CCTV SYSTEMS

POLICY AND CODE OF PRACTICE DOCUMENT

CENTRAL SECURITY SERVICES

New policy Sept 2017

Review date Sept 2019

SUNDERLAND CITY COUNCIL

POLICY FOR THE USE OF CCTV SYSTEMS

1. This document sets out the Council's Policy and Code of Practice on the use of CCTV systems.

2. The Council acknowledges that the use of CCTV systems can play a significant part in reducing crime, the fear of crime and anti social behaviour. The Council will use and operate CCTV systems in accordance with the Data Protection Act, 1998 and all relevant guidelines. A summary of the Data Protection Act is attached as "Appendix 1" of this document. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the conduct of 'covert' and 'directed' surveillance and this is the subject of a separate guidance document.

3. Council CCTV systems will form part of the Council's data protection registration.

4. CCTV Applications and Uses (Overt and Covert)

   CCTV may be used in the following circumstances:-

   - To monitor Council buildings and locations to reduce crime and risk to staff and others using overt systems.

   - To secure evidence against persons who carry out criminal and anti social acts to the detriment of the Council's property, employees, or inhabitants of the Council's area in public places using overt or covert systems as appropriate.

   - To secure evidence where the activities of employees may constitute criminal conduct using covert systems. A policy on this aspect was agreed by the Personnel Sub-Committee on 2nd July 1997. A copy of this document is attached as "Appendix 2" of this document.

5. Right to Privacy

   The Council recognises its obligations under the Human Rights Act 1998 and in particular the individual's right to privacy is acknowledged as a vital consideration for all areas of CCTV usage.

6. Responsibilities

   - The Office of the Chief Executive will be responsible for the implementation of the attached Code of Practice for the use of CCTV Systems and for ensuring compliance.

   - Council Departments will liaise with the Security Services Manager regarding all current and future CCTV systems, to ensure efficiency and compliance with the code.

7. Accountability

   The Security Services Manager will prepare an annual report on the operational

status of all CCTV systems. The report shall include information showing a summary of all CCTV activities and results.

CCTV
CODE OF PRACTICE

New policy Sept 2017

Review date Sept 2019

THE USE OF CCTV FOR OVERT SURVEILLANCE
CODE OF PRACTICE

General Principles

1.0 This code of practice is to provide the strict basis for operational requirements for the use of CCTV systems. It should be read in conjunction with the Council's Policy Statement for the Use of CCTV Systems together with Data Protection Act 1998 (The 1998 Act) which directly relates to CCTV recording (see Appendix 1).

1.1 When the use of CCTV for covert surveillance is 'directed' the procedures for authorisation must be followed. These are detailed in a separate guidance note which complies with the Regulation of Investigatory Powers Act 2000 (The 2000 Act).

1.2 The purpose of the use of CCTV equipment is to assist with the prevention and detection of crime and anti social behaviour together with reducing risk to Council buildings, locations, staff and users. All systems will be subjected to internal Council registration (Appendix 3).

1.3 Sunderland City Council supports the individual's right to privacy and acknowledge that this is a vital consideration with regard to public CCTV systems.

1.4 Sunderland City Council fully supports the use of CCTV systems but the support is conditional upon there being appropriate consultation as well as compliance with any relevant legislation and official guidelines of relevance.

1.5 Paragraphs 2 to 8 below describe the procedures that the Council will adopt for Overt Surveillance. Paragraph 9 summarises the requirements of the Regulation of Investigatory Powers Act 2000.

2.0 Fairness

2.1 Individuals must be made aware that they are about to enter an area where CCTV video recording is active. This will be achieved by prominent signage placed at the entrances of buildings or the perimeter and approaches of an open or less well defined area. The Council's name must be apparent. (This will not apply in the case of covert recording. (See 9.0 below). All signage will be compliant with Data Protection Act guidelines. Advice on wording, size and siting of signage must be obtained from Security Services (signs and template available).

3.0 System Installing and Camera Positioning

3.1 The installation and use of all CCTV systems will be subject to agreement by the Office of the Chief Executive, Security Services.

3.2 The siting and re-siting of Digital Video Recorders, cameras and monitors will be subject to agreement with the Office of the Chief Executive, Security Services.

DVR's must be stored in suitable, secure cabinets within a lockable office or cupboard together with the required CCTV Register and logs. The cabinet should be fitted with a cooling system and an Uninterruptible Power Supply (UPS) to ensure optimum operating conditions for the equipment.

3.3 Views of residential properties and non-Council locations will, as far as possible, be excluded from the field of vision. Every effort must be made to prevent close up views into windows of living accommodation. Advice on how this can be achieved, by either physical or electronic measures, will be given by Security Services.

3.4 The installation of CCTV in public places shall be carried out in consultation with Northumbria Police through the Office of the Chief Executive, Security Services and any relevant partners.

3.5 'Directed' surveillance of persons, buildings or vehicles in public places shall only be undertaken after detailed consultation with the Office of the Chief Executive, Security Services and appropriate officers of Northumbria Police. Any Authority for 'Directed' surveillance will only be granted in accordance with the Regulation of Investigatory Powers Act.

4.0 **Control of Operation of Cameras**

4.1 Operators and monitors of CCTV equipment must act with the utmost probity.

4.2 Only staff with responsibility for using the system shall have access to operating equipment and must have access to a clear statement of the objectives of the system contained in the CCTV Registration Form and responsibilities of those involved in its operation and management.

4.3 All use of the equipment shall accord with the purposes of that individual system and shall fully comply with this code of practice.

4.4 Cameras must not be used so as to look into private property.

4.5 Systems operators should be subject to supervision procedures to ensure compliance.

5.0 **Digitally Recorded Material**

5.1 Digitally recorded material will be recorded for no more than 31 days with equipment programmed to automatically overwrite data thereafter.

5.2 No unauthorised access is to be allowed to digital recordings.
All requests for access should be made to the Council's Security Services Manager who must be satisfied that access is for proper purposes.

6.0 **Evidential Use of Recordings**

6.1 Requests to download digitally recorded materials shall be made to the Security Services Manager and/or the City Alarm and Emergency Centre who can facilitate this service.

6.2 CDs required for evidential purposes shall be individually packaged, sealed and securely stored.

6.3 Any CD that is provided for evidential purposes must be of proven integrity and accountable through the CCTV register.

7.0 **Access to Recorded Material**

7.1 Recording equipment must be secured in a lockable enclosure.

7.2 Access to digital recordings will be restricted to those who have day-to-day responsibility for the system and those directly concerned with achieving the objects of the system.

7.3 The Police may apply for access to recordings where they believe that access to specific images is necessary for the investigation and detection of a particular offence(s) or for the prevention of crime.

7.4 All requests for Data must be made in association with, and comply with the requirements of the Data Protection Act, Codes of Practice and other relevant legislation.

Any request for Data by the Police or other person / organisation must be made on the 'Request to View' form or the Northumbria Police form DPA1/2 and directed to the Security Services Manager and / or CAEC before a download is commenced.

8.0 **Subject Access**

8.1 Under the Freedom of Information Act 2000, an individual may request a copy of any recording that exists of them; this would normally be in the form of a recording on a digitally recorded CD. They may also request a description of the purposes of the recording.

8.2 The system owner's / manager's rights are that:

- The request is made in writing.
- Sufficient information is provided in order that she or he can satisfy her or himself of the identity of the individual.
- Sufficient information is provided to locate the relevant recording, a specific date and reasonable time window.
- He / she has up to 40 days to respond.
- He / she may continue with the established recording management routine.
- He / she may charge a fee up to the statutory maximum (currently £10 but, under review).

8.3 If the system owner / manager cannot comply with a request without disclosing identifiable images of third parties she / he is not obliged to comply with the request. If however, the third parties have given consent, or it is reasonable in all circumstances to comply without consent she / he may comply.

All requests for subject access will be made to Security Services.

9.0 **Covert Recording**

9.1 An exemption to Section 29(1) of the Data Protection Act allows personal data processed for reasons of prevention or detection of crime or the apprehension or prosecution of offenders to be obtained without signs providing that the following criteria is met:

- The Council have assessed that if the individual (s) were informed that recording were taking place then it would prejudice the objective.
- The Council have reasonable cause to suspect specific criminal activity is taking place.
- That covert processing is only carried out for a limited and reasonable period of time and relates to the specific suspected criminal activity.

9.3 Where covert recording is to be adopted, authorisation must be obtained from an Assistant Chief Officer or designated officers with delegated powers in accordance with the requirements of the Regulation of Investigatory Powers Act 2000 for covert surveillance as described in the separate guidance note.

10.0 **Complaints**

10.1 All complaints about the operation of Council CCTV systems will be dealt with under the Council's normal complaints procedure.

THE DATA PROTECTION ACT 1998

New policy Sept 2017

Review date Sept 2019

“APPENDIX 1”

THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 relates to data processing of all types. The definition of data under the Act includes information which is being processed by equipment operating automatically in response to instructions given for that purpose or is recorded with the intention that it should be processed by means of such equipment.

The definition of Processing is much wider in its scope than previous legislation and includes obtaining, recording or holding information or data, or carrying out any operation or set of operations on the data, organisation of the data by transmission, dissemination, or otherwise making available, alignment, combination, blocking, erasure or destruction.

Data in the case of CCTV recordings is in the form of recorded images of individuals that can be identified from these images.

Having regard for these definitions, it will be recognised that the use of CCTV for surveillance purposes is encompassed by the requirements of the Data Protection Act.

The Data Protection Act principles which the Council, as a data controller, must comply with (unless a specific exemption applies) are set out in Schedule 1 of the Act and may be summarised as follows:-

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specified and lawful purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and where necessary, kept up to date.

5. Personal data shall not be kept for longer than is necessary.

6. Personal data shall be processed in accordance with the rights of data subjects under the act.

7. Appropriate measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or damage to it.

8. Personal data shall not be transferred to a country outside the European Economic Area without adequate safeguards.

The Office of the Chief Executive and Security Services Manager has responsibility to ensure that the Council fully complies with the Data Protection Act with regard to CCTV operations.

"**APPENDIX 2"**

PERSONNEL SUB-COMMITTEE

2ND JULY 1997

Criminal Conduct – Surveillance

Report of the Chief Executive, Director of Administration and Director of Personnel

1. Purpose of Report

1.1 To establish a framework for the use of surveillance equipment (CCTV) involving the investigation, as part of the Council's disciplinary procedures, of alleged criminal conduct by employees.

2. Background

2.1 In exceptional circumstances it is necessary to use surveillance equipment (CCTV) to secure evidence where the activities of employees may constitute criminal conduct. The Local Conditions of Service already set out the procedures to be followed when contacting the police in serious disciplinary matters.

2.2 Although the usage of surveillance equipment in such cases is extremely rare, it is proposed to set out a framework for the guidance of Chief Officers in future. The framework is designed to cover the circumstances in which the equipment will be used, the authorisation arrangements, safeguards for the employees involved and the subsequent use and security of any evidence collected.

3. Proposed Framework

The proposed framework is as follows:

i) The surveillance equipment will only be used where criminal conduct is suspected;

(ii) The surveillance equipment will only be used where it is considered necessary to secure relevant evidence;

(iii) Requests to use such equipment by Chief Officers will be made to the Chief Executive, who will authorise the use of the equipment, in consultation with the Chairman of Personnel Sub-Committee.

(iv) The installation of the equipment will be arranged by the Director of Development and Regeneration, Security Services.

(v) In cases involving theft, fraud or embezzlement, the Head of Corporate Finance will also be consulted;

(vi) Any recordings made will become the responsibility of the Chief

Officer who will be required to ensure secure storage;

Continued…….

vii) Access to the recordings made will be strictly controlled and will only be made available to those who have a right to see it, including the police.

viii) Should disciplinary action be pursued, any evidence collected will be made available to the employee, as soon as practicable, within the terms of the disciplinary procedures.

(ix) Any recordings which are not required as evidence will be destroyed immediately.

(x) Any evidence collected will be stored for a period of twelve months or until appropriate procedures and processes have been exhausted, which ever is the longer, at which point it will be destroyed.

4. Recommendation

4.1 The Sub-Committee is requested to approve the framework as set out in paragraph 3.

CCTV SYSTEM REGISTRATION FORM

New policy Sept 2017 Review date Sept 2019

"APPENDIX 3"

CCTV SYSTEM REGISTRATION FORM

To be completed by the Head Teacher;

All CCTV systems should be registered under the Data Protection Act with the Data Commissioners Office. This is done on an annual basis in conjunction with the renewal of the normal Data registration scheme. Simply add the fact that the school has a CCTV system onto the registration form. There are no additional fees in respect of this addition on the Registration form.
It is recommended that the following document be completed and attached to the relevant CCTV File / Folder so if required, a formal document can be provided to show the purposes etc of the system and support the integrity of it.

3.01 Introduction

Closed Circuit Television System installed at: Hetton School, North Road, Hetton le Hole. DH5 9JZ

The System will be operated in accordance with the City Council's CCTV Code of Practice.

The Data Manager is :- Michelle Brannon

The System is overseen by : Dan Turner, School Business Manager
Other Key Personnel (Authorised operators) are :

Name	Job Description
Craig Knowles	Acting Headteacher
Stephen Ferguson	Senior Leader
Jane McKeown	Assistant Headteacher
Keith Woods	Network Manager

3.02 Objectives

- ✓ To assist in the detection of crime
- ✓ To provide evidence of crime
- ✓ To deter those having criminal intent
- ✓ To give confidence to staff and visitors that they are in a secure environment
- ✓ To provide information relating to vehicle traffic management

3.03 System

The system consists of the primary items of equipment listed below:

Tick

☑ Fixed position cameras *Number Internal 25, External 7*

☐ Fully functional cameras (pan, tilt and zoom external) (Number 0.)

☐ Covert cameras (Number 0)

Camera Type ☐ IP / Network ☐ Hardwire

Viewing monitor ☐ Stand alone ☐ Network Link to Desk Top

Public Awareness Monitor ☐

☑ Multiplexer – *housed in Server room*

☑ Digital Video Recorder ☑ Number 1 ☐ Keyboard

☐ Download / Archive / Copy facilities

☐ DVD / CD burner USB/PC ☐ other ☐

☐ External Monitoring by CAEC.

☑ Public information signage re CCTV monitoring : *placed at every entrance*

3.04 Recording Management

The recording system is:-

tick

☑ DIGITAL FREE STANDING HARD DRIVE
Please state make & model…Hikvision 32 channel DVR

☐ PC BASED HARD DRIVE
Please state operating system / software programme
(Internal) Windows XP

☐ System Password Protected

3.03 Operations Manual

An operations manual relating to the specific items of equipment has been compiled by the installer of the system and is located for internal cameras in Room

number P003 (rear of main office) drawers, and for external cameras in the Safe room.

It is the responsibility of the system manager to ensure that staff are aware of the function and capable of operating the various items of equipment within the system.

3.04 General Principles

The principles detailed in the CCTV Code of Practice will be observed in the operation and management of the system.

3.05 CCTV Register

A CCTV register will be maintained incorporating the following sections:-

1. Digital Recorder (make, model, hard drive space), recording rate and period (i.e. 25 frames per second and 28 days or otherwise)
2. Incident Report
3. Operator Duty Log
4. Visitor Log
5. Repairs and Maintenance
6. Copy of Data Protection Act & CCTV Codes of Practice
7. Request To View Form

A loose-leaf file is recommended which will cover the 7 sections.
(See Appendix 4-8)

3:06 System Checks

The functionality of the cameras and recorder including the time and date display (as appearing on screen) must be regularly checked for faults and accuracy.
All faults must be reported immediately and rectified in accordance with the Maintenance Agreement.

3:07 Incident Reporting

An Incident Report will be completed for each incident requiring investigation.

The original evidence CD will be inhibited from being recorded over and then placed in a tamper evident secure evidence bag together with the original of the incident report.

The evidence bag will be held in either the CAEC or handed to Northumbria Police for retention.

3:08 System Maintenance

The maintenance of the CCTV System is not currently under contract with any external supplier.

Service / repair to the system is available through EDL who installed the system.

Any fault, call out or routine maintenance visit will be reported in the CCTV Register.

NB
Engineers required to work on the system MUST sign in on the Visitor Log

3:09 Visitors

3:9:01

Visitors to site having any connection with CCTV system i.e. Police, Service Engineers, Members of the Public, in connection with a Subject Access request, previously agreed with the System Manager must log on and off site in the CCTV Register.

Signed_____

Dated_____

Appendix 4

Incident Log

Time/Date	Description of Incident	Action Taken	Signed

Appendix 5

Operator Log

Time / Date	Name of Operator	Reason for Use	Signature

Appendix 6

Visitor Log

Time/Date	Name and Address	Reason	Operator	Signature of Visitor

Appendix 7

Repairs and Maintenance Log

Time / Date Fault Notified	Nature of Fault	Time/Date Repaired	By Whom	Company name	Operator Signature

Appendix 8

CCTV DATA DOWNLOAD LOG

Time & Date of Download	..... am/pm…../…../2010
Request to View DPA 1/2	Received Y / N
Date of Incident	……../……./ 20…..
Times between	……and……

Camera No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
DVR NO																
1																
2																
3																
4																
5																
6																

Download completed by:	Name:…… Signature……
No of Discs:	…….
Handed to:	Name:……. Rank & No.…… Signature……. Address……

	…… ……
Operator:	Name:……

Appendix 9

Request to view CCTV footage

City Alarm & Emergency Centre

Return Fax No.: - 0191 553 1995

Sunderland City Council

Name: Signature:	Company: Address Tel:
Date/Time of incident: From: to:	Exact Nature of incident
Location of incident	
Details of offenders and/or vehicles involved	

for CAEC use only:

Operator ID			
Log of found data	Time	Description	Camera

Persons contacted	Date	Name	Message left

If download is required for Northumbria Police - request and attach their DPA2 form