



BRIDGEND COUNTY BOROUGH COUNCIL

CCTV POLICY STATEMENT

1. INTRODUCTION

- 1.1 Bridgend County Borough Council uses Closed Circuit Television (CCTV) systems in public spaces, within car parks and at several Council owned sites across the Borough.
- 1.2 This document, along with individual systems Codes of Practice is designed to give clear guidelines on the Council's use of CCTV and to protect the Council and its CCTV operators from allegations of misuse of the system and to protect staff and the public from any abuse of the CCTV system.
- 1.3 This policy covers the use of CCTV equipment and the gathering, storage, use and disposal of visual data. This policy applies to all staff employed by Bridgend County Borough Council and should be the standard expected from any persons that operate CCTV systems on its behalf.
- 1.4 This document should be read in conjunction with the CCTV systems Code of Practice and Operational Manual. Failure to comply with these documents could lead to disciplinary action, which may lead to dismissal and, in certain circumstances, criminal proceedings against the individuals concerned.

2. OBJECTIVES OF CCTV SYSTEMS

- 2.1 It is important that everyone, especially those charged with operating the CCTV systems on behalf of Bridgend County Borough Council, understands why each system has been introduced and what the cameras will and will not be used for.
- 2.2 Each CCTV system will have its own site or task specific objectives. These will include some or all of the following:

- **Protecting areas and premises used by Council staff and the public.**
- **Deterring and detecting crime 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 staff.**
- **Reducing fear of crime, anti-social behaviour, and aggression.**
- **Protecting Council property and assets.**
- **Maintaining and enhancing the commercial viability of the towns and encouraging continued investment.**
- **Assisting in staff disciplinary, grievance, formal complaints and Health and Safety Investigations.**

2.3 The systems will not be used for any other purpose than those set out in this document without prior consultation with the Council's Chief Executive, Head of I.C.T. or Customer Services Manager and, where appropriate, notification to staff and following consultation with the Trade Unions.

2.4 Cameras will not be used to monitor the progress of staff or individuals in the ordinary course of a lawful business in the area under surveillance. Nor are Managers permitted to use cameras to observe staff working practices, timekeeping or to assist in the day-to-day management of their staff.

2.5 Individuals will only be monitored if there is reasonable cause to suspect a criminal offence or a serious breach of discipline that could amount to misconduct that has been committed or is about to be. Monitoring in these circumstances will require authorisation, possibly a RIPA authorisation.

2.6 The last objective in this list is covered in more detail below.

3. LEGISLATION

3.1 In addition to council policies, procedures, guidelines and Codes of Practice, CCTV and its operation are subject to legislation under:

3.1.1 The Data Protection Act 1998 (D.P.A.).

3.1.2 The Human Rights Act 1998 (H.R.A.).

3.1.3 The Freedom of Information Act 2000 (FOIA).

3.1.4 The Regulation of Investigatory Powers Act 2000 (RIPA).

3.1.5 A brief guide on how each Act affects CCTV operations and some guidance on how to remain within the respective Acts is attached to The Code of Practice, but it will be rare for small building CCTV systems to be required to respond to requests for assistance under RIPA. However, Responsible Officers must understand the corporate procedures set out by the Head of Legal Services regarding RIPA requests.

3.2 It is important that the operation of all Council run CCTV systems comply with these Acts, policies, procedures, guidelines and Codes of Practice. This ensures that Council staff running the CCTV systems, the public and the Council, are protected from abuses of the CCTV systems. The Responsible Officer will be responsible for reviewing all CCTV documentation relating to their system annually or as changes occur, ensuring all information is up to date. The Council's CCTV Manager will assist in this process.

4. RESPONSIBILITY

4.1 Directors or Group Managers will have overall responsibility for CCTV systems used within their Departments. Close supervision rests with the Heads of Service.

4.2 The day-to-day operational responsibility rests with the designated Responsible Officer and the staff who operate the CCTV equipment and handle the data.

4.3 The Council's CCTV Manager is responsible for the day-to-day operation of the Public Space Surveillance CCTV system and acts as the central coordinator and point of contact on all issues relating to CCTV within Bridgend County Borough Council.

4.4 The CCTV Manager will be responsible for ensuring all users are kept up to date on legislation and changes in procedures and will review the Council's Policy and Codes of Practice documents annually.

4.6 THE RESPONSIBLE OFFICER

Is responsible for:

- 4.6.1 The day-to-day operation of the CCTV system within their charge, and the security and accountability of all equipment and media used by their system.
- 4.6.2 Making sure that authorised staff who use the system (the Responsible Officer, their operating team, the CCTV Manager and people authorised to view images) are properly trained to use the equipment and comply with the Code of Practice policies and procedures. They are not to permit any other staff to operate the equipment or view images without authorisation.
- 4.6.3 Act as the first point of contact for inquiries, complaints and requests for evidence. And as the liaison officer for all external and internal contacts.

4.7 CCTV STAFF OPERATING CCTV SYSTEMS

- 4.7.1 Staff 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.
- 4.7.2 They must ensure training is up to date.
- 4.7.3 They are responsible for bringing any faults or misuse of the equipment to the Responsible Officer's attention immediately.

5. PURCHASE AND DEPLOYMENT OF CCTV CAMERAS

- 5.1 Bridgend County Borough Council is committed to respecting people's rights to privacy and supports the individual's entitlement to go about their lawful business. This is a primary consideration in the operation of any CCTV system, although there will inevitably be some loss of privacy when CCTV cameras are installed.
- 5.2 It is crucial, therefore, that serious consideration is given to the necessity for cameras in any given location and the possible impact on the privacy of individuals using those areas where cameras are installed.
- 5.3 Cameras are not to be installed in such a way that they can look into private spaces, such as houses, unless they can be fitted with privacy zones, which block out private areas so that they cannot be viewed or recorded. This doesn't make sense to me!
- 5.4 Covert cameras are not to be deployed into areas used by staff or the public. Cameras should be visible and clearly signed.

- 5.4.1 Bridgend County Borough Council will not use CCTV cameras if there are cheaper, less intrusive and more effective methods of dealing with the problem.
- 5.4.2 Once a decision is made to purchase CCTV cameras, advice should be sought from the Council's Procurement Team to ensure correct procedures are followed.
- 5.5.3 It is a requirement under the Information Commissioners Code of Practice and the new National CCTV Strategy that any equipment purchased is fit for purpose and will meet the objectives set down for the scheme. There is also a clear requirement for all CCTV schemes to have an effective maintenance schedule and Code of Practice. Officers purchasing new CCTV equipment need to ensure these requirements are met.
- 5.4.3 Bridgend County Borough Council does not deploy 'Dummy' cameras as these give a false sense of security. Neither are officers to purchase cameras that can monitor conversation or be used to talk to individuals, as this is an unnecessary invasion of privacy.

6. REDEPLOYABLE CCTV CAMERAS (RCCTV)

- 6.1 Re-deployable CCTV cameras (RCCTV) are used by the Council's main CCTV system, and requests made via the Neighbourhood Management Group. They are to comply with the requirements set out in this Policy Document. The RCCTV cameras will also follow the main Code of Practice, but the Code of Practice will need to include additional information to cover the unique deployment tasks of this equipment to demonstrate:
- Secure anchorage and power supply for the cameras are available, and there are suitable locations for CCTV *in use signs to be displayed*.
 - A Privacy Impact Assessment for each deployment.
 - An Operational Assessment to justify the deployment.
 - A Risk Assessment of the safety of staff deploying the cameras.
 - A checking mechanism to establish whether RIPA authorisation is required and if so that the deployment is: Proportionate, Legal, Appropriate and Necessary.

7. MONITORING

- 7.1 CCTV monitors sited in reception areas are intended to provide live monitoring of reception areas by Departments. It is the responsibility of the Responsible Officer in the Department concerned to ensure those observing the monitors are properly trained, and that the ability to view monitors is restricted to those authorised to **do so**.
- 7.2 Monitoring of other cameras where required will only be carried out by persons authorised by the Responsible Officers.

8. VIEWING IMAGES AND THE PROVISION OF EVIDENCE

- 8.1 The casual viewing or trawling of images is strictly forbidden and must only be done for specific and legitimate reasons.
- 8.2 The provision of evidence, or viewings, will normally be requested by the police or other enforcement agencies or a council department conducting an investigation into criminal activities, disciplinary matters, complaints, grievances or Health and Safety issues.
- 8.3 Enforcement agencies such as the police have a legal requirement to 'seize' any relevant evidence when investigating a crime, and Supervising Officers must comply with their request. But the enforcement agencies are bound by the same rules as everyone else.
- 8.5 Enforcement agencies are not permitted to trawl the Council's CCTV system on the off chance of detecting a crime. They must provide the Responsible Officer with a Crime or Incident number or other such proof that they are conducting a legitimate investigation.
- 8.6 The release of evidence, or permission to view images, can only be authorised by the Responsible Officer or in their absence, the Head of Service or the Group Manager. Where an enforcement agency requests copies of an image, one copy must be made, but there is no requirement for the Responsible Officer to retain or produce any further copies.
- 8.7 If the matter concerns a staff member, there is no automatic right to view or release images. Viewings and images will only be released to an authorised investigating officer following a formal request to the Head of Service, Director or Group Manager.
- 8.8 The Responsible Officer will then hold the relevant footage on the computer's hard drive (but not copy it to disc) and seek authority to

release the images from the Head of Service or Director, the Head of Human Resources, and, when appropriate, the Head of Legal Services, should also be consulted before the images are released to the investigating officer.

- 8.9 It is appreciated that this process may take time, and officers should move quickly to complete the process so that any investigation is not unnecessarily delayed. *To ensure the images are not lost due to retention time, the investigating Officer can formally ask the Responsible Officer to retain the images until the viewing/release of evidence process has been completed. This last doesn't make sense.*
- 8.10 Once authorised, arrangements should be made to enable the investigating officer to view the images and, if necessary, be issued with two copies of recorded material on suitable recording media. Note: Only the Investigating Officer is allowed to view the images at this stage.
- 8.11 The reason for a second disc is that if it is decided to use CCTV images in an employment related hearing, the person being investigated must receive a copy of the images to permit them and their representatives to mount a defence. At the end of the hearing, ALL copies of the images will be collected by H.R., held on file and destroyed once the appeals process and or any Employment Tribunal processes are complete.
- 8.12 Staff who are subject to Council disciplinary, complaints or grievance procedures have the right to request that footage be retained if they believe it will support their defence. The process will be exactly the same as that shown above for the investigating officer.
- 8.13 The Council will not permit viewings or release images to people being investigated by an enforcement agency or in an internal investigation, which may be handed over to an external agency such as the police. The responsibility for investigating and disclosing images to those involved in the investigation is covered by the Police and Criminal Evidence Act (PACE), and the Evidence and Disclosure Act. And prosecuting authorities are required to follow the procedures set out in these Acts. It should be noted that other enforcement agencies will operate under other legislation, but the use of evidence still rests with them.
- 8.14 It is critical that a full and detailed record is kept of all 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 authorising officer.

- The date, time, name, and contact details of the person viewing or removing images.
- The reason for the viewing/issue of images and
- The person who released and received the images' signatures.
- Any media containing images should be uniquely marked and the number recorded for ease of identification.

9. INSURANCE CLAIMS

- 9.1 CCTV involvement in insurance claims falls into two categories. First incidents, which may result in claims against Bridgend County Borough Council and secondly claims involving third parties, normally traffic accidents.
- 9.2 CCTV cameras may be able to assist in incidents that could result in a claim against the Council. When a report is received which may result in a claim, the Officer responsible for dealing with the incident should consider whether CCTV covers the area. If so, they should then ask the CCTV systems Responsible Officer to hold images for that period but this must be done within 28 days from the date of the incident. The Officer dealing with the incident should then follow the procedures for viewing and obtaining evidence, which are set out in section 8 above.
- 9.3 If evidence is issued to the Officer dealing with the incident, they become responsible for the security, safety, and integrity of the images. All recorded media must be stored in a secure place with access limited only to those people involved in the subsequent claim. At the end of the waiting period or after any claim has been dealt with this Officer will be responsible for the destruction of the recorded media by shredding and a record in the form of a signed letter/email to that effect will be kept for a period of 12 months.
- 9.4 Requests for assistance from CCTV cameras in third party claims are increasing especially with regard to traffic accidents. Often it is the person involved in the accident who will contact CCTV and ask either if we have any images or if they can come and view them. Requests of this kind should normally be refused. Instead, members of the public should be advised to contact their insurance company and ask them to write to the Responsible Officer formally, giving as much detail about the incident as possible and requesting assistance. It is also important that it is stressed to the person requesting the information that the letter is received before the overwrite period on the recorder. No other action should be taken at this stage.
- 9.5 If the letter arrives within the recording period, the Responsible Officer should view the images. If the incident was not caught on camera the

insurers or solicitor can be called and informed and the case can be closed. If the letter arrives after the recording period, there will be no relevant images to view and the person requesting the images should be informed.

- 9.6 If relevant images are found on the recorder, the insurance company/ solicitor should be informed and asked if they want a copy. If they do, then they need to be informed that there will be a fee. The fee should be based on the amount of time spent by staff viewing, copying, and processing the images based on the hourly salary rate rounded up to the nearest hour. It should also include post and packaging and the cost of the media supplied. This should then be sent as an invoice to the recipient. No charges will be raised against internal Council requests for assistance.
- 9.7 The images may then be copied and sent to the relevant person accompanied by two copies of a letter reminding them that Bridgend County Borough Council retains 'copyright' over the images, that they are responsible for the security and destruction of the images and that the images may not be used for any other purpose other than the one they were released for. The details of the media released should be included (i.e. U.R.N.) in the letter and they should be asked to sign one copy of the letter confirming they have received the images and accepting the conditions of release. A detailed record of all actions must be maintained. Failure to comply with Bridgend County Borough Council's conditions of release may result in legal action being taken against the person who signed the acceptance letter.

10. SIGNAGE

- 10.1 All areas where CCTV is in use should be clearly signed to comply with the Data Protection Act. This is to warn people that they are about to enter an area covered by CCTV cameras or to remind them that they are still in an area covered by CCTV. The signs will also act as an additional deterrent. CCTV signs should not be displayed in areas which do not have CCTV cameras.
- 10.2 Where 'Covert' cameras have been authorised for deployment, signage will not normally be erected.
- 10.3 The signs should have a yellow background with all writing in clear black print. The sign should carry the CCTV camera and Bridgend County Borough Council logo. The signs, the positioning and the writing should be large enough to enable people to easily read the information.

11. THIRD PARTY ACCESS REQUESTS

- 11.1 Under the Data Protection Act and the Freedom of Information Act members of the public and other organisations have the right to ask to see data held by Local Authorities and other Public Bodies. This data includes visual images captured by CCTV.
- 11.2 As a general principle, access to this data should not be refused. However, there are certain circumstances when it will not be possible to provide images from CCTV - for example, when the images form part of a criminal investigation. In all instances where Access Requests are received, they should be passed onto the Council's Data Information Officer (who has responsibility for dealing with Access Requests/F.O.I), before CCTV images are released.

12. RECORDING SYSTEMS

- 12.1 The majority of the Council's CCTV recording systems are digital, although one or two are still analogue.
- 12.2 All staff required to operate CCTV equipment are to receive training in the use of the equipment and must conform to this Policy Document and their systems Code of Practice at all times. Staff who operate the recorders will be required to sign a 'Confidentiality Statement', which prohibits them from making any material available for purposes other than those stated in the Code of Practice. Any other staff having access to the equipment will also sign a Confidentiality Statement. Once signed, the Confidentiality Statement should be kept on file.
- 12.3 **EXCEPT FOR EVIDENTIAL PURPOSES IMAGES WILL NOT BE COPIED IN WHOLE OR PART**
- 12.4 Recorded material will not be sold or used for commercial purposes or 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.
- 12.5 Recording equipment and recording media will be kept in secure accommodation and no access will be granted to unauthorised staff.
- 12.6 All images will remain the property and copyright of Bridgend County Borough Council.
- 12.7 Each new recording disc/tape must be clearly marked with a unique reference number in indelible ink before it is brought into operation.

- 12.8 All media will be disposed of securely when no longer in use.

13. DISCIPLINARY OFFENCES AND SECURITY

- 13.1 Tampering with or misuse of cameras, monitoring, or recording equipment, images, or recorded data by staff may be regarded as misconduct and could lead to disciplinary action, which may result in dismissal or criminal prosecution.
- 13.2 Any breach of this Policy Document or the CCTV Code of Practice will be regarded as a serious matter. Staff that are in breach of these instructions will be dealt with according to the Council's disciplinary procedures.
- 13.3 The responsibility for guaranteeing the security and proper use of the system will rest with the Responsible Officer of the system concerned. These officers will, in the first instance, investigate all breaches or allegations of breaches of security or misuse and will report his/her findings to their Head of Service and Director.

14. STATISTICS

- 14.1 CCTV installation like any other purchase by a Local Authority is spending public money and needs to be justified. CCTV systems are required to show how effective the cameras are in dealing with the objectives set out for their use.
- 14.2 Responsible Officers will be required to submit an annual set of statistics showing the effectiveness of their systems to their Head of Service with a copy being sent to the Council's CCTV Manager.

15. INSPECTIONS/VISITS

- 15.1 All CCTV systems may be subject to inspections or visits by a member of the Information Commissioners Office or the Regulation of Investigatory Powers Commissioner. In addition, systems may also be subject to visits/inspections by Members, Directors, Heads of Service, or the Council's CCTV Manager.
- 15.2 These visits/inspections are designed purely to ensure that the Systems are being run in accordance with current legislation, this Policy Guideline, their own Codes of Practice, and to offer advice for improvement where required.

16. HEALTH AND SAFETY

- 16.1 The Responsible Officer is to ensure that staff are made aware of and comply with all Council policies on Health and Safety. In particular, they are to be aware of policies relating to working with electrical equipment, and VDU Regulations.

17. COMPLAINTS

- 17.1 Complaints about the operation of a CCTV system should be addressed initially to the Customer Services Manager. Complaints will be dealt with in accordance with the Council's formal complaints procedure.

18. FURTHER ADVICE/INFORMATION

- 18.1 Further advice on CCTV related matters may be obtained from the individuals and organisations shown below:
- General advice from their own line managers.
 - Advice on CCTV issues from the Council's CCTV Manager.
 - Legal Advice and RIPA from the Head of Legal Services.
 - Advice on issues affecting staff from the H.R. Department.
 - Third Party Access/F.O.I. Requests from the Council's Data Information Officer.
 - Health and Safety advice from the Health and Safety Advisor.
 - Technical advice and training on individual systems from Systems Installer and the Council's CCTV Manager.

