedom of Information Act), please contact the Force Data Protection Officer at Derbyshire Constabulary Headquarters, Butterley Hall, Ripley, Derbyshire DE5 3RS. Telephone number 101.

Completion Guidance

Police officers or staff completing this form should type and tab between the fields on the form. The information required field should provide the recipient with sufficient information to allow them to locate the information sought. Where a signature and/or counter signature are required the form will need to be printed off and signed manually. Some organisations may require a counter signature to be added to the form. Normally this should be the supervisor or line manager of the person completing the form, but may be a higher rank if reasonably required by the recipient.

Further guidance on the use of this form may be obtained from the Force Data Protection Officer.

Guidance Notes

This form is used by the police when making a formal request to other organisations for personal data where disclosure is necessary for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, or to protect the vital interests of individuals.

The General Data Protection Regulation (EU) 2016/679 (GDPR) regulates the processing of personal data where the processing is carried out for non-Law Enforcement purposes.

<u>Disclosure for preventing and detecting crime or the apprehension or prosecution of offenders.</u>

The U.K. Parliament used the Data Protection Act 2018 to set out certain exemptions from the GDPR which can be applied in some circumstances. They mean that some of the data protection principles and data subject rights within the GDPR need not be applied or can be restricted when personal data is used or disclosed for particular purposes in the public interest.

Version 2.0 29th May 2018

Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 (Crime & taxation: general) provides an exemption that can be applied to enable the disclosure of personal data by an organisation whose processing is subject to the GDPR, to the police for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.

It permits the restriction or non-application of the GDPR data protection principles and data subject rights (as listed in the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 1) to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

In effect the exemption means that an organisation can provide personal data to the police where it is necessary for the prevention or detection of crime or the apprehension or prosecution of offenders without fear of breaching the GDPR or the Data Protection Act 2018.

It is acknowledged that the exemption places no compulsion on the recipient to disclose the requested personal data, but it should provide reassurance that a disclosure for these purposes can be made in compliance with the GDPR and the Data Protection Act 2018.

Disclosure to protect the vital interests of individuals.

Article 6(1)(d) of the GDPR provides a lawful basis for organisations to disclose personal data to the police where the disclosure is necessary in order to protect the vital interests of the data subject or of another natural person.

Appendix 5: South Derbyshire District Council Surveillance Inventory

Number	Type of Surveilance	Location/Area Surveillance covers	Asset Owner	Surveillance Administrator	Details of those trained to operate the system(s)	Footage is Recorded	Active Monitoring	Details of Active Monitoring	Operational Issues	Retention Period Does not exceed 30 Days
1	Fixed CCTV Cameras in Swadlincote Town Centre	13x Cameras at 6 locations covering Swadlincote Town centre	Communities Manager	Communities Assistant	Communities Manager & Communities Assistant	Yes	No	None		Yes
2	Fixed SDDC Offices CCTV Cameras (External)	4 Cameras cover the outside of the Council building including the public car parks	Communities Manager	Communities Assistant	Communities Manager & Communities Assistant	Yes	No	None		Yes
3	Fuxed CCTV in Midway Community Centre	6 Cameras on building covering surrounding area	Cultural Services Manager	Cultural Services Officer	Cultural Services Officer & Midway Community Centre Assistant	Yes	No	None		Yes
4	Fixed Rosliston Forrestry Centre CCTV Cameras	Cameras cover area around the buildings at Rosliston Forrestry Centre	Cultural Services Manager	Rosliston Manager	Duty Manager and Maintenance Manager	Yes	No	None		Yes
5	CCTV Located in Refuse Lorries	Whole District whilst on collections	Head of Operational Services	Head of Operational Services	Head of Operational Services	Yes	No	None		Yes
6	Fixed Depot CCTV Cameras	Cameras cover Outside of the Depot building	Head of Corporate Property	Head of Operational Services	IT Service Assistant	Yes	No	None		Yes
7	Tracking Devices in refuse lorries	Used to record daily routes, speed, mileage, fuel use, weights etc	Head of Operational Services	Waste and Transport Manager	Waste and Transport Manager, Waste and Transport Supervisor, Waste and Transport Officer	Yes	No	None		Yes
8	Body Warn Cameras	Whole District whilst patrolling	Environmental Health Manager	Senior Neighbourhood Warden	3 x Community Safety Enforcement Officers & 1x Park Warden	Yes	No	None		Yes
9	Redeployable Flytipping Cameras	Whole District covering Flytipping hotspot sites	Environmental Health Manager	Senior Neighbourhood Warden	4 x Community Safety Enforcement Officers	Yes	No	None		Yes
10	Redeployable Noise Monitoring Equipment	Used across the whole district to investigate noise complaints	Environmental Health Manager	Pollution Control Officer	3 x Environmental Health Officers	Yes	No	None		Yes
11	Fixed CCTV in Alexander Road Flats	Cameras cover the inside and directly outside of the flats	Improvement & Repairs Team Leader	Project Officer Housing Services	Project Officer Housing Services	Yes	No	None		Yes
12	Fixed SDDC Offices Cameras (Internal)	10 x Cameras located inside the main Council offices	Improvement & Repairs Team Leader	Project Officer Housing Services	Project Officer Housing Services	Yes	No	None		Yes
13	System Covering IT Surver room	4x static cameras inside Server room	ICT Operations Manager	ICT Manager	IT Officers	Yes	No	None		Yes