Appendix 'D'

Closed Circuit Television (CCTV) Policy 2017

Lancashire County Council

www.lancashire.gov.uk

Closed Circuit Television Policy 2017

The following policy relates to surveillance camera equipment and the gathering, storage, use and disposal of CCTV system recorded data. The council uses surveillance camera devices for various purposes. These include CCTV systems within council premises and car parks as well as on the highway, body worn video camera equipment, automatic number plate recognition and unmanned aerial vehicles (drones). In this policy, such devices shall be referred to as 'CCTV systems'.

This policy covers all CCTV systems used by Lancashire County Council but does not cover Lancashire schools.

Lancashire County Council is referred to as 'the council' throughout this policy.

This document should be read in conjunction with following codes of practice for surveillance cameras:

- Surveillance Camera Code of Practice and 12 Guiding Principles 2013
- In the picture: A data protection code of practice for surveillance cameras and personal information 2015 – Information Commissioners Office (ICO)
- National Surveillance Camera Strategy for England and Wales 2016

Details of all CCTV systems, policy documents, legislation, procedures and templates can be found on the council's CCTV intranet page.

Definitions

Camera	Any device used as part of a CCTV system. This includes unmanned aerial vehicles (drones).
CCTV	Closed Circuit television.
CCTV System	Any system or device used by the council to monitor an area including CCTV, cameras used on the highway, body worn camera devices or unmanned aerial vehicles.
Image	Any image captured by a CCTV system.
Overwrite Period	The period between an image being recorded and it being automatically deleted from the CCTV system.
Responsible Officer	The officer with responsibility for a specific CCTV system in operation, usually a premises manager.
CCTV Manager	The officer with responsibility for CCTV policy and its use throughout the council.

1. Introduction

1.1. Use of cameras and other electronic recording devices in public places has escalated over recent years and the advance of technology has meant that the variety of devices available has expanded. Whilst these perform a

useful role in preventing and detecting crime and keeping people and property safe, such use has led to much greater intrusion into the private lives of individuals going about their lawful business. This policy aims to set out standards relating to the use of such equipment that maximises effectiveness whilst at the same time minimises interference with the privacy of individuals whose images are captured by the devices.

1.2. Officers undertaking covert surveillance with or without recording devices must comply with the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Codes of Practice issued pursuant to that legislation. This policy does not apply to such activities.

2. Objectives

2.1. It is important that everyone and especially those charged with operating the CCTV systems on behalf of the council understand exactly why each of the CCTV systems and each camera used as part of a CCTV system has been introduced and what the cameras should and should not be used for.

2.2. Each CCTV system will have its own site or task specific objectives. These could include some or all of the following:

- Protecting areas and premises used by council officers and the public.
- Deterring and detecting crime and anti-social behaviour.
- Assisting in the identification of and apprehension of offenders.
- Deterring violent or aggressive behaviour towards council officers.
- On-site traffic and car park management.
- Monitoring traffic movement.
- Identifying those who have contravened parking regulations.
- Assisting in traffic regulation enforcement.
- Protecting council property and assets.
- Assisting in grievances, formal complaints and investigations.
- Surveying buildings for the purpose of maintenance and repair.

2.3. CCTV systems must not be used to monitor the activities of council officers or members of the public in the ordinary course of their lawful business. Council officers are not permitted to use CCTV systems to observe the working practices and time keeping of other council officers.

3. Legislation

3.1. CCTV systems are subject to legislation under:

- The Data Protection Act 1998 (DPA).
- 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
- The Criminal Procedures and Investigations Act 1996

4. Responsibilities

The CCTV Manager

4.1. The CCTV Manager is responsible for ensuring all those involved in the use of CCTV systems can view current legislation and guidance relating to CCTV systems. This is done through the council's CCTV intranet page.

4.2. The CCTV Manager will review the CCTV policy annually.

4.3. The CCTV Manager will take the CCTV policy to the Corporate Information Governance Group (CIGG) to receive policy approval.

4.4. The CCTV Manager will submit an annual report to the Senior Information Risk Owner (SIRO) detailing how effective, in the previous year, CCTV systems have proved to be, in meeting the objectives listed in Section 2.

The Responsible Officer

4.5. The day-to-day operational responsibility for each CCTV system rests with the designated responsible officer at each council building. The responsible officer will likely be the premises manager. A list of all CCTV systems and their responsible officer will be recorded and available in a CCTV register on the council's CCTV intranet page. This will also be the case when a third party under the direction or control of the council operates the CCTV system.

4.6. The responsible officer shall ensure that council officers involved in the operation of the CCTV system are trained in the use of the equipment and are aware of this policy and the procedures in place to manage CCTV systems at the council.

4.7. The responsible officer should act as the first point of contact for all enquiries relevant to the CCTV system in their premises and should ensure that only authorised council officers are able to operate or view images.

4.8. The responsible officer shall investigate any reported misuse of a CCTV system and report it immediately to the CCTV Manager.

4.9. The responsible officer shall report any faults in the CCTV system equipment to the CCTV Manager and take steps to remedy the fault at the earliest opportunity.

5. CCTV Operations

5.1. Council officers operating CCTV systems are responsible for operating the equipment in accordance with all requirements set out in current legislation, this policy document, relevant guidelines, codes of practice and local operational manuals.

5.2. Council officers operating CCTV systems must be familiar with the requirements of information governance and should complete the councils IG eLearning course. Heads of Service shall take steps to ensure that any council officers that they manage who are involved in operating CCTV systems have completed this training.

5.3. Council officers involved in the use of CCTV systems shall report any misuse to the responsible officer and shall cooperate with any investigation by the responsible officer. The responsible officer shall investigate any reported misuse of a CCTV system and report it immediately to the CCTV Manager.

5.4. Council officers operating CCTV systems shall be responsible for bringing any equipment faults to the responsible officer's attention immediately.

5.5. A number of council owned CCTV systems are located in premises occupied by third parties. In these cases, it is important that there is a clear understanding between the council and the organisations concerned as to who is responsible for each aspect of the CCTV system. This should be recorded and signed by both parties. A copy of this document should be given to the council's CCTV Manager.

6. Purchasing and Deployment of CCTV Cameras

6.1. It is advisable when purchasing CCTV systems to purchase from suppliers that are registered with the Surveillance Camera Commissioner's Third Party Certification Scheme. Certification enables organisations to demonstrate that they use their CCTV systems transparently, effectively and proportionately.

6.2. It is advisable that third party data processing contracts are in place with third party CCTV system suppliers to ensure that the suppliers protect the data to the council information governance standards.

6.3. Those responsible for introducing and operating CCTV systems must ensure that the use of cameras is proportionate to the intended objective and that individuals' right to privacy is respected at all times. A clear operational objective for the CCTV system must be identified and an assessment on the impact on privacy must be carried out and reviewed each year. A template 'privacy impact assessment' can be found on the council's CCTV intranet page. A 'privacy impact assessment' must be completed for each CCTV system in use within the council.

6.4. Care must be taken to ensure that cameras do not capture images or sounds of private spaces such as dwelling houses.

6.5. Covert cameras are not permitted to be deployed under the auspices of this policy. Such activities fall under the ambit of RIPA or shadow RIPA and authorisation must be obtained for such activity under the relevant RIPA procedures. CCTV systems should normally be clearly visible with unobstructed signage situated close to the device informing those in the vicinity that they are being monitored and/or recorded. The content of such a sign or notice may differ according to the nature of the device being used, the area it is being used in and the purpose of its use.

6.6. All costs associated with CCTV systems are covered under the council's scheme of delegation.

6.7. The council does not deploy ‘dummy’ cameras as part of its CCTV systems as these can provide a false sense of security.

6.8. The council does not generally operate cameras that can monitor conversation or be used to talk to individuals as this is seen as an unnecessary invasion of privacy. This does not apply to body worn camera devices.

6.9. Upon the introduction of a static CCTV system, a copy of the location of the camera should be sent to the CCTV Manager for inclusion in the council’s central register of CCTV systems. Use of CCTV systems should be considered as part of planning a building construction or refurbishment. Authorisation for the deployment of CCTV systems should be shared at an early stage in building design with the Head of Service for whom the building is being constructed. This is so that this policy can be applied and either an alternative method adopted or an acceptable CCTV system built into the designs. Information about the CCTV system should be retained as part of the file relating to the completed building.

7. Monitoring

7.1. CCTV system monitors sited in reception areas are intended to provide live monitoring of reception areas by security or other council officers. The ability to view the CCTV system monitors must be restricted to those authorised to see them. Monitors must not be visible to all entering the premises.

7.2. Monitoring of CCTV systems where required will only be carried out by persons authorised by the relevant responsible officer.

7.3. CCTV will only be subject to the Data Protection Act 1998 if the footage captured “relates to living individuals who can be identified” from it.

7.4. If the Data Protection Act 1998 does apply, the CCTV operator will be required to do a number of things:

- Register as a data controller with the Information Commissioner's Office. The council has already done this, it's registration number is Z542705X
- Put up signs notifying people that CCTV is in use and who operates it.
- Give any individual who requests it, copies of footage of themselves. (Subject Access Request).
- Ensure that any footage stored is kept for no longer than necessary for the purposes for which it is obtained.
- Ensure that footage is not disclosed to anyone else without the consent of the individuals shown in it unless it is for a reason permitted under the Data Protection Act 1998, such as the prevention or detection of crime.

7.5. In addition to the obligations under the Data Protection Act 1998, the Human Rights Act requires any public authority using CCTV cameras to do so compatibly with Article 8 of the convention.

7.6. The council occasionally uses body worn cameras in order to protect council officers dealing with members of public in situations where they are particularly vulnerable to abuse or where there is an ongoing need to capture images or speech for evidential purposes. An example of this is Civil Enforcement Officers. Officers using body worn cameras must only activate them when there is a need to do, for example, if they consider that a member of the public is becoming abusive or may challenge evidence that could be recorded using the camera. Continuous recording is not permitted, as it is excessive and would cause a great deal of collateral intrusion.

7.7. Details of CCTV systems data collection should be included in the council's privacy notice: http://www.lancashire.gov.uk/about/privacy-statement.aspx

8. Viewing Images

8.1. The casual viewing or trawling of images or sounds captured by a CCTV system is strictly forbidden. Viewings must only be carried out for a specific, legitimate purpose.

8.2. Under Section 7 of the Data Protection Act 1998, data subjects are entitled to know what personal data the council holds about them and they are entitled to receive a copy of their personal data. All such requests, known as **Subject Access Requests**, must be made through the council's Information Governance Team at dataprotection@lancashire.gov.uk.

8.3. Under the Freedom of Information Act 2000, people can request access to any recorded information (with certain exemptions) that the council holds. However, if individuals are capable of being identified from the CCTV system footage then it is personal information about the individual concerned and is unlikely to be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the Data Protection Act 1998. All **Freedom of Information requests** relating to CCTV system images should be directed to the council's Information Governance Team at freedomofinformation@lancashire.gov.uk.

8.4. On occasion **council services may wish to access images and recordings captured on CCTV systems as part of a legitimate investigation** into criminal activities, civil claims, potential disciplinary matters, complaints, grievances or health and safety issues. Viewings and images will only be released to a properly authorised investigating council officer upon the submission of a formal request to the CCTV Manager via cctv@lancashire.gov.uk. The viewing request should include:

- The name of the authorising officer (CCTV Manager, responsible officer, Head of Service)
- The name and contact details of the person viewing images
- The reason for viewing the images

Viewing Requests should be made in a timely manner as the retention period for most CCTV systems in operation in the council is 6 weeks. Council officers who are subject to council disciplinary, complaints or grievance procedures have the right to see and retain footage of themselves and can request copies as a Subject Access request via the Information Governance Team at dataprotection@lancashire.gov.uk.

8.5. On occasion, **police officers may request to view images taken from CCTV systems during the investigation of criminal activity**. This is acceptable under the Data Protection Act 1998 (Section 29). However, the police officer making the request must complete a DP1 form (available on the council's CCTV intranet page) confirming that the information is needed for the detection or prevention of a specific crime. The form must be signed by a senior police officer and returned to the council's Information Governance Team at dataprotection@lancashire.gov.uk. Police officers are not permitted to trawl the council's CCTV systems on the off chance of detecting a crime.

8.6. Occasionally **insurance companies or solicitors will request footage, generally over disputes regarding damage to cars in car parks**. As the footage may identify the individual drivers or vehicles involved it is classed as personal information. Copies of personal information can be requested making a Subject Access Request under the Data Protection Act, 1998 to dataprotection@lancashire.gov.uk. Ordinarily you are only entitled to information about yourself; however, in certain circumstances it is

reasonable to include information about third parties, and this is permitted by the Data Protection Act. Such circumstances may include where a third party has caused damage to you or your vehicle. All such requests must be made through the council's Information Governance Team, who log all such requests and who may need to redact third party information.

8.7. A record of all disclosures is kept in the council case management system Norwel.

9. Signage

9.1. All areas where CCTV is in use should be clearly signed. Such signs warn people that they are about to enter an area covered by a CCTV system or to remind them that they are still in an area covered by a CCTV system. Signs will also act as an additional deterrent. CCTV system signs should not be displayed in areas that do not have CCTV cameras.

9.2. Signs should alert road users to CCTV systems operated in connection with highways management or enforcement activity. Such signage will also be subject to additional requirements under the relevant road traffic or highways legislation. It is important that these signs do not affect the safety of road users.

9.3. Where body worn cameras are in use, officers using them must display a clear notice that this is the case on their person, usually as part of their uniform. This notice should not be covered up or obscured but should be visible at all times during an interaction that is being recorded or may be recorded. Where there is doubt that a member of the public is aware of this, officers should make it clear that they are wearing body worn cameras.

9.4. Signs should be an appropriate size depending on context. For example, whether they are viewed by pedestrians or car drivers.

9.5. Signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a CCTV system. This is particularly important when an ANPR system is being used that covers a large area.

9.6. Unmanned Aerial Vehicles (drones) act as a safe and effective method of surveying buildings but whilst photographing parts of buildings from above, they also capture the images of passing individuals. Some thought should be given to whether signs should be erected on a temporary or permanent basis where drones are in use for buildings maintenance. This may be advisable in relation to buildings where such activity is carried out regularly or routinely. In other circumstances, the potential use of temporary removable signs should be considered if practical.

9.7. Signs should:

- Be clearly visible and readable;
- Contain details of the organisation operating the system;
- The purpose for using the surveillance system;
- Contact details such as a simple website address, telephone number or email address.

10. Storage and Retention

10.1. CCTV system images are stored for 6 weeks and then overwritten.
10.2. Recorded material will not be sold or used for commercial purposes.
10.3. CCTV systems will be kept secure from unauthorised access.
10.4. All images remain the property and copyright of the council.
10.5. All images are stored on secure servers.
10.6. Each new recording disc will have a unique reference number.
10.7. All images are time and date stamped.
10.8. Image resolution should be relevant to purpose.
10.9. All media will be confidentially disposed of when no longer needed.
10.10. No CCTV system images will be stored in the Cloud
10.11. No CCTV system images will ever be published to the Internet

11. Inspections

11.1. CCTV systems at the council can be inspected at any time by:

- The CCTV Manager.
- The relevant responsible officer.
- The relevant Head of Service.
- Any of the CCTV specialist advisors named in Section 14 of this policy.
- A member of the Information Commissioners Office.
- A member of the Surveillance Camera Commissioners Office.
- The council's senior management team or elected members.

11.2. Spot checks and audits of the council's CCTV systems will take place sporadically.

12. Health and Safety

12.1. The relevant responsible officer or relevant Head of Service should ensure that officers are made aware of and comply with all council policies on health and safety, in particular, working with electrical equipment, VDU regulations and working with heights.

13. Complaints

13.1. Any complaints regarding CCTV systems at the council should be directed to the relevant responsible officer, the relevant Head of Service or

CCTV Manager or the Corporate Complaints Team. All complaints will be dealt with in accordance with the council's complaints procedure.

14. Contacts

14.1. CCTV Manager: Paul Bond
14.2. CCTV IG Advisor: Debbie Bonser
14.3. CCTV Legal Advisor: Laura Sales
14.4. CCTV Facilities Advisor: Andrew Clarkson
14.5. CCTV Audit Advisor: Judith Taylor

Version Control

Named Owner:	Ian Young - Senior Information Risk Owner (SIRO) Paul Bond – CCTV Manager
Version Number:	1.00
Date Of Creation:	November 2016
Last Review:	November 2016
Next Scheduled Review:	November 2017
Overview of Amendments to this Version:	