



CCTV Policy

Dated: May 2022
Review Due: May 2025

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	5
7. Data Protection	6
8. Covert Cameras	7
9. Purchase and Deployment of CCTV Cameras	7
10. Deployable Mobile CCTV Cameras	7
11. Housing Stock	8
12. Body Worn Video	9
13. Fleet Video Devices	10
14. Quality of System	11
15. Signage	11
16. Requesting Footage / Provision of evidence	11
17. System Use	12
18. Data Retention	12
19. Complaints	12
20. Review	12
21. Useful Links	13

1. INTRODUCTION

- 1.1. New Forest 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. Subject to any exceptions outlined within this policy, CCTV will only be deployed within the boundaries of the Council.
- 1.2. The Council’s public space CCTV is centrally managed at the control room situated at Appletree Court, Lyndhurst. The recording of the system is also managed from this location. The Council has secondary monitoring facilities for public space cameras located at the Police Control Centre, Netley.
- 1.3. 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 (referred to collectively in this policy as “Surveillance Camera System(s)”) and the gathering, storage, use and disposal of personal data.
- 1.4. This policy applies to all employees of New Forest 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.
- 1.5. A detailed list covering the location of all public space CCTV cameras is published on the Council’s website [CCTV - New Forest District Council](#). This is kept under review and updated with any changes.

2. POLICY OBJECTIVES

- 2.1. 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 deployable CCTV.
 3. To set out the process of how images can be obtained and used.

3. LEGISLATION

- 3.1. In addition to Council policies and procedures, applicable guidelines and Codes of Practice (as detailed further below) for CCTV and BWV, the operation of CCTV systems is subject the following legislation:
 - Data Protection Act 2018 (“DPA”)
 - UK General Data Protection Regulation (“UK GDPR”)
 - Human Rights Act 1998 (“HRA”)
 - Freedom of Information Act 2000

- Regulation of Investigatory Powers Act 2000 (“RIPA”)
- Protection of Freedoms Act 2012 (“POFA”)
- Criminal Procedures and Investigations Act 1996
- Criminal Justice and Public Order Act 1994.
- Equalities Act 2010.

3.2. The HRA gives effect in the UK to the rights set out in the European Convention on Human Rights (“ECHR”). Article 8 of the ECHR 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 HRA. Surveillance that may interfere with such a right should only be carried out where it is necessary and proportionate to do so.

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

4. SURVEILLANCE CAMERA COMMISSIONER: CODE OF PRACTICE

4.1. The Council is a relevant authority as defined by the POFA and it recognises that it must have regard to the Surveillance Camera Commissioner’s Code of Practice (“the Code”) 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 Surveillance Camera 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

- 5.1 **Housing Estates Management & Support** - The CCTV responsibility forms part of the Governance & Housing Executive area and responsibility sits with the Service Manager for Housing Estates Management & Support who oversees the day to day operational management, in both a financial and organisational context. The Service Manager is responsible for ensuring users within the Council are up to date with the legislation and changes in procedures.
- 5.2 **CCTV Operations Manager** – They have current responsibility for operational management of the CCTV control room. 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.
- 5.3 **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, Codes of Practice and the Council's Operational Procedural Manual. 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.
- 5.4 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 CCTV Operations Manager or deputies and also logging each fault as required through to the maintenance contractors.

6. PURPOSE AND INSTALLATION

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

6.2. The objectives of the Council's Surveillance Camera Systems are:

- 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;
- Community reassurance and reducing the fear of crime;
- Reducing violent or aggressive behaviour towards employees;
- Public safety; and
- Protecting Council property and assets;

6.3. The location of the CCTV equipment is important and must be carefully considered. Particular considerations should be taken into account as follows:

- Cameras must only monitor those spaces intended to be covered;
- Cameras must be sited to ensure that they comply with purpose;
- Adjustable cameras must be operated to prevent unintended areas being monitored; and
- Some areas have heightened expectations of privacy, such as public toilets or communal areas within housing stock, and cameras must not contravene privacy and the right to respect for private life.

6.4. The Surveillance Camera Systems will not be used for any other purpose than those set out in this policy without prior consultation with the Housing Estates Management & Support Service Manager and, if appropriate, residents via community consultation.

7. DATA PROTECTION

7.1. CCTV systems may involve the processing of personal data because they may capture personal information that could identify someone. Accordingly, the Council's use of any CCTV system, must be carried out in accordance with the UK GDPR and the DPA.

7.2. In addition, the Information Commissioner's Office ("ICO") has issued Guidance on Video Surveillance ("the ICO Guidance"). This ICO Guidance provides good practice for those involved in the operation of CCTV and sets out 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 ICO Guidance also provides advice as to when CCTV and BWV devices can be used and the governance arrangements around them. The Council will have regard to the ICO Guidance in its CCTV activities.

7.3. The Council will also comply with the Council's Data Protection Policy, Law Enforcement Policy and Protection Special Category Data Policy when processing personal data obtained through CCTV.

8. COVERT CAMERAS

- 8.1. The Council is committed to respecting individuals' 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.
- 8.2. Covert cameras can only be placed where there is a lawful RIPA authorisation in place and the Council's Surveillance Policy is adhered to.

9. PURCHASE AND DEPLOYMENT OF CCTV CAMERAS

- 9.1. The purchase of Surveillance Camera System equipment shall be undertaken in accordance with the Council's Procurement Policies and subject to the approval of the Housing Estates Management & Support Service Manager. All new equipment shall comply the minimum security and ICT specifications as required to meet the Council's statutory obligations.
- 9.2. The Council is committed to respecting the right to privacy and supports the entitlement for individuals to go about their lawful business. This is a primary consideration in the operation of any Surveillance Camera System equipment, although there will inevitably be some loss of privacy when CCTV cameras are installed. Therefore, authorisation for the installation and use of any CCTV cameras must be limited to only when is necessary and proportionate.
- 9.3. Camera installation, where necessary, to protect the privacy of residential dwellings should include privacy screens, which restrict observation of sensitive areas.
- 9.4. If it is deemed proportionate and necessary that additional CCTV is the only suitable solution to achieve the Council's objectives as outlined at paragraph 6.2 above a Data Protection Impact Assessment ("DPIA") will be conducted to ensure there is a clear operational objective for the system and each camera is identified, to assess any potential impact of data processing on individuals' rights and freedoms in addition to identifying and, where possible, mitigating any risks identified to those rights and freedoms. The DPIA will be prepared in consultation with the Council's Data Protection Officer.
- 9.5. The Council do not deploy 'Dummy' cameras as these give a false sense of security.

10. DEPLOYABLE (MOBILE) CCTV

- 10.1. The Council may use deployable CCTV cameras where these are required to meet the objectives outlined at paragraph 6.2 above in relation to a specific issue at an identified site which is not already covered by the Council's principal CCTV system. Each deployment must comply with the requirements set out in this policy.
- 10.2. All applications for the deployment of deployable cameras should be in the form available on ForestNet and submitted to the Housing Estates Management & Support Service Manager. Each application must be supported by:
 - An operational assessment to justify the deployment and to consider whether it is both necessary and proportionate to do so.
 - Evidence that secure anchorage and power supply for the cameras is available and there are suitable locations for CCTV signs.
 - A DPIA.

- An Equality Impact Assessment, if appropriate.
- A Risk Assessment of the safety of employees deploying the cameras and the risk of damage or loss of equipment.
- A checking mechanism to confirm that the deployment does not amount to covert surveillance which would then require separate authorisation under the Council's Surveillance Policy.

10.3. Applications must also take the following requirements into consideration:

- **Justifiable** - there must be adequate reason to show that the cameras are an appropriate response. This will usually be shown by evidence of repeated complaints of past incidents, or intelligence on future incidents or events;
- **General** - the target of the surveillance must be in a public area or against unknown offenders. If a known individual(s) as this could become 'Direct Surveillance' and the deployment will additionally have to be authorised, as permitted, under RIPA.
- **Reviewable** - there must be a clear time limit for the duration of the deployment and an identified process of ongoing evaluation of the need for the cameras' continued use in a specific location. Deployments will reviewed after 7 days to ascertain whether the deployment should continue.
- **Objective** - there must be specified objectives to be achieved by the camera deployment and the achievement of these objectives should be monitored.

10.4. Whilst every effort will be made to deploy cameras on Council owned property, there may be occasions where it is necessary to deploy cameras on property in third party ownership. Where cameras are deployed on property accommodating or owned by third parties it is essential that the owner's written permission is obtained indicating that they have had the implications of the deployment explained to them. This should outline that any images obtained may be used as evidence in court proceedings; and that under the rules of disclosure it may be possible to identify their place of residence or their identity.

10.5. Deployment will only be permitted following the satisfactory completion of all steps outlined above and following the written authorisation from the Housing Estates Management & Support Service Manager, or in their absence, the Executive Head of Governance and Housing.

10.6. For the appropriate security and audit records pertaining to deployable equipment, all devices must be stored within CCTV services at Appletree Court.

11. HOUSING STOCK

11.1. As a Landlord, the Council provides and manages temporary accommodation building blocks across the district. Where it is deemed appropriate by the Housing Estate Management & Support Service Manager, CCTV will be installed at the entrance and exit of the buildings, communal internal areas and within the grounds of the exterior of those buildings.

11.2. The Council's intention is to balance the privacy rights of individuals, with its responsibilities to prevent and detect anti-social behaviour or crime. The Council will ensure the use of CCTV is proportionate to the impact of anti-social behaviour or crime on

individuals or communities.

- 11.3. The Council holds details on the location of all cameras that cover each site, with records of the CCTV system and quality checks. Cameras are in a fixed position, situated in prominent locations with no ability for operatives to pan and tilt or zoom. This prevents intrusion on private or sensitive areas.
- 11.4. Signs are prominently placed at strategic points and at the entrance and exit of the sites to advise residents, visitors and members of the public that a CCTV system is in use. Signage also contains information about the data controller and contact details.
- 11.5. The system is passively monitored only from within the confines of the CCTV secure control room at Appletree Court.
- 11.6. Images and footage will only be viewed for the following purposes:
 - Servicing and maintenance of the system;
 - Request from Police following the submission of a completed and authorised DP2; and
 - Regular site checks where CCTV is installed to ensure functionality and camera condition.
- 11.7. Hard-drives for the cameras are located within secure areas of each building with restricted access to authorised personnel only. They cannot be reviewed from their location with access to the footage only being permissible from the CCTV control room.

12. BODY WORN VIDEO

- 12.1. BWV involves the use of cameras that are worn by a person, and are often attached onto the front of clothing or a uniform.
- 12.2. BWV devices can be used for the following purposes:
 - Reduce incidences of public disorder.
 - Preserve evidence.
 - To protect officers.
 - Exercising Legal Powers / Authority.
- 12.3. Where any team wishes to use BWV for those purposes, they must comply with the requirements set out in this policy.
- 12.4. In the first instance, all applications for the use of BWV should be in the form available on ForestNet and submitted to the Housing Estates Management & Support Service Manager. Each application must be supported by:
 - An operational assessment to justify the use and to consider whether it is both necessary and proportionate.
 - A DPIA for the use.
 - An Equality Impact Assessment, if appropriate.

- A Risk Assessment of the safety of employees wearing the BWV and the risk of damage or loss of equipment.
- A checking mechanism to confirm that the use of the BWV does not amount to covert surveillance which would then require separate authorisation under the Council's Surveillance Policy.

- 12.5. The use of BWV will only be permitted following the written authorisation from the Housing Estates Management & Support Service Manager, or in their absence, the Executive Head of Governance and Housing. The use of BWV should be regularly reviewed to check that it is still necessary and proportionate.
- 12.6. 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.
- 12.7. BWV equipment will not routinely record and monitor activity on a continuous basis. To do so could 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.
- 12.8. The BWV device will be clearly worn by the officer in an overt manner and the device will clearly show that it is a CCTV recording device by signage. When activating the recording the officer must inform or verbally announce to individuals that the recording of video or audio or both is about to take place, and the reasons why, prior to turning on the BWV device. Data subjects will be informed of the Council's Privacy Notice accessible on the Council's website.
- 12.9. It is acknowledged there will be occasions where it will not be practicable to provide instruction as set out above, and as such, the officer must document reasons for the recording and the reasons why it was not appropriate to notify the individual. i.e. because of immediate safety concerns, risk to life etc.
- 12.10. Where requests to the officer are made to cease recording, the officer must determine if in doing so, there will be a loss of material or essential evidence. It is good practice for the officer to continually review the need to maintain recording and whether this is proportionate and necessary.
- 12.11. Officers are required to use the equipment in line with this policy, associated procedures, and operational guidance, and will receive full instructions on its use and the relevant legislation.
- 12.12. Devices will be stored only on Council's buildings and data transfer and storage will only be on approved Council ICT equipment. This will be in line with the Council's ICT and Security Policies.

13. FLEET VIDEO DEVICES

- 13.1. 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 data is recorded on a secure server with access only obtainable on Council computers to authorised personnel outlined below:

- Service Manager-Waste and Transport
- Transport Manager
- Insurance and Risk Officer

13.2. The Council may also use vehicles that have CCTV / Dash Cams fitted and, where this is the case, there will be clear signage so that any drivers/passangers 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.

13.3. As Fleet video devices are integrated within the vehicles, they may potentially be operated outside of the district boundaries.

14. QUALITY OF SYSTEM

14.1 The Councils' Public Space CCTV systems are managed centrally from Appletree Court.

14.2 Recordings are kept in a secure location and no access will be granted to unauthorised employees. This includes those systems independent of the main CCTV system, for example the Housing Stock system detailed in section 11 of this policy.

14.3 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.

15. SIGNAGE

15.1 The Council will erect signage where CCTV is in operation to inform 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.

15.2 CCTV signage used by the Council will include the Council logo and contact details.

16. REQUESTING FOOTAGE / PROVISION OF EVIDENCE

16.1 Only authorised members of staff will be permitted to view footage from any Surveillance Camera System equipment.

16.2 All other requests for information will be dealt with in accordance with the Council's Data Protection Policy, UK GDPR and DPA and, where appropriate, the Freedom of Information Act 2000.

16.3 It is paramount that a full and accurate record is kept of all requests for information received from third parties, including data subjects or third party agencies such as the police, 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.

16.4 All Subject Access Requests (“SARs”) and Freedom of Information (“FOI”) requests must be sent to the Council’s Information Governance and Complaints Team by email to data.protection@nfdc.gov.uk (for SARs) or foi@nfdc.gov.uk (for FOIs).

16.5 Requests from third party agencies, including the police are submitted on a DP2 form and disclosures will only be made in accordance with the UK GDPR and DPA where an applicable exemption applies.

17. SYSTEM USE

17.1 CCTV images will be viewed in a controlled environment at Appletree Court. The Council will also allow review of video evidence by authorised officers and Service Managers where applicable in relation to a Surveillance Camera System for their respective areas.

17.2 Surveillance Camera Systems will only be accessible to those who have been authorised in accordance with this policy.

17.3 Tampering with or misuse of Surveillance Camera Systems, images or recorded data by employees may be regarded as misconduct and could lead to disciplinary action, which may result in dismissal or prosecution.

17.4 Any breach of this policy may be dealt with according to the Councils’ disciplinary procedures.

18. DATA RETENTION

18.1 CCTV will be retained for a period of 28 days where upon it is automatically deleted from the Council’s servers.

18.2 CCTV footage will not be kept longer than 28 days unless this is for lawful reason e.g., investigation, criminal or civil proceedings or because there has been a request for information including a SAR.

18.3 Any information captured and used in evidence as part of an investigation or prosecution led by the Council may be kept for a maximum of 6 years from the final hearing by the Council’s Legal Services.

19. COMPLAINTS

19.1 Complaints will be dealt with in accordance with the Councils’ corporate complaints procedure.

19.2 If an individual wishes to raise a corporate complaint they may do so by emailing complaints@nfdc.gov.uk.

20. REVIEW

20.1. This policy will be reviewed at least every three years and will be updated whenever there is a change in applicable legislation, Codes of Conduct or Guidance. This will ensure the document is fit for purpose and up to date.

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/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version>

‘Guidance on video surveillance’ ICO

[Video Surveillance | ICO](#)