Appendix 1

CCTV Policy

North Tyneside Council

Contents

Definitions

"**Personal Data**" means any data which relate to a living individual who can be identified.

"**Special Category Data**" means personal data consisting of information as to;

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

"**Data Controller**" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

"**Data Processor**" means any person who processes the data on behalf of the data controller.

"Data Protection Impact Assessment" ("DPIA") is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals.

"**Authority**" means the Local Authority, North Tyneside Council.

“**Camera**” means any device used as part of a CCTV system. This includes unmanned aerial vehicles (drones) and body worn camera devices.

“**CCTV**” means Closed Circuit Television.

“**CCTV System**” means any system of 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**” means any image captured by a CCTV system.

“**BWVs**” Body Worn Video or Camera device.

Section One Introduction and Objectives

1.1 Introduction

The Authority operates several Closed-Circuit Television (CCTV) systems. The systems comprise of a number of cameras installed at locations across the borough. Not all cameras are pro-actively monitored, some are monitored on-site, some are monitored remotely, and some are monitored on behalf of a third party under contract or agreement. The Authority also uses mobile CCTV technology and there is scope for the use of Body Worn Video (BWV).

1.2 Aims and Objectives of this Policy

The aim of this document is to set out the Authority's policy in relation to its use of overt CCTV surveillance. It covers three main areas:

- The legal context in which the Authority operates CCTV;
- What central controls will apply to the use of CCTV on behalf of the Authority; and
- What service areas and delivery partners need to do to comply with the relevant legislation.

1.3 Scope of the Policy

This policy, and its guidance, will apply to any CCTV camera being operated by, or on behalf of the Authority.

It should be noted that this policy only covers the Authority's use of *overt* CCTV systems. The use of any CCTV for covert activity is covered under the Authority's Surveillance Policy which details how the Authority complies with the provisions of the Regulation of Investigatory Powers Act (RIPA) 2000 and is therefore beyond the scope of this policy.

1.4 Compliance with the Policy

All services engaged in the use of CCTV systems (as set out in Definitions) must comply with this policy in order to comply with all relevant legislation.

A Code of Practice (COP) must be maintained for each CCTV system in use and made available for Audit. This must be signed off by the relevant Head of Service, reviewed at least annually and will be held with Information Governance. The COP is built around the 12 Guiding Principles document produced by the Surveillance Camera Commissioner (SCC).

1.5 Breaches of this Policy

Failure to adhere to this policy will place the Authority at significant risk and may also result in a breach of legislation. All breaches and near misses of this policy **must be reported** direct to the Information Governance Team (IGT).

Actions or neglect leading to a breach of this policy, or failure to report a breach will be investigated in line with current disciplinary procedures.

Section Two Legal Context

2.1 The Data Protection Act 2018 (DPA)

The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government. Everyone who is responsible for using data must comply with current legislation, this policy, and the supporting procedures that CCTV Operators follow.

2.2 Right to Privacy

The Authority recognises its obligations under the Data Protection Act 2018, Human Rights Act 1998 and in particular an individual's right to privacy. To fulfill these obligations, we will do the following:

- Where an overt CCTV system is in place, individuals will be made aware that they are about to enter an area where CCTV is active. This will be achieved by prominent signage placed at either the entrances to a building or the perimeter and approaches of a less well-defined area – a town center for example.

- The Authority's Responsible Officers for CCTV systems will ensure that signage complies with the relevant statutory guidance. An annual check of all signage is undertaken to ensure it is still visible and contains the correct information.

- For any CCTV camera, a full Privacy Impact Assessment must be in place. A clear review date and process must be identified within the assessment. Completed assessments should be submitted to the IGT for publication on the Authority website.

2.3 The Protection of Freedoms Act 2012 (POFA)

Since its introduction, the POFA has seen the introduction of a new surveillance camera code of practice published by the Home Office and the appointment by the Secretary of State of a SCC. The Information Commissioners Office (ICO) is tasked with the enforcement activity that regulates the application of this legislation. The Authority's overt CCTV Policy is written with the guidance document 'In the picture: A data protection code of practice for surveillance cameras and personal information' which was released in May 2015 and acts as a key guide to compliance with the POFA.

In addition to the guidance, there are also 12 guiding principles of practice which are set out in Appendix 1. These form the basis of the required Code of Practice for each CCTV system.

The Authority has nominated its Data Protection Officer as its Senior Responsible Officer to the SCC.

2.4 Guidance and Codes of Practice

This Policy has been written using the following legislation and guidance:

- The Data Protection Act 2018 (DPA)
- General Data Protection Regulation 2016 (GDPR)
- The Protection of Freedoms Act 2012 (POFA)
- Human Rights Act 1998 (HRA)
- 'In the picture: A data protection code of practice for surveillance cameras and personal information' May 2015
- 'Twelve Guiding Principles' guidance, the Surveillance Camera Commissioner.

There are some cameras which the Resilience and Security Team monitors on behalf of other parties. The Authority's clients include:

- Nexus
- Northumbria Police
- Schools in North Tyneside
- Capita (as part services it delivers on behalf of the Authority)
- Internal services (libraries, Customer First Centers etc.)

In these cases, the Private Security Industry Act 2001 also applies to operations.

Section Three Central Controls

3.1 Information Governance

The ICO has produced a Data Protection Code of Practice for CCTV to assist organisations who use CCTV to comply with the Data Protection legislation. The Code gives guidance in areas such as deciding when CCTV should be used, governance of the personal data a CCTV system may collect, how to use the equipment and organisational responsibilities. As with the SCC Code of Practice, the ICO Code has also been adopted, in full, by the Authority.

3.2 Designated Roles

The Authority acts as the Data Controller for the information captured by the cameras that it owns.

The Authority may act as Data Processor for the information captured by cameras operated on behalf of third parties. This will be detailed in existing service level agreements or contracts.

The Data Protection Officer acts as the SRO for the Authority in relation to the SCC. Where a CCTV system exists, a specific Code of Practice will name a Responsible Officer for each system.

3.3 Processing and Handling of Recorded Material

Access to the equipment used to download footage and record images will be strictly controlled to CCTV Operators. Operators need to know how to recognise any formal request and must know the procedure for dealing with that request for footage.

The DPA 2018 will apply at all times to the information recorded on CCTV as it relates to personal data. Subject access requests must be dealt with in line with standing procedures with the Information Governance Team. Any third-party

requests for footage must be considered on a case by case basis and with advice from Information Governance.

Where law enforcement agencies make a request for footage, it must be clearly in connection with the investigation of a crime or suspected crime using a specific piece of legislation. Advice must be sought from Information Governance about releasing footage on receipt of a request.

A retention and disposal procedure detailing secure disposal of footage (usually automatic deletion) for each system will be clearly stated in the appropriate COP.

3.4 Secure Storage of Information

Each part of the Authority's CCTV system must be housed in a secure building or facility and access strictly controlled to authorised personnel only. Processes must be in place within each COP.

3.5 Operators

All Authority CCTV Operators must receive relevant training in the requirements of the Human Rights Act 1998, Data Protection Act 2018, and Regulation of Investigatory Powers Act 2000, this policy and the relevant COP. It is the responsibility of the individual Responsible Officers to ensure that training is provided and is both adequate and proportionate

Authority officers operating CCTV systems must be familiar with the requirements of information governance and should complete the Authority's Information Governance mandatory eLearning course as a minimum.

In most cases, Operators of public space surveillance systems must be licensed with the Security Industry Authority (SIA). Responsible Officers should seek advice directly form the SIA in relation to current licensing requirements.

Appendix 1 12 Guiding Principles

These are taken from the Surveillance Camera Code of Practice.

System operators should adopt the following 12 guiding principles:

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 system 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 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.

Appendix 2 Code of Practice Requirements

Principle	What you should include in the COP
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.	A clearly stated objective for the use of a camera (or system) must be in place. A Data Protection Impact Assessment DPIA is the right place to record this information, but the objective should also be displayed on appropriate signage where possible. A system can have an overall COP but each individual camera must have a DPIA.
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.	A DPIA must be carried out before placing a camera anywhere in the borough. Each camera should be evaluated against the impact on individuals' privacy. Details of any privacy screens or limitations on viewing zones in the operation of the equipment should be detailed here. A review date must be set for both permanent and mobile or re-deployable cameras. The Resilience, Security Services and Community Safety Team maintain a re-deployable camera process.
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 surveillance.	Each system must have appropriate signage with full contact details of the Responsible Officer (this should be role based, not named individuals in terms of public signs). The DPIA must be published on the Authority website to aid transparency.
There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.	The Data Protection Officer is the Senior Responsible Officer for the Surveillance Camera Commissioner. Each CCTV system should also have a Responsible Officer who will be responsible for completing the COP and DPIA's.

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.	These should clearly demonstrate a reasonable level of control over: who will use it, how they will use it, how they will be managed and how their access and what they are viewing will be monitored, how complaints and access requests will be dealt with, how to report faults, what the maintenance arrangements are for the equipment,
No more images and information should be stored than that which is strictly required for the stated purpose of a camera system, and such images and information should be deleted once their purposes have been discharged	The COP must detail a retention policy for any footage recorded, details of how footage will be securely destroyed, how any downloaded footage will be stored, handled, transferred (where necessary) and recorded.
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.	Who will have access to footage? Who can view footage? Who makes decisions? How will advice be sought from Information Governance? How and where will records of these be held? This should be cross referenced with current Information Governance procedures. A record of any disclosures, the reasons, the method of transfer and a signed acceptance by the receiving party should also be included in the COP.
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.	List all that apply to your system and operators, including whether operators need to be licensed with the SIA or whether any exemptions apply.
Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.	Detail how you will ensure this and restrict access. Licensing considerations must also be a factor.
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.	The COP's are all subject to internal audit checks and inspection by the Information Governance Manager and SCC.
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	Are the images of good evidence quality? Has the equipment been purchased through the third-party certification scheme?

law enforcement with the aim of processing images and information of evidential value.	
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.	Not applicable – relates to Automatic Number Plate Recognition and Facial recognition software which are not in the scope of this policy.