Use of Overt Surveillance Systems Policy

May 2020

Bolsover District Council

North East Derbyshire District Council

We speak your language

Polish
Mówimy Twoim językiem

French
Nous parlons votre langue

Spanish
Hablamos su idioma

Slovak
Rozprávame Vaším jazykom

Chinese
我们会说你的语言

If you require this publication in large print or another format please call: Bolsover District Council on 01246 242424 or North East Derbyshire District Council on 01246 231111

CONTROL SHEET FOR Use of Overt Surveillance Systems Policy

Policy Details	**Comments / Confirmation** **(To be updated as the document progresses)**
Policy title	Use of overt surveillance systems (Joint policy)
Current status – i.e. first draft, version 2 or final version	Final Version
Policy author (post title only)	Information, Engagement & Performance Manager
Location of policy (whilst in development)	S Drive
Relevant Cabinet Member (if applicable)	Portfolio holder for Corporate Governance (BDC) Portfolio holder for Council Services (NEDDC)
Equality Impact Assessment approval date	
Partnership involvement (if applicable)	
Final policy approval route i.e. Joint Strategic Alliance Committee, Cabinet/Executive/Council	Customer Service & Transformation Scrutiny (BDC) Organisation Scrutiny (NEDDC) Executive (BDC) Cabinet (NEDDC)
Date policy approved	
Date policy due for review (maximum three years)	2023
Date policy forwarded to Performance (to include on Extranet and Internet if applicable to the public)	

CONTENTS

1. Introduction

1.1. This document sets out Bolsover District Council's and North East Derbyshire District Council's ('the Councils) policy on the use of overt surveillance systems.

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

1.3. A surveillance camera is a broad term to describe close circuit television (CCTV), body worn cameras and other devices used for overt surveillance purposes.

1.4. The Councils use overt surveillance systems for the purposes of public safety, crime prevention, detection and prosecution of offenders, monitoring council buildings and assets to protect the public, staff, elected members and visitors, and its property.

1.5. The Councils fully recognise that the use of overt surveillance systems need 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).

1.6. 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 and the Information Commissioner's CCTV Code of Practice.

1.7. This policy together with Councils' Data Protection Policy and operational guidance will support surveillance system owners, managers and users on the management, administration and operation of surveillance systems for overt use.

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.
Data controllers	Those who determine the purposes and means of processing personal data i.e. the Councils.
(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 owner	A designated lead officer who has overall responsibility for the specific surveillance system.
System manager	An operational lead officer for the day to day running of a specific surveillance system.
System user	Designated members of staff who are authorised to use the surveillance equipment and/or system.

Legislation

The policy takes into account the:

- Surveillance Commissioners, Surveillance Camera Code of Practice. https://www.gov.uk/government/organisations/surveillance-camera-commissioner
- Information Commissioners CCTV Code of Practice https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
- Protection of Freedoms Act 2012. (2012 Act) http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
- Documents issued by the Home Office in October 2016 (revised 2018):
  - Technical Guidance for Body Worn Video Devices
  - Safeguarding Body Worn Video Data
- Requirements for processing personal data as set out in the General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Right to privacy as set out in Article 8 of the European Convention on Human Rights https://www.echr.coe.int/Documents/Convention_ENG.pdf

2. Scope

2.1. The policy is applicable to all employees and service areas which operate any form of overt surveillance system.

2.2. 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).

2.3 This policy will be made available to the public.

3. Principles

3.1 The Surveillance Camera Code of Practice (the Code) was issued in 2013 following the introduction of the Protection of Freedoms Act 2012 and further updated in 2014. The Code provides guidance on the appropriate and effective use of surveillance camera systems.

3.2 The Councils are relevant authorities as defined by section 33 of the Protection of Freedoms Act and therefore must have regard to the Code.

3.3 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.

3.4 The Code provides 12 guiding principles which the Councils have 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.

4. Statement

4.1 Use of surveillance camera systems

Surveillance camera systems operating in public places must always have a clearly defined purpose in pursuit of a legitimate aim and necessary to address a pressing need.

The Councils use CCTV on and within its buildings to:

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

The Councils will publish a list of areas where CCTV is in operation.

The Councils designate officers undertaking relevant job roles 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 Councils also authorise 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 Councils have 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.

Any proposals for the use of new 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) undertaking 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 demonstrate that both the necessity and extent of any interference with Article 8 rights (Human Rights Act – respect for private and family life) has been considered.

The Councils note 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 Councils note that they cannot proceed with the processing until this consultation has taken place. Where the Councils can take steps to reduce the risk then there is no requirement to consult with the ICO.

The Councils may also need to 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.

4.2 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 Councils recognise that continuous recording will require strong justification as it is likely to be excessive and cause a great deal of collateral intrusion.

The Councils will therefore only deploy surveillance systems in public places where there is a particularly high expectation of privacy, such as toilets or changing rooms, to address a particularly serious problem that cannot be addressed by less intrusive means. Such deployment will be subject to regular review, to ensure it remains necessary.

The Councils note the Code's statements on a surveillance camera system use on recording conversations between members of the public as highly intrusive and requiring a strong justification of necessity to establish its proportionality.

The Councils will prescribe guidance to officers covering the use of surveillance camera especially in situations where a higher level of privacy is expected, for example, use of BWV cameras in private dwellings. This guidance will also cover use with vulnerable individuals and sensitivities around religious or cultural beliefs and practices.

With regards to CCTV and deployable camera installations every consideration will be given to 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' preventing privacy intrusions.

4.3 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 Councils will publish information on its websites on the surveillance camera systems that they use, how to make requests for images and how to make a complaint about the use of surveillance camera systems. The Councils will use their corporate complaints policies and procedures for this purpose. Information on surveillance camera systems is also included in its published privacy statements.

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). Users will also carry cards to give to individuals as and when required providing the purpose for the use and contact information for further information.

The Councils will prescribe guidance on how to record an incident using a BWV camera including making a verbal announcement at the start of any recording or as soon as it is practicable to do so which is captured for the record and informs the individual concerned.

4.4 Accountability

The Councils will have proper governance arrangements for each surveillance camera system and understands that it is good practice to have a designated individual responsible for the development and operation of a surveillance camera system.

The Councils are the system operators and data controllers for each surveillance system. A system owner (lead officer) will be established for each system. They are responsible for the system as whole and its compliance with this policy and associated documentation. Other roles as required will be assigned for each system with clearly documented responsibilities in operational procedures or guidance supporting this policy.

4.5 Use or processing of images and information

The Councils recognise that having clear policies and procedures aid the effective management and use of a surveillance camera system.

All system users will undertake training and be issued with guidance before they use a surveillance camera. This will ensure that staff have the necessary skills and knowledge on the operational, technical and privacy requirements and fully understand the policies and procedures. This also ensures the reliability of staff having access to personal data including images and information obtained by surveillance camera systems as required by data protection legislation.

4.6 Retention

The Councils 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 Councils 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 Councils will ensure that information is stored so that recordings relating to a specific individual or event can be easily identified, located and retrieved.

4.7 Access

Access to surveillance systems will be restricted to those who need access as part of their job role to support the purpose of the system in question. The disclosure of images and other information obtained from a surveillance camera system will be controlled and consistent with the stated purpose for which the system was established.

The Councils have clear policies and guidelines in place to deal with any requests that are received.

4.8 Application by individual data subjects

Individuals can request images and information about themselves through a subject access request under GDPR. The Councils have a centralised team which handles requests. The Councils publish information on its websites on how to make a request and also have specific forms to request CCTV and BWV footage. Data subjects rights and the Councils' processes for handling requests are covered in the corporate data protection training which is mandatory for all new employees with refresher training provided every two years.

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.

4.9 Access to and disclosure of images to third parties

Disclosure of images or information may be appropriate where the Data Protection Act 2018 makes exemptions which allow it provided that the requirements of the Act are met, or where permitted by other legislation such as the Counter Terrorism Act 2008. These exemptions include where non-disclosure would be likely to prejudice the prevention and detection of crime, and for legal proceedings purposes.

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 Councils will consider such requests with care and in accordance with data protection legislation.

The Councils have 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 Councils have disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image.

The Councils will include in its operational guidance supporting this policy arrangements for secure disclosures to third parties.

4.10 Freedom of information

The Councils are relevant public authorities under the Freedom of Information Act. As surveillance systems record the activities of individuals then in most cases requests for information will concern personal data and are unlikely be disclosed in response to a freedom of information request. Requests may need to be administered under data protection legislation instead.

Some requests may ask for information regarding the operation of surveillance systems, the siting of cameras, or the costs and such requests will fall under the scope of the Freedom of Information Act.

The Councils have resources and processes in place to administer freedom of information requests. Information on how to make a request is published on its websites.

4.11 Standards for the surveillance camera industry

The Surveillance Camera Commissioner has a statutory role to provide the surveillance camera industry with a current list of standards. The Councils will adhere to those standards where appropriate and any supporting guidance, for example Technical Guidance for BWV devices (2018).

4.12 Security measures for surveillance camera system images and information

The Councils will have effective security safeguards in place to help ensure the integrity of images and information should they be necessary for use as evidence in legal proceedings.

This policy together with operational guidance supports the requirement under data protection legislation (General Data Protection Regulation and Data Protection Act 2018) to have a clear policy on how images and information are stored and who has access to them. The Councils will only use or process images and information for the purpose (or consistent with that purpose) of the camera deployment and purpose stated for collection of images.

Security extends to technical, organisational and physical security and the Councils will have measures in place to cover these aspects and guard against unauthorised use, access or disclosure.

Organisational measures

The Councils will not use surveillance cameras if there are less intrusive and more effective methods of dealing with the problem. As such prior to any decision to procure a new surveillance camera system a Data Protection Impact Assessment (DPIA) will be

undertaken to inform the decision making process and advice sought from the Councils' Data Protection Officer.

Other measures include this policy, supporting guidance and the Councils' Data Protection policy.

No equipment other than that authorised by the Councils shall be used to undertake overt surveillance and record images.

All system users will receive training on all relevant aspects of the surveillance camera system before using the system. This training will be refreshed as required.

Technical measures

The Councils will ensure that that any surveillance camera system procured will be fit to meet the stated purposes for the system and can produce images of the right quality. This will include the involvement of relevant technical employees in the procurement process, completion of a data protection impact assessment, adherence to procurement procedures and due diligence.

Permanent (e.g. CCTV) and movable cameras (e.g. Deployable) will be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property.

All surveillance camera systems will be fully maintained and any faults or defects dealt appropriately with in accordance with the procedure for that system.

Physical measures

Where any CCTV or deployable camera is installed the Councils will display signage to inform the public. Signs that cameras are operating will be displayed in and around surveillance areas in visible locations. There is however no requirement to place signs directly under individual cameras. The signs will state who is operating the system i.e. the data controller and provide a contact number for further information.

No unauthorised persons will have access to any restricted CCTV control rooms without an authorised member of staff being present. Any monitors showing live images will be positioned so that they are visible to relevant staff and members of the public will not be allowed access to the area where staff can view them.

Viewing of BWV or deployable footage will only take place in a location agreed by a System Manager. Any footage (including audio) will not be played in an area where it might be overseen or overheard by others.

The casual viewing or trawling of images is strictly forbidden. Viewings must only be undertaken for a specific, legitimate and documented purpose and anyone accessing footage for a purpose not consistent with this may be subject to disciplinary action.

4.13 Review and audit mechanisms

The Councils will review annually the continued use of their surveillance camera systems to ensure that it remains necessary, proportionate and effective in meeting its stated purpose for deployment.

4.14 Processing images and information of evidential value

The Councils recognise that the effectiveness of a surveillance camera system will be dependent upon its capability to capture, process, analyse and store images and information at a quality which is suitable for its intended purpose. Wherever the purpose of a system includes crime prevention, detection and investigation (as for body worn video and deployable cameras) then the Councils note that the system needs to be capable through its processes, procedures and training of system users, of delivering images and information that is of evidential value to the police and the criminal justice system.

Such recorded material will be stored in a way that maintains that meta data e.g. time, date and location, is recorded reliably, and compression of data does not reduce its quality. A record will be kept as an audit trail of how images and information are handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court.

The Councils body worn video surveillance system can (with appropriate safeguards in place):

- Export images and information when requested by a law enforcement agency without interrupting the operation of the system.
- Export images and information on a format which can be readily accessed and replayed by a law enforcement agency.
- Preserve the quality of the original recording and any associated meta data e.g. time, date and location.

4.15 Reference databases

Whilst not in use by the Councils they note that any use of technologies such as ANPR (Automatic number plate recognition) or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.

5. Responsibility for Implementation

Keeping the policy under review and updating the policy is the responsibility of the Data Protection Officer for the Councils. The Director of Corporate Resources and Head of Paid Service has overall responsibility for the policy.

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.

System managers have operational responsibility for the surveillance system under their control and adherence to this policy, associated legislation and codes of practice. Key

areas of responsibility include the implementation of and adherence to operational guidance, that system users have received appropriate training and that the equipment and surveillance system is working effectively.

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