



# **Ashfield District Council CCTV and Surveillance Policy September 2021**

## Contents

1. Introduction	3
2. Policy Objectives	3
3. Legislation	3
4. Surveillance Camera Commissioner: Code of Practice	4
5. Responsibility	5
6. Purpose and Installation	6
7. Code of Practice for Surveillance Cameras & Personal Information	7
8. Covert Cameras	7
9. Purchase and Deployment of CCTV Cameras	7
10. Deployable Mobile CCTV Cameras	8
11. Body Worn Video	8
12. Fleet Video Devices	10
13. Noise Monitoring Equipment	10
14. Quality of System	10
15. Signage	10
16. Requesting Footage / Provision of evidence	11
17. Security	12
18. Data Retention	12
19. Statistics	12
20. Health and Safety	12
21. Complaints	13
22. Useful Links	13

## 1. Introduction

Ashfield District Council (“the Council”) utilises Closed Circuit Television (“CCTV”) systems in public spaces, covering town centres, neighbourhoods, car parks and Council owned sites across the District.

The Council’s public space CCTV is centrally managed at the control room situated at Sherwood Lodge, Nottinghamshire Police Headquarters. The recording of the system is also undertaken from this location, as is most of the reviewing of footage. However, reviewing of footage can also be completed from the Community Safety Hub located at Ashfield District Council Urban Road offices.

This document is designed to give clear guidelines on the Council’s use of CCTV and how the systems can be accessed by partner agencies and the public, in line with legislative provisions and guidance. This extends to the use of Body Worn Video (“BWV”), deployable CCTV cameras, Fleet video equipment and noise monitoring equipment, and the gathering, storage, use and disposal of personal data.

This Policy applies to all employees of Ashfield District Council including contractors and agency workers and outlines the standards expected from employees and any external agencies such as the police who may have access to the CCTV equipment if a lawful request arises.

## 2. Policy objectives

The three objectives of this policy are as follows:

1. To outline the responsibilities of those involved in the Council’s CCTV system.
2. To clearly state the purposes for which the CCTV system was installed and should be used, including temporary and mobile CCTV.
3. To set out the process of how images can be obtained and used.

## 3. Legislation

In addition to Council policies and procedures, guidelines and Codes of Practice for CCTV and BWV, the operation of CCTV systems is subject to legislation under:

- The Data Protection Act 2018 (“DPA 2018”) (as amended)
- UK General Data Protection Regulation Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2019 made on 28<sup>th</sup> February 2019 (as amended by the Data Protection, Privacy and Electronic communications (amendments etc) (EU Exit) Regulations 2020 Laid on 14<sup>th</sup> October 2020)
- The Human Rights Act 1998 (HRA).
- The Freedom of Information Act 2000 (FOIA).

- The Regulation of Investigatory Powers Act 2000 (RIPA).
- The Protection of Freedoms Act 2012 (POFA).
- Criminal Procedures and Investigations Act 1996 (CPIA)

The Human Rights Act 1998 gives effect in the UK to the rights set out in the European Convention on Human Rights (ECHR) Article 8 provides for a person's right to respect for their private and family life, home and correspondence, and is one of the qualified rights within the Act. Surveillance that may interfere with such a right should only be carried out where it is necessary and proportionate to do so.

The purpose of this policy is to ensure that the above legislation is complied with at all times when operating the CCTV and Body Worn Video systems/devices and to ensure compliance with the codes of practice as outlined below.

#### **4. Surveillance Camera Commissioner: Code of Practice Legislation**

Ashfield District Council is a relevant authority as defined by The Protection of Freedoms Act 2012 (POFA) and it recognises that it must have regard to the Surveillance Camera Commissioner's Code of Practice when exercising any of the functions to which the code relates. This policy recognises the importance of the 12 guiding principles of the Code (outlined below). All employees must adhere to these principles in conjunction with the lawful operation of the CCTV and BWV systems and devices. The following principles are designed to provide a framework for operators and users of surveillance camera systems so that there is proportionality and transparency in the Council's use of surveillance.

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 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 securely 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. Responsibility

- **Directorate of Place and Communities** - The CCTV responsibility forms part of the Place and Communities Directorate of the Council and contact responsibility will remain with the Director however day to day supervision and management, both financial and organisational, will be the responsibility of the Community Safety Team. They will be responsible for ensuring users within the Council are up to date with the legislation and changes in procedures. This includes meeting with any third party provider of CCTV operators to ensure they have the relevant up to date provisions in place.
- **Community Safety Manager** – They have current responsibility for strategic and operational management of CCTV. This may include dealing with complaints, agreeing standard reviewing of images and requests for reviews, reporting of problems and faults and general liaison between customers and the CCTV service. They are not authorised to commit to any works requiring additional expenditure.

- **CCTV Operators** – The personnel operating CCTV systems are responsible for operating the equipment in accordance with requirements set out in current legislation, this policy document, guidelines, confidentiality certificates, Codes of Practice and local Operational Manuals. This also includes permitting downloading of images, being involved in operations run by a third party and use of radios and other telephony systems linked to the CCTV system.

They must ensure that their training is up to date and any qualifications or security checks are kept valid and in date. They are responsible for bringing any faults or misuse of the equipment to the attention of the Community Safety Manager or deputies and also logging each fault as required through to the maintenance contractors.

- **Responsible Officers Alternative Sites** - Where CCTV systems have recording facilities or equipment within the Council there is a requirement that each site has a responsible officer to ensure the security and confidentiality of the equipment. A list of these responsible personnel is attached as Appendix A.

## 6. Purpose and Installation

It is important that everyone and especially those charged with operating the CCTV systems within the Council understands exactly why each of the systems has been introduced and what the cameras will and will not be used for.

Each CCTV system will have its own site or task specific objectives. Below is a list of reasons why CCTV could be installed across the District:

- Protecting areas and premises used by Council employees and the public;
- Preventing and detecting crime, disorder and anti-social behaviour;
- Assisting in the identification of offenders leading to their arrest and successful prosecution or other appropriate action;
- Reducing violent or aggressive behaviour towards employees;
- Public safety – including reducing fear of crime and anti-social behaviour and aggression;
- Protecting Council property and assets;
- Assisting in employee disciplinary and grievance, formal complaints and Health and Safety investigations.

The location of the CCTV equipment is important and must be carefully considered. The areas to be covered must be clearly identified, and the way in which images are recorded must comply with Data Protection Principles as follows:

- Cameras must only monitor those spaces intended to be covered.
- Cameras must be sited to ensure that they comply with purpose.

- If there is a risk of a neighbouring area being monitored the owner of the area must be consulted.
- Adjustable cameras must be operated to prevent unintended areas being monitored.
- Some areas have heightened expectations of privacy, such as changing rooms and toilets, and cameras must not contravene privacy and the right to respect for private life.

The systems will not be used for any other purpose than those set out in this document without prior consultation with the Director of Place and Communities and where appropriate notification to employees and following consultation with the Trade Unions and where appropriate, residents via community consultation.

Employees or those working on behalf of the Council will only be monitored if there is a reasonable cause to suspect a criminal offence or serious breach of discipline, potentially amounting to gross misconduct has been, or may be, about to be committed and this will only be permitted when authorised. Covert monitoring will only take place if RIPA authorisation has been obtained.

## **7. Data Protection Code of Practice for Surveillance Cameras and Personal Information**

This code provides good practice for those involved in the operation of CCTV and the code of practice advises how best to comply with the seven principles outlined in the UK GDPR and the six principles outlined in the DPA part 3 (criminal processing). The code also provides guidance as to when CCTV and BWV devices should be used and the governance arrangements around them.

This policy and this code of guidance should be read in conjunction with the Data Protection, data retention provisions, shared service policy and agreements, and operating procedures. All operators of CCTV, BWV and Noise Monitoring equipment must have suitable training/experience.

## **8. Covert Cameras**

Ashfield District Council is committed to respecting our citizens right to privacy. Any decision that impacts on that potential loss of privacy must be considered carefully and cameras deployed only where it is necessary and proportionate to do so.

- Cameras should be clearly visible and clearly signed.
- Covert cameras can only be placed where there is a lawful RIPA authorisation in place and the Council's RIPA policy and guidance is adhered to.

## **9. Purchase and Deployment of CCTV Cameras**

The Council's commitment to respecting people's rights to privacy and support the individual's entitlement to go about their lawful business. This is a primary consideration

in the operation of any CCTV system or surveillance equipment, although there will inevitably be some loss of privacy when CCTV cameras are installed. Therefore, it is pivotal that serious consideration is given to the necessity for cameras to be installed and used across the District.

Cameras are not to be installed in such a way that they can look into private space, such as houses, unless they can be fitted with privacy zones, which block out private areas so that they cannot be viewed or recorded.

If after looking at all the alternatives it is decided that CCTV is the only suitable solution a Data Protection Impact Assessment (“DPIA”) will be conducted to ensure clear operational objective for the system and each camera is identified, to assess any potential impact of data processing on individual’s rights and freedoms in addition to identifying and, where possible, mitigating any risks identified to those rights and freedoms.

Ashfield District Council do not deploy ‘Dummy’ cameras as these give a false sense of security. Concealed and unsigned cameras within Council property may on rare occasions be deployed in areas of high security where there is no legitimate public access and where employee access is controlled and restricted. Ashfield District Council and Police personnel who normally work in these areas should, where appropriate, be informed of the location of these cameras, their purpose and where the monitor is kept.

## **10. Deployable (Mobile) CCTV**

Deployable CCTV cameras are used by the Councils’ main CCTV system. They should comply with the requirements set out in this Policy Document and demonstrate:

- That an operational assessment has been undertaken to justify the deployment and to consider whether it is both necessary and proportionate to do so.
- Secure anchorage and power supply for the cameras is available and there are suitable locations for CCTV signs.
- A DPIA for each deployment.
- An Equality Impact Assessment if appropriate.
- A Risk Assessment of the safety of employees deploying the cameras.
- A checking mechanism to establish whether RIPA authorisation is required and if so, that the deployment is: proportionate, lawful, appropriate and necessary. Any deployable camera to be used in a covert operation must have a RIPA authorisation.
- Where cameras are deployed on property accommodating or owned by third parties that their written permission is obtained from the owner indicating that they have had the implications of the deployment explained to them.

## **11. Body Worn Video**



Body Worn Video (“BWV”) devices can be used by Community Safety and Environmental Enforcement Teams for the following purposes:

- The prevention and detection of crime, through the gathering of intelligence including use of images and sound as evidence in criminal and/or civil proceedings.
- Reduce incidences of public disorder.
- Present evidence to support the Council’s procedures/action.
- Address issues associated with staff practices.
- Identification of training needs.
- To safeguard officers from malicious complaints / allegations
- Exercising Legal Powers / Authority.

The UK GDPR applies because CCTV cameras capture personal information that could identify someone. This policy outlines the principles the Council adhere to, the processes that are followed and related policies and processes, such as those about how to request information including CCTV images.

BWV equipment is capable of capturing primary evidence in such a way that it is able to bring a compelling and an indisputable account of the circumstances at that time. This will not replace the need to capture other types of evidence but will go a considerable way in reducing any ambiguities and should be considered as an additional aid.

BWV equipment will not be routinely recording and monitoring all activity on a continuous basis. To do so could potentially infringe rights and freedoms of law abiding members of the public, as well as the privacy of employees going about their work. This cannot be justifiable from the perspective of proportionality and legitimacy.

The use of BWV equipment will be used primarily for incidents and circumstances presented to Enforcement Officers (authorised employees) as set out above; scenarios include, responding to reports of Anti-Social Behaviour and Environmental incidents e.g. Littering Offences, Street Drinkers, Noise investigations. Scenarios would also include unexpected incidents that result in risk, threat, harm and vulnerability. This is not an exhaustive list and this would apply to a wide range of incidents.

The BWV device will be clearly worn by the enforcement officer in an overt manner and the device will clearly show that it is a CCTV recording device by signage in addition to verbal instruction as appropriate. Data subjects will be informed of the Council’s Privacy Notice accessible on the Council’s website.

It is acknowledged there will be occasions where it will not be practicable to provide instruction as set out above, and as such the enforcement officer must document reasons and justification for recording. i.e. because a colleague or resident was in immediate danger, risk to life etc.

There will be occasions where a member of the public requests the enforcement officer to cease recording and as such, the officer must determine if continued recording is justified. It is good practice for the officer to provide justification for continued recording.

Enforcement officers are required to use the equipment in line with this policy, associated procedures, organisation strategies and the law, and will receive full instructions in its use and the relevant legislation.

Devices will be stored in the Council's Building and will only be used in conjunction with Council approved software and devices and have password protection to prevent tampering or misuse of equipment. This will be in line with the Council's IT and Security Policies.

## **12. Fleet Video Devices**

The Council has CCTV camera systems fitted to a number of vehicles for the reasons outlined throughout this policy. The cameras operate automatically via vehicle ignition and can only be accessed by authorised officers in line with this policy.

The Council may also use vehicles who have CCTV / Dash Cams fitted and where this is the case, there will be clear signage so that any occupants of the vehicles will be aware of any CCTV. A DPIA will be in place for any such usage in addition to bespoke policies as necessary.

## **13. Noise Monitoring Equipment**

The Council utilises noise monitoring equipment and may use this equipment to install into residential and commercial premises. This will be for the purposes of investigating allegations of noise nuisance and/or anti-social behaviour. All equipment will be tested and calibrated appropriately as part of ongoing maintenance contracts and will be utilised in accordance with the Council's Anti-Social Behaviour Policy, Environmental procedures, and associated noise installation protocols.

Information may be retained for up to 7 Years in line with the Council's retention policies and be recorded onto the case management systems ECINS / FLARE.

## **14. Quality of System**

The Councils' Public Space CCTV systems are managed centrally from the Police Control Room under a contractual arrangement between Newark and Sherwood District Council and Broxtowe Borough Council.

Under these provisions recording equipment and recording media will be kept in a secure location and no access will be granted to unauthorised employees. This includes those systems independent of the main CCTV system.

All Council devices will be subject to a maintenance contract and ongoing routine maintenance as well as fault rectification to ensure that the system is working appropriately. This includes cleaning of lenses and checking of settings. Unavoidably, due

to the technical and specialist nature of CCTV, there will occasionally be camera/recording downtime, however this will be kept to a minimum through periodic maintenance.

When replacing or adding to the system value for money will always be considered however quality will not be compromised and the quality of the system shall be maintained to a good standard. This is to ensure the system complies with relevant legislation and is fit for purpose.

## **15. Signage**

The Council will erect signage where CCTV is in operation and will use signage to advise individuals that they are about to enter or are in an area covered by CCTV cameras. The signs can act as a deterrent to deter anti-social behaviour or criminal activity.

Where 'Covert' cameras have been authorised under RIPA for deployment, signage will not necessarily be required.

CCTV signage used by Ashfield District Council will include the Council Logo and reference to the Council's Privacy Notice as set out by Advice by the Information Commissioners Office:

## **16. Requesting footage / Provision of Evidence**

Members of the public and external agencies outside of shared service provisions are not permitted to review the Councils' CCTV systems without making a formal subject access request ("SAR"), DPA 2018 Schedule 2, FOIA or other appropriate disclosure requests. If matters are relating to a recent incident it is anticipated the request or submits this promptly as it may be deleted after 30 days in line with the Council's retention policies.

It is paramount that a full and accurate record is kept of SAR requests and viewings of the systems and all instances when images are issued. This information must include:

- Date, time, camera number and location of the incident.
- The name of the lead officer,
- The date, time, name and contact details of the person viewing or removing images.
- The reason for the viewing/issue of images.
- Signatures of the person who released and received the images.

If any CCTV evidence of stills of footage are used in disciplinary / grievance hearings or employment tribunals, the footage will be retained and held on file until the appeals process and any employment tribunal and appeal have been completed. The recording will then be destroyed in line with the Council's retention policy.

Employees who are subject to performance matters or disciplinary, complaints or grievance procedures have the right to request that footage be retained if they believe it will assist their case. For disciplinary or grievance matters, the request must come from the officer / investigator (the authorised officer) who has been nominated to establish the facts / investigate the matter. Viewings will be permitted and images will only be released to the authorised officer in line with the Council's HR Policy.

Any other requests made, for example in contemplation or in respect of legal proceedings, will only be granted where it is a lawful request and it has been validated by the Council's Legal Team. All SAR and FOI requests must be sent to the Council's Legal Team by email to [foi@ashfield.gov.uk](mailto:foi@ashfield.gov.uk) or in writing.

Council recorded material will not be sold or used for commercial purposes or for the provision of entertainment. Images provided to the police or other enforcement agencies or for internal investigations shall at no time be used for anything other than the purposes for which they were originally released.

## **16. Security**

CCTV images will be viewed in a controlled environment which includes both CCTV Control Room and Community Safety Hub. The Council will also allow review of video evidence by authorised leads and heads of service in respect of assets and fleet vehicles in their respective areas.

CCTV recordings should not be displayed in a public space or left to display where public/visitors could view the screens. Including, and not restricted to, leaving CCTV displays unattended which allow a non-authorised person to lean over a desk, or walk around, to see what is on the screen.

Recording equipment should only be accessible to those who have a genuine need to access them. Any cameras that are installed to protect premises should be locked down so unauthorised users cannot access its material.

Tampering with or misuse of cameras, monitoring or recording equipment, images or recorded data by employees may be regarded as misconduct and could lead to disciplinary action, which may result in dismissal or prosecution.

Any breach of this Policy Document or the CCTV Code of Practice may be dealt with according to the Councils' disciplinary procedures.

## **17. Data Retention**

CCTV will be kept in line with the Council's retention policy and the records management provisions of Ashfield District Council. CCTV footage will not be kept longer than 30 days unless this is for lawful reason e.g., investigation, criminal or civil proceedings.

Any information captured and used in evidence as part of an investigation or prosecution may be kept for a maximum of 7 years.

## **18. Statistics**

CCTV installation, like any other purchase by a Local Authority, involves spending public money and this needs to be justified. CCTV systems are required to show the effectiveness of the cameras in dealing with the objectives set out for them. Therefore, performance data is monitored monthly through the Shared Service to illustrate this.

## 19. Health and Safety

All Council employees are required to comply with the Council's Health and Safety policy and provisions.

## 20. Complaints

Complaints about the operation of a CCTV system should be addressed initially to the Community Safety Manager, or the responsible officer. Complaints will be dealt with in accordance with the Councils' formal complaints procedure.

## 21. Useful Links

### Data Protection Act 2018

<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

### Regulation of Investigatory Powers Act, 2000

<http://www.legislation.gov.uk/ukpga/2000/23/contents>

### Protection of Freedoms Act, 2012

<http://www.legislation.gov.uk/ukpga/2012/9/contents>

### 'Surveillance Camera Code of Practice'

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/204775/Surveillance\\_Camera\\_Code\\_of\\_Practice\\_WEB.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf)

'In the picture: A data protection code of practice for surveillance cameras and personal information', ICO, May 2015

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

## **Appendix A- Alternative Sites**

Camera Type	Location	Post Responsible
Housing Cameras for ADC Homes, Courts and Complex's	ADC Urban Road, Council Offices	Service Manager, Housing Manager and Tenancy Services
CCTV Cameras for Council Assets	ADC Urban Road, Council Offices	Facilities Officer, Assets Manager
CCTV Cameras for Fleet Vehicles	Station Road, Council Offices	Environment Neighbourhood Service Manager

## **Appendix B – Background papers**

CCTV POLICY 2021

CCTV Shared Contract Agreement

DPIA 2021

BWV Manual

CCTV 2021 Audit

Privacy Notice

BWV User Guide

CCTV Responsibility List