South Derbyshire District Council

Surveillance Policy

Version Control

Version	Reason for review (review date/legislation/process chances)	Effective Date	Review date
1.0	First Surveillance Policy	November 2018	Nov 2021
1.1	Scheduled review, additional section on CCTV in the workplace, inclusion of Head of Service under responsibilities and revised Surveillance Inventory	June 2020	June 2023
1.2	Scheduled 3-year review	November 2023	Nov 2026

Approvals

Approved by (Committee/Leadership Team)	Date
H&CS Committee	22.11.2018
H&CS Committee	07.07.2020
H&CS Committee	01.02.2023

1.0 Content

Contents

2.0 Introduction

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.

A surveillance system is a broad term for the linked equipment used for capturing, recording and viewing images for overt surveillance purposes.

This Policy applies to all overt 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. The Council cannot undertake covert surveillance without a RIPA authorisation and only in circumstances that are allowed by Statute. The Council has its own RIPA Policy which details when and how covert surveillance can be undertaken.

Surveillance systems collectively refers to closed circuit television, mobile CCTV, motion activated cameras, body worn cameras and other devices used for overt surveillance purposes. Systems covered by this policy include those situated in public locations and those covering Council buildings, both internal and external.

3.0 Purpose

This policy outlines the use of CCTV surveillance by the Council to enhance public safety, protect council buildings, assets, staff, elected members and visitors and support law enforcement activities while respecting individual privacy and civil liberties.

The overarching purpose of this Policy is to enable operators of surveillance camera systems to make legitimate use of available technology in a way that the public would rightly expect and to a standard that maintains public trust and confidence.

The Council fully recognises that the use of overt surveillance systems needs to comply with a legal framework notably the General Data Protection Regulation (GDPR) and Data Protection Act 2018, and Article 8 of the European Convention on Human Rights (the right to respect for private and family life). The Council has established lawful bases under data protection legislation for the processing of personal data for these purposes.

The use of established surveillance cameras shall be accordance with the purposes specified under this Policy.

The Policy covers the use of surveillance camera systems and processing of images and information obtained from those systems. The Policy takes on board guidance provided in the Surveillance Commissioner's, Surveillance Camera Code of Practice 2013 (Amended Nov 2021) https://www.gov.uk/government/publications/update-to-surveillance-camera-code

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.

The Council uses CCTV on and within its buildings to:

- Protect staff, Elected Members, visitors and customers
- Protect its premises and other assets

The Council uses CCTV in Public Places such as Swadlincote Town Centre to:

- Prevent Crime or Disorder

And to fulfil other statutory grounds including:

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

The Council designates officers to use body worn video (BWV) cameras to:

- Protect staff and residents

- Protect premises and other assets
- Collate evidence for enforcement action, including tenancy management, premises inspections, prosecution and to support the issuing of fixed penalty notices
- Increase personal safety and reduce the fear of crime
- Deter and reduce incidents of violence and aggression to staff members
- Support the Police in reducing and detecting crime
- Assist in identifying, apprehending and prosecuting offenders
- Provide a deterrent effect and reduce criminal and antisocial behaviour

The Council also authorises the use of deployable cameras to:

- Collate evidence for enforcement action and to support the issuing of fixed penalty notices
- Assist in identifying, apprehending and prosecuting offenders
- Provide a deterrent effect and reduce criminal and antisocial behaviour

The Home Office Surveillance Camera Code of Practice states Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

This Policy does not apply to covert surveillance for investigation purposes which must only be carried out in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA) and the Council's RIPA Policy.

4.0 Objectives

- To support the prevention and detection of crime and anti-social behaviour and enhancing public safety.
- To ensure that the Council's surveillance systems are operated in accordance with regulatory requirements in a transparent 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.

5.0 Performance and Monitoring

5.1 Guidance on Effective use of Surveillance Systems

The Surveillance Camera Code of Practice (the Code) was issued in 2013 following the introduction of the Protection of Freedoms Act 2012 and most recently updated in 2021. The Code provides guidance on the appropriate and effective use of surveillance camera systems.

The Council is a relevant authority as defined by section 33 of the Protection of Freedoms Act and therefore it must have regard to the Code.

The Code applies to the use of surveillance camera systems that operate in public places, regardless of whether or not there is any live viewing or recording of images or information or associated data.

The Code provides **12 guiding principles** which the Council has adopted. These are:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

5.2 Data Protection Impact Assessment

Any proposal for the use of surveillance cameras or systems or for existing surveillance cameras or systems to be used for a new purpose will require a Data Protection Impact Assessment (DPIA) before the procurement and implementation stages. This will enable the impact on privacy to be assessed and for any appropriate safeguards to be put in place. It will also assess the necessity of the inference and extent of any interference with Article 8 rights (Human Rights Act – respect for private and family life).

The Council notes the need to consult with the Regulator (Information Commissioner's Office – ICO), when after conducting a DPIA a high risk to the rights and freedoms of individuals remains. Under these circumstances the Council will not proceed with the commissioning of the surveillance cameras or systems until this consultation has taken place. Where the Council can take steps to reduce the risk it will act on those steps to a point where there is no requirement to consult with the ICO.

The Council will also consider whether consultation with those most likely to be affected is required before any decision is taken if proposing an extension to the purposes for which a surveillance system was established or considering a new surveillance system Data Protection Impact Assessment and record its decision making and consultation results.

5.3 Privacy

The right to respect for private and family life is set out in Article 8 of the European Convention on Human Rights. The use of any form of surveillance may impact on an individual's privacy and rights under the Human Rights Act and data protection legislation (General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018).

BWV cameras are likely to be more intrusive than CCTV and deployable surveillance systems because of its mobility. BWV cameras have the ability to be switched on or off. The Council recognises that continuous recording will require strong justification as it is likely to be excessive and cause a great deal of collateral intrusion.

The Council notes the Code's statements on a surveillance camera system use on recording conversations between members of the public as highly intrusive and notes that strong justification of necessity is required to establish its proportionality.

With regards to CCTV and deployable camera installations, the Council will consider the right of the general public to go about their daily business with minimum loss of privacy. Whilst total privacy cannot be guaranteed within a CCTV area, the cameras and their recordings will not be used to unduly monitor persons going about their lawful business. Where appropriate, cameras will be configured with 'privacy screening'.

5.4 Transparency

People in public places should normally be made aware whenever they are being monitored by a surveillance camera system, who is undertaking the activity and the purpose for which that information is to be used. This is an integral part of overt surveillance and a legal obligation under data protection legislation.

The Council will publish information on its website, the surveillance camera systems that they use, the areas in which they are installed, how to make requests for images and how to make a complaint about the use of surveillance camera systems. The Council will use its corporate complaints policies and procedures for this purpose.

Any new, additional or replacement surveillance equipment will be logged by the Council on its Corporate Surveillance Inventory and be published.

Appendix 1 details the type and location of the Council's Surveillance Camera systems as at the date of this Policy.

Signage will be displayed informing individuals that CCTV or a deployed camera is in operation. This information will include the purpose for the installation and a contact number for enquiries.

BWV cameras will be worn on the users uniform or clothing in a prominent and overt position and will show that it is a recording device (the recording screen faces outwards).

5.5 Retention

The Council will keep images and information obtained from a surveillance camera system for no longer than necessary to fulfil the purpose for which they were obtained in the first place. This period will be decided in advance, be the minimum period necessary and documented in supporting operational procedures. The retention period for different surveillance camera systems will vary due to the purpose for the system and how long images and other information need to be retained so as to serve its intended purpose.

On occasions the Council 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.

The Council will ensure that all recorded data is stored securely and so that recordings relating to a specific individual or event can be easily identified, located and retrieved.

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.

5.5 Data Security and Protection

Viewing and downloading of live or recorded imagery will normally be restricted to the

Surveillance Administrators (System Managers) and System Users, there may be occasions where other authorised person(s) are required to view footage as a matter of necessity ie other Council colleagues involved in investigations or the Police. Permission should be sought from System Managers prior to this.

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.

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.

5.6 CCTV in the Workplace

The Council may wish to use surveillance equipment in Council buildings for various reasons, the Data Protection Act does not prevent employers from monitoring the workplace or its workers, but it recognises that employees are entitled to some privacy at work.

The Council will inform employees in advance about any monitoring taking place inside council buildings and the reason for it. The Council will ensure all monitoring is proportionate, justifiable, and not too intrusive. 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 any monitoring is taking place.

If surveillance equipment is installed within the Council building, signs will be displayed near to the cameras to inform staff and visitors that there are cameras monitoring, and its purpose.

The information gathered through monitoring should only be used for the aim it was intended for and other circumstances as detailed in this Policy.

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.

5.7 Data Usage and Sharing

CCTV data may be used for law enforcement investigations, evidence in legal proceedings, or council operations. Sharing of data with external agencies, when necessary, will be done in accordance with legal requirements.

The Council has discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once the Council has disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image.

Requests by the Police (pursuant to section 29 of the Data Protection Act 2018) must be approved by the Surveillance Administrator (system manager) and logged accordingly. Requesting Police Officers will need to supply Derbyshire Police prescribed 807 personal data request form.

There may be other limited occasions when disclosure of images to another third party, such as a person whose property has been damaged, may be appropriate. The Council will consider such requests with care and in accordance with data protection legislation.

5.8 Application by Individual Data Subjects

Individuals can request images and information about themselves through a subject access request under GDPR. The Council has a centralised team which handles requests. Any enquiries should be directed to dataprotectionofficer@southderbyshire.gov.uk

The Council's data request form (which includes making subject access requests) can be found on the Council website: https://www.southderbyshire.gov.uk/about-us/data-privacy-and-cookies/data-protection-act-2018

The disclosure of images to data subjects is done securely to ensure that they are only seen by the intended recipient. Consideration is also given to whether images of other individuals need to be obscured to prevent unwarranted identification.

5.9 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 through overt of covert means and in accordance with the law.

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

5.10 Use of Surveillance Data to Identify Offenders

It is permitted for regulatory purposes to publish images of persons of interest on media platforms, however the Council will take care when wording any such requests to ensure that no personal data is disclosed and that there is no inference of guilt.

5.11 Complaints

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

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.

5.12 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.

5.13 Contact Details

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

Email: DataprotectionOfficer@southderbyshire.gov.uk
Telephone: 01283 595795

6.0 Definitions

Term	Definition
BWV (Body worn video)	Body worn video (BWV) is a wearable audio, video, or photographic recording system used to record events by relevant council officers. They are typically worn on the torso of the body on the officer's uniform.
CCTV (Closed circuit television)	The use of video cameras to transmit a signal to a specific place on a limited set of monitors. Frequently used for monitoring public space.
(DPIA) Data Protection Impact Assessment	A process designed to help data controllers (the Councils) to systematically analyse, identify and minimise the data protection risks of a project or plan. These are a legal

	requirement under general data protection regulation (GDPR) for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals.
Deployable	A mobile camera which can be moved and fixed in a location for a specific purpose and period. Used to detect environmental crime and monitor hotspots e.g. fly-tipping.
Overt	Done or shown openly e.g. in a public place.
Surveillance Camera	Broad term to describe CCTV, body worn cameras and other devices used for overt surveillance purposes including deployable cameras.
Surveillance System	Broad term for the linked equipment used for capturing, recording and viewing images for overt surveillance purposes. They are used to monitor or record the activities of individuals, or both.
System Operator	Those with overall responsibility for the surveillance systems i.e. the Councils.
System Owners	Have overall responsibility for the operation of the surveillance system under their control and adherence to this policy, associated legislation and codes of practice.
Surveillance Administrator (System Managers)	A designated lead officer who has overall responsibility for the specific surveillance system/s.
System Users	Designated members of staff who are authorised to use the surveillance equipment and/or system.

7.0 Roles and Responsibilities

Responsible	Accountable
• ***JOB ROLE/SERVICE AREA*** ***Heads of Service (System Owners)*** 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:	• ***JOB ROLE/SERVICE AREA*** ***Chief Executive (System Operator)*** 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 System Owner and Surveillance

- 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 (System Managers)

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.

System Users are responsible for using the surveillance equipment and systems in accordance with this policy and operational guidance.

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)

Consulted	Informed
• ***Environmental Health*** *Environmental Heath use a variety of different surveillance systems including re-deployable cameras for capturing Fly tippers and Body Warn Cameras for ASB Patrols. The Environmental Health Head of Service has been consulted.* • ***Legal Services*** *Legal services consulted to ensure the Policy is fit for purpose*	• ***JOB ROLE/SERVICE AREA/ STAKEHOLDER*** • ○ ***Senior Management Team*** *For information* ○ ***Elected Members via Committee*** *For information* • ***Trade Unions (where applicable)*** *Trade unions were previously consulted regarding the CCTV in the Workplace section of the Policy. The wording in that section hasn't been amended so no need to consult with them again.*

8.0 Sustainability Impact Assessment

This assessment is completed using the below table. You must select the potential impact of this policy on the environmental, economic and societal aspects within the corporate plan. Your assessment should be detailed in the "findings" section. You must detail the reasoning and the mitigation of any negative impacts. If there is 'no impact' no detail needs to be given.

Our Environment	Potentially positive impact (Y/N)	Potentially negative impact (Y/N)	No disproportionate impact (Y/N)	**Sustainable Assessments findings** *(Please utilise the guidance provided for assessment findings.)*
Improve the Environment of the District	Y			*Provides EH with Tools to combat Fly Tipping and ASB including Damage and Graffitti*
Tackle Climate Change			Y	
Enhance the attractiveness of South Derbyshire	Y			*By targetting flytipping and criminal damage it wil Improve public spaces to enjoy the environment?*
Our People				
Engage with Communities			Y	
Supporting and safeguarding the most vulnerable	Y			*Will help with keeping the public safe and assisting the police in investigating crime and disorder.*
Deliver Excellent Services			Y	
Our Future				
Develop Skills and careers				

			Y	
Support economic growth and infrastructure	Y			*CCTV in the Town Centre will assist in reducing business crime to support economic growth through keeping the town safe and encouraging new businesses.*
Transforming the Council	Y			*Supports the councils aims including to keeping* • *Improve the environment of the District* • *Enhance the attractiveness of South Derbyshire* • *Enhance the appeal of Swadlincote town centre as a place to visit.* • *Improve public spaces to create an environment for people to enjoy.* • *Help tackle anti-social behaviour & crime through strong and proportionate action.*

9.0 Policy Review

In order to comply with the Surveillance Camera Code of Practice, this policy will be reviewed every three years.

10.0 References

- Home Office Surveillance Camera Code of Practice 2013 (Amended Nov 21)
- 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 2018
- 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
- 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 (Amended Nov 2021)

11.0 Associated Documentation

Description of Documentation	Document Reference
SDDC RIPA Policy	136
SDDC Information Security Policy	41
SDDC Corporate Plan	
SDDC Council Data Retention Policy	195
SDDC Data Protection Policy	166
SDDC Disposal of IT Equipment Policy	153

12.0 Appendices / Glossary

Appendix 1 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	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 & CSO	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 & CSO	Yes	No	None	Yes
3	Fixed CCTV in Midway Community Centre	6 Cameras on building covering surrounding area	Head of Corporate Property	Building Services Manager, Property Services	Communities Manager, CSO and Facilities Supervisor	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 Head of Service	Principal Community Safety Enforcement Officer	5 x Community Safety Enforcement Officers & 1x Park Warden	Yes	No	None	Yes
9	Redeployable Flytipping Cameras	Whole District covering Flytipping hotspot sites	Environmental Health Head of Service	Principal Community Safety Enforcement Officer	5 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 Head of Service	Principal EHO (Environmental Protection)	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
14	Fixed CCTV Cameras at Stenson Community Centre	13 Static Cameras, 5 covering external locations and 8 covering internal locations	Head of Corporate Property	Building Services Manager, Property Services	Communities Manager, CSO and Facilities Supervisor	Yes	No	None	Yes
15	Dash Cams	3 Cameras situated in the Vans used by Community Safety Enforcement Officers	Environmental Health Head of Service	Principal Community Safety Enforcement Officer	5 x Community Safety Enforcement Officers	Yes	No	None	Yes
16	Window cill cams	Mobile cameras for anti-social behaviour investigations	Environmental Health Head of Service	Principal Community Safety Enforcement Officer	5 x Community Safety Enforcement Officers	Yes	No	None	Yes
17	Drone	Third party equipment for aerial surveillance	North West Leicestershire DC	Principal Community Safety Enforcement Officer	No internal staff	Yes	No	None	Yes
18	Static roadside CCTV cameras	Static camera for fly tipping hot spots	Environmental Health Head of Service	Principal Community Safety Enforcement Officer	5 x Community Safety Enforcement Officers	Yes	No	None	Yes
19	Static roadside ANPR cameras	Static camera for fly tipping hot spots	Environmental Health Head of Service	Principal Community Safety Enforcement Officer	5 x Community Safety Enforcement Officers	Yes	No	None	Yes
20	Solar mobile CCTV cameras	Mobile camera for fly tipping hot spots	Environmental Health Head of Service	Principal Community Safety Enforcement Officer	6 x Community Safety Enforcement Officers	Yes	No	None	Yes

12.1 Equalities Impact Assessment Form

The Equality Impact Assessment - Preliminary Assessment Form has been completed and there are no potentially negative impacts on any of the protected characteristics and therefore a full EIA is not required.

12.2 Policy Briefing Form

Introduction

This form is to provide a brief update to summarise the changes/amendments to an existing policy or to provide a summary for a new policy. This form should be used for the consultation, approval and communication of all adopted policies.

Policy update

A summary of the policy is detailed below

Policy Name: Surveillance Policy

Policy Date: Version 1 – 2018

Version Number: 3

Summary of Policy*:*

This policy outlines the use of CCTV surveillance by South Derbyshire District Council to enhance public safety, protect council buildings, assets, staff, elected members and visitors and support law enforcement activities while respecting individual privacy and civil liberties

Summary of key changes made to an existing policy.

Section	Amendment
5.1	New – added in detail on 12 Guiding principles from The Surveillance Camera Code of Practice
7.0	New - Roles and responsibilities
8.0	New – Sustainable Impact Assessment
12.1	New – Equalities Impact Assessment

Following final adoption of the policy, this form will be used by the communication team to be included in Core Brief as part of the communication plan.

Further information can be found in the 'My Policies' section in Connect.