Appendix 1

CCTV Policy - (Overt Surveillance)

Contents

Appendix:

1. Definitions

UK GDPR	The General Data Protection Regulation 2016 / 679
HRA	Human Rights Act 1998
DPA	The Data Protection Act 2018
RIPA	The Regulation of Investigatory Powers Act 2000
POFA	The Protection of Freedoms Act 2012
FOIA	Freedom of Information Act 2000
CCTV	Closed Circuit System
BWC	Body Worn Cameras
ICO	Information Commissioners Office
ICO Code	"In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information" – ICO May 2015
SCC	Surveillance Camera Commissioner
SCC Code of Practice	Surveillance Code of Practice 2013

2. Summary

2.1 Rotherham Borough Council (the Council) has in place Closed-Circuit Television (CCTV) and other surveillance systems. This policy details the purpose, use, and management of the systems, and details the procedures to be followed to ensure that the Council complies with relevant legislation and Codes of Practice where necessary.

2.2 This policy and the procedures therein detailed, applies to all the Council's CCTV and surveillance systems, including overt and covert installations capturing images of identifiable individuals for the purpose of viewing, and / or recording the activities of such individuals.

2.3 CCTV and surveillance system images are monitored and recorded in strict accordance with this policy.

3. Introduction

3.1 The Council uses CCTV and surveillance system images for the prevention and detection of crime, public safety, to monitor the Council's buildings in order to provide a safe and secure environment for staff, volunteers, contractors, and visitors, and to prevent the loss of, or damage to, the Council's contents and property.

3.2 The CCTV and surveillance systems are owned by the Council and managed by the Council and / or its appointed agents. The Council is the system operator, and data controller, for the images produced by the CCTV and surveillance systems, and is registered with the Information Commissioner's Office, Registration number **Z5759798**.

3.3 This policy applies to CCTV and other surveillance camera devices that view or record individuals, and covers other information that relates to individuals, for example vehicle registration marks captured by Automatic Number Plate Recognition (ANPR) equipment.

3.4 This policy uses the terms 'surveillance system(s)', 'CCTV' and 'information' throughout for ease of reference, and would include (but is not limited to) the following types of systems:

- Fixed CCTV (networked)
- Body Worn Video
- Automatic Number Plate Recognition (ANPR)
- Unmanned aerial systems (drones)
- Stand-alone cameras
- Re-deployable CCTV
- Fleet vehicle cameras
- Mobile enforcement vehicle(s) i.e., CCTV van

3.5 The policy does not cover video recording devices that the Council may supply to victims of crime or potential victims of crime as a way of enhancing personal or building security. An example of this type of equipment would be a video doorbell to allow the victim or potential victim of crime to see who is approaching their property, or who has approached their property. Once this type of equipment is handed to the client it becomes the sole property of the client and a form of disclaimer is obtained to reflect this clarity of ownership and future responsibility.

3.6 This policy should be read in conjunction with the following codes of practice and guidance for surveillance cameras that have been adhered to in the development of this policy:

3.7 **Surveillance Camera Code of Practice 2013 (Amended November 2021).**

https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf

3.8 **Surveillance Camera Commissioner – A guide to the 12 principles of the surveillance camera code of practice.**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1054263/Code_of_Practice-

guide_to_the_12_principles.pdf

3.9 **Surveillance Camera Commissioner Code of Practice – Steps to complying with the 12 principles of the surveillance camera code of practice.**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1054264/Code_of_Practice_-_steps_to_compliance.pdf

3.10 **"In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information" – Information Commissioners Office.**

https://ico.org.uk/media/1043340/surveillance-by-consent-cctv-code-update-2015-jonathan-bamford-20150127.pdf

3.11 **Surveillance Camera Commissioner – Data protection impact assessments – guidance for carrying out a data protection impact assessment on surveillance camera systems.**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881538/SCC___ICO_DPIA_guidance_V3_FINAL_PDF.pdf

3.12 **Information Commissioners Office – CCTV and video surveillance guidance.**

https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/

3.13 **Overlap with Regulation of Investigatory Powers Act 2000 (RIPA)**

All those involved with CCTV operations must be keenly aware of the difference between overt and covert operations. Overt cameras are covered by this Policy; the use of covert cameras can, and must, only be authorised through the Council's RIPA Policy. The current policy can be viewed at:

https://rotherhammbc.sharepoint.com/:w:/r/sites/PoliciesPlansandProcedures/_layouts/15/Doc.aspx?sourcedoc=%7BD809D24B-D339-4BEB-B242-EDD33B14B768%7D&file=Regulation%20of%20Investigatory%20Powers%20Act%20(RIPA)%20Policy%202019.doc&action=default&mobileredirect=true&DefaultItemOpen=1

3.14 Deployment of cameras in circumstances that can be considered directed surveillance, must follow the RIPA authorisation process and not the Council's Overt CCTV Policy.

3.15 Directed Surveillance is defined as any surveillance which is covert, but not intrusive, and is:

- Carried out for the purposes of a specific investigation or operation.
- Likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) and.
- Conducted otherwise than by way of an immediate response to events or in circumstances where it would not be practical to seek an authorisation.

3.16 Covert surveillance is defined as: '*surveillance carried out in a manner that is calculated to ensure that persons who are subject to surveillance are unaware that it is or may be taking place'.*

3.17 Concealed cameras are not necessarily the same as covert cameras. Where very clear signage indicates that CCTV is in operation and that concealed cameras are in use, then the Council may be able to use the overt CCTV Policy, so long as the use of the cameras does not constitute directed surveillance. The only current example of the use of concealed cameras in this way is in relation to fly-tipping cases. If officers are proposing to use concealed cameras under this policy in different circumstances, or if there appears to be any risk of directed surveillance, or any uncertainty, then Legal Services must be consulted before CCTV is used in those circumstances.

4. Purpose

4.1 This Policy governs the installation and operation of all CCTV and surveillance systems at the Council.

4.2 CCTV surveillance is used to monitor and collect visual images for the purposes of:

- To help reduce the fear of crime to provide a safe and secure environment for residents of, and visitors to, the areas covered by the scheme.
- To help deter and detect crime and provide evidential material for court proceedings.
- To assist in the overall management of the Council.
- To assist in the management of the Council's housing stock.
- To assist in the management of other locations and buildings owned or controlled by the Council.
- To enhance community safety, including the prevention and detection of harassment, to assist in developing the economic well-being of the borough.
- To assist the Local Authority in their enforcement and regulatory functions within the borough.
- To assist in traffic management and encourage safer and more sustainable use of all modes of transport and provide travel information to the media and public.
- To assist in supporting civil proceedings.
- To identify breaches of tenancy terms and to supply evidence to

support enforcement action, this may include civil proceedings.

- To monitor all modes of travel to enable improvement and better management of the public highway (traffic cameras).
- To assist the Council in discharging its health and safety obligations towards staff
- To investigate allegations of staff misconduct

4.3 CCTV systems must not generally be used to monitor the activities of Council officers or members of the public in the ordinary course of their lawful business. The general principals adhered to regarding monitoring employees in the workplace can be viewed at:

4.4 **Information Commissioners Office – The employment practices code (Part 3).**

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

5. Policy Statement

5.1 This policy statement and the following guidance must be always complied with on Council premises.

5.2 The Council will operate its CCTV systems in a manner that is consistent with respect for the individual's privacy.

5.3 The Council complies with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Surveillance Camera Commissioner's Surveillance Code of Practice to ensure CCTV is used responsibly and safeguards both trust and confidence in its continued use.

5.4 The CCTV systems will be used to observe the areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

5.5 The use of the CCTV systems will be conducted in a professional, ethical, and legal manner, and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.

5.6 Cameras will be sited so they only capture images relevant to the purposes for which they are installed. In addition, equipment must be carefully positioned to:

- cover the specific area to be monitored only.
- keep privacy intrusion to a minimum.

- ensure that recordings are fit for purpose and not in any way obstructed (e.g., by foliage).
- minimise risk of damage or theft.

5.7 Before any CCTV system is installed, service areas will consider other, less intrusive methods to achieve the objectives of having a CCTV system in place (e.g., improving lighting in an area to prevent crime).

5.8 A CCTV Deployment Approval Form must always be completed, and management must ensure that there is reasonable justification before CCTV is approved and used (CCTV Deployment Approval Form – **Appendix 1**).

5.9 The intended use of the CCTV will be documented, and the system must not be used for anything other than this purpose (CCTV System Code of Practice – **Appendix 2**)

5.10 The processing of personal data using CCTV systems is likely to result in a high risk to rights under the data protection legislation. Therefore, all schemes require an assessment of their potential impact on people's privacy. A Data Protection Impact Assessment (DPIA) must be carried out before the CCTV system is installed and reviewed regularly (Data Protection Impact Assessment – **Appendix 3**).

5.11 A designated manager will have responsibility for compliance with the schemes operational processes and procedures.

5.12 Regular training will be provided to ensure operators are kept up to date with relevant legislation and operating procedures.

5.13 Permanent or movable cameras must not be used to view areas that are not of interest and not intended to be the subject of the scheme. They must be used in accordance with the CCTV System Code of Practice.

5.14 There are areas where there is an expectation of heightened privacy and CCTV may only be used in very extreme cases and this must not be undertaken without discussing with the senior manager of the site, for example siting CCTV outside a school.

5.15 The CCTV will only be used at relevant times, for example times when site security is at risk.

5.16 The equipment used must be maintained to ensure reliability and the highest quality video images and recordings.

5.17 No sound recording technology is to be used, with the exceptions outlined in the Council's Licensing Policy.

5.18 Material must not be stored for longer than is necessary and must be deleted as soon as possible. For example, as soon as it is obvious that no crime has occurred, then the data must not be kept beyond the retention period.

5.19 Images must be viewed in a secure/restricted area with access only to authorised persons.

5.20 Images must not be released to third parties unless a valid request in line with appropriate legal exemptions is received and accepted.

5.21 Individuals who are recorded may request access to the images, via a data subject access request, subject to exemptions.

5.22 There must be adequate signage to let people know that surveillance is taking place. Where cameras are discreet, the notices must be more prominent. Where cameras are concealed, the notices must confirm this fact.

5.23 The CCTV systems must not be used to systematically monitor people. If this is required to obtain the information that is needed, then authorisation to carry our directed surveillance under the Regulation of Investigatory Powers Act (RIPA) 2000 will be required and the relevant officers must immediately contact Legal Services for advice.

6. Legislation and Guidance

6.1 In addition to the policy, the use of CCTV cameras is subject to the following legislation:

- The General Data Protection Regulation 2016 / 679 (UK GDPR)
- The Data Protection Act 2018 (DPA 2018)
- Human Rights Act 1998 (HRA 1998)
- Freedom of Information Act 2000 (FOIA 2000)
- Regulation of Investigatory Powers Act 2000 (RIPA 2000)
- Protection of Freedoms Act 2012

6.2 The Human Rights Act 1998 gives effect in the UK to the rights set out in the European Convention on Human Rights (ECHR) Article 8 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 Act. Surveillance that may interfere with such a right should only be carried out where it is necessary and proportionate to do so.

6.3 The purpose of this policy is that the above legislation and the previously referred to Surveillance Camera Commissioner Code of Practice is always complied with when operating the CCTV systems.

7. Responsibilities

7.1 CCTV SPOC – Council Single Point of Contact (SPOC)

- The role is delivered by the Service Manager for Regulation and Enforcement
- The SPOC will comply with the roles and responsibilities as set out by the Surveillance Commissioner for CCTV systems.
- The SPOC is responsible for ensuring all those involved in the use of CCTV systems can view current legislation and guidance relating to CCTV systems.
- The SPOC will be required to be fully trained in relation to the use of, and policies relating to, overt and covert camera usage and where RIPA is applicable.
- The SPOC will review the CCTV policy annually and refresh the Policy every three years.
- The SPOC will authorise the deployment of all CCTV systems.
- The SPOC will be responsible for maintaining a central register of all corporate surveillance equipment, including location, asset reference and manager responsibility.
- The SPOC will establish a local Code of Practice which sets out the governance arrangements that all schemes must comply with. This code must set out the regulatory framework that each scheme must comply with, the internal assessment programme that each scheme must undertake, and the processes required to establish a new surveillance camera scheme or upgrade an existing scheme.
- The SPOC will be responsible for maintaining the code and providing regular guidance and updates to scheme managers to ensure that all surveillance camera schemes continue to operate in full compliance with the regulatory framework governing its use.

7.2 Designated Manager (The Scheme Manager)

- The role will be undertaken by a Community Protection and Environmental Health Manager.
- This will be a minimum M2 Grade Manager who is liable for the deployment of CCTV and its legality.
- The Scheme Manager is liable for the actions of the Nominated and Investigating Officers.

7.3 Responsible Officer (Supervising Officer or System Operator responsible to the Designated Manager)

- The role will be undertaken at a service principal officer/team leader/delegated officer level such as Principal Officer or equivalent. In the absence of the Principal Officer or equivalent, the Community Protection and Environmental Health Manager or equivalent will fulfil this role or delegate to a named competent officer
- The day-to-day operational responsibilities for each CCTV system rests

with the nominated officer.

- A list of all CCTV systems and their nominated officers will be recorded and available in a CCTV register held by the Council's SPOC
- Person or persons that take a decision to deploy a surveillance camera system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.
- The responsible officer shall ensure that Council officers involved in the operation of CCTV systems 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.
- 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 officers are able to operate or view images.
- The responsible officer shall investigate any reported misuse of a CCTV system and report it immediately to the CCTV SPOC. It will be the responsibility of the CCTV SPOC to refer any misuse of CCTV to the relevant immediate line manager.
- The responsible officer shall report any faults in the CCTV system equipment to the CCTV SPOC and take steps to remedy the fault at the earliest opportunity.

7.4 Investigating Officer (System User)

- The role will be undertaken at an operational officer level such as Environmental Health Officer, Community Protection Officer, Enforcement Officer, or equivalent authorised officers.
- Person or persons who have access to live or recorded images or other information obtained by virtue of such system.
- Person or persons who are trained to burn images and deal with access requests.

8. Process

8.1 This process relates to the following across the council:

- The formal authorisation
- Purchasing and deployment
- Monitoring and handling
- Access to images
- Signage and privacy notices
- Storage
- Inspection and audit
- Complaints

9. CCTV Approval Process

9.1 This procedure covers overt surveillance only. There will be occasions where concealed cameras are deployed, but only in conjunction with very clear

signage confirming that fact. During a previous Regulation of Regulatory Powers Act 2000 (RIPA) inspection the Office of Surveillance Commissioners (OSC) Inspector found that 'such signage renders the proposed surveillance overt and therefore does not require authorisation under RIPA'. Consequently, in these circumstances it brings the surveillance within the Council's CCTV Policy & Guidance regime.

9.2 **Approval Procedure**

9.3 To ensure compliance with the requirements of the CCTV Policy, the CCTV Deployment Approval Form (Appendix A) and CCTV Code of Practice document (Appendix B) must be completed. These should be drawn up between the Investigating Officer and the Responsible Officer.

9.4 No officer, unless they have attended suitable training and are deemed competent by the CCTV SPOC, shall take a lead role as an Investigating Officer, Responsible Officer or Scheme Manager.

9.5 Despite being an overt surveillance operation, there may still be a risk of intrusion into people's privacy and a risk of collateral intrusion. To address this, regard must be given to the necessity, proportionality, and risk of collateral intrusion of the scheme. To demonstrate this, the CCTV Deployment Approval Form (Appendix A) should [under 'Storage and Retention'] detail issues such as how long it is intended to have the camera in place for and how regularly the recordings will be reviewed. If necessary, an addendum can be added to ensure all information has been provided in order to allow a decision to be taken.

9.6 All applications for authorisation to deploy overt CCTV will be accompanied by a Data Protection Impact Statement (DPIA) (Appendix C). No application will be authorised without a DPIA.

9.7 Guidance Points for CCTV Deployment Approval Form (Appendix A):

9.8 In addition to the information provided in the CCTV Code of Practice document (Appendix B), the following shall be included:

- Column 1 – **'Property'** – Property where CCTV camera is located
- Column 2 - **'Purpose of CCTV Camera**' – Should identify the purpose of the installation as referred to previously in Section 4.
- Column 3 – **'Public Awareness'** – Should describe how individuals are to be made aware that a CCTV system is in use, which should include a description of signage and its location.
- Column 4 – '**Responsible Officer'** – this should include the responsibilities and names of the Responsible Officer, Scheme Manager, and Investigatory Officer(s)

- Column 5 – **'Storage and Retention'** - should include details such as how long it's intended to have the camera in place for and how regularly the recordings will be reviewed. The footage needs to be regularly reviewed so that cameras can be removed if it is deemed that the objective of the CCTV system has been achieved and any material that is of no use shall be deleted. It shall be ensured that any material that is of use is retained securely.

9.9 **Submission of Application**

9.10 The Scheme Manager shall ensure that the surveillance and associated documentation is CCTV Policy compliant. Appendix A, Appendix B and the DPIA at Appendix C shall be submitted direct to the SPOC for the purpose of this policy. Only applications submitted according to this process will be deemed as a valid application.

9.11 In the absence of the SPOC, a Community Protection and Environmental Health Manager, will have delegated authority to authorise applications.

9.12 **Authorisation**

9.13 The SPOC will review and authorise CCTV camera deployment only when satisfied that there is full compliance with the CCTV Policy.

9.14 When approved, authorisation will be confirmed by the CCTV SPOC by email, including named officers responsible for the deployment and management of the deployment within the remit of the CCTV Policy.

9.15 In most cases requests for CCTV camera deployment will have emanated through the borough Community Action Partnerships (CAP) and the Borough multi-agency Operational Tasking Groups.

9.16 The respective Operational Tasking Group responsible for deploying the CCTV camera(s) shall keep a documented record of each deployment together with location and supervising and investigating officers. The record will be maintained as a live document and reviewed and updated at the group meetings. The Tasking Group is responsible for updating the relevant CAP group in respect of outcomes related to the camera(s) deployment.

9.17 The SPOC will ensure that a master record of all CCTV camera deployments within the Council is maintained.

9.18 Parameters contained within an application might change prior to deployment or during the lifetime of that deployment, these would include, but not exclusively:

- Change of surveillance times
- Change of equipment
- Breakdown and repair of equipment
- Adjustment of location

- Vandalism and theft of signs
- Vandalism and theft of cameras

9.19 In all such circumstances the SPOC must be informed immediately and a reviewed and updated application presented to the Scheme Manager for authorisation.

9.20 Deployment within the altered parameters must only take place once authorisation has been granted.

10. Purchasing and Deployment

10.1 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.

10.2 Where a third party is responsible for the storage or processing of data from CCTV systems, then third-party data processing contracts must be in place with the third party to ensure protection of the data and compliance with the Council's Information Governance Policy. The Council Information Governance Policy can be found at:

https://rotherhammbc.sharepoint.com/sites/PoliciesPlansandProcedures/All%20policies%20plans%20and%20procedures/Forms/AllItems.aspx?id=%2Fsites%2FPoliciesPlansandProcedures%2FAll%20policies%20plans%20and%20procedures%2FInformation%20Governance%20Policy%202018%2Epdf&parent=%2Fsites%2FPoliciesPlansandProcedures%2FAll%20policies%20plans%20and%20procedures

10.3 Those responsible for introducing and operating CCTV systems must ensure that the use of cameras is proportionate to the intended objective and that an individual's right to privacy is always respected. A clear operational objective for the deployment of a CCTV system must be identified and a Data Protection Impact Assessment (Appendix C) must be carried out and reviewed yearly. an assessment on the impact on privacy must be carried out and reviewed each year.

10.4 A Data Protection Impact Assessment must be completed for each CCTV system in use.

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

10.6 Covert surveillance is not permitted to be carried out under the auspices of this policy. Such activities fall within RIPA and authorisation must be obtained for such activity under the Council's RIPA procedures and the Council's Legal Services must be consulted about acquiring such authorisation.

10.7 The Council does not generally use cameras that can monitor conversation or

be used to talk to individuals as this is viewed as an unnecessary invasion of privacy. This, however, does not apply to body cameras where interactions may be recorded.

10.8 Where body 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 always visible during an interaction that is being recorded or may be recorded. If there is any doubt that a member of the public is aware of a body camera being used, then the officer should proactively inform the member of the public that a body camera is being worn.

10.9 Where dashcams or similar are in use in vehicles, an officer using them must display a clear notice that this is the case on their vehicle, in a prominent and clear position. This notice should not be covered up or obscured but should be always visible. Where dashcams or similar may be used to record interactions outside of the vehicle between an officer and a member of the public, if there is any doubt that the member of the public is aware of the dashcam, the officer should inform the member of the public that a dashcam is being used.

11. Handling, Monitoring and Access to Images

11.1 Where CCTV monitors are providing live monitoring for security or other Council officers, and are sited in reception areas and areas open to the public or visitors, the ability to view the CCTV system monitors must be restricted to those authorised to see them. Monitors must not be visible to those entering the premises.

11.2 Monitoring of CCTV systems will only be carried out by officers authorised to do so.

11.3 CCTV will only be subject to the Data Protection legislation if the footage captured relates to individuals who can be identified from it.

11.4 Access to images must follow one of the following routes:

11.5 **Subject Access Request**

11.6 Members of the public have the right to request access to their personal information (images) in line with Data Protection legislation. Access will only be granted when a completed request form has been submitted and identity verified.

11.7 CCTV access requests can be made through the ‘Right to Access’ page of the Council’s website:

https://www.rotherham.gov.uk/contact-council/right-access

11.8 **Law Enforcement**

11.9 Organisations responsible for the detection and prevention of crime, taxation recovery or duties of similar nature can request access to personal information (images) in line with Data Protection Legislation.

11.10 Consideration to allow access will only be granted when a formal request has been received through existing and approved procedures.

11.11 **Solicitors/Insurance Companies**

11.12 Organisations acting on behalf of individuals dealing with legal claims or responding to court orders can request access to personal information (images) in line with Data Protection Legislation.

11.13 Access will only be granted when a formal request has been received that complies with current data protection exemption legislation or is subject of a Court Order.

11.14 In all cases, the councils Information Management Team will verify the request and identity of the person or organisation making the request before forwarding to the CCTV SPOC to enable an appropriate response.

12. Signage and Privacy Notice

12.1 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 CCTV.

12.2 Where signs are used on the highway to alert road users to the use of CCTV systems, these should not affect the safety or road users.

12.3 Where CCTV signage is used and there might be penalties incurred from the images recorded, then the signs must reflect the risks. For example, where CCTV is used in relation to environmental offences, the signage must warn that legal action is a risk if offences are recorded.

12.4 Where body 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 always visible during an interaction that is being recorded or may be recorded. Where they may be doubt that a member of the public might be aware of this, then the officer should inform the member of the public that a body camera is being worn.

12.5 Signs should be of appropriate size depending upon context such as whether the signs are to be read by road users or pedestrians. If concealed cameras are being deployed, then the signs should clearly state this fact.

12.6 Data Protection legislation provides individuals with the right to be informed

about processing of their personal data. All CCTV processing must be detailed within the Council and Directorate Privacy Notice.

12.7 Guidance on the content of Privacy Notices can be found on the Information Management Team intranet site at:

https://www.rotherham.gov.uk/contact-council/privacy-notice-right-informed/9

13. Storage and Retention

13.1 Images and information obtained from a CCTV surveillance camera system will not be retained for longer than necessary to fulfil the purpose for which they were obtained.

13.2 Unless required for evidentiary purposes, the investigation of an offence, or as required by law, CCTV images will be retained for no longer than 31 calendar days from the date of recording (or for certain systems, until storage limitations require that footage needs to be overwritten). Images will be automatically overwritten or destroyed after this time.

13.3 Any footage downloaded and retained for evidential purposes must be reviewed after three months by the Scheme Manager, and either a destruction date or review date must be set, with written justification for further retention recorded.

13.4 Recorded material will not be sold or used for commercial activities or published on the internet.

13.5 All CCTV systems will be kept secure and free from unauthorised access.

13.6 All recorded images are the property and copyright of the Council.

13.7 All images will be stored securely on servers and no images will be stored to a cloud.

13.8 Where, for evidential and viewing purposes, recordings are placed onto removeable storage equipment, they will have a unique reference number and always remain secure.

13.9 All images will be time and date stamped.

13.10 All images and media will be confidentially disposed of when no longer needed.

14. Monitoring/Inspections

14.1 CCTV systems can be inspected or audited at any time by:

- The SPOC
- Relevant Head of Service
- Members of the Information Management team

- Members of the Corporate Complaints team
- Members of the senior management team
- Legal Services (RIPA process)
- Internal Audit
- Members of the Information Commissioner's Office

15. Complaints

15.1 All complaints relating to the use of CCTV systems will be subject to the Council's Corporate Complaints Procedure:

https://www.rotherham.gov.uk/downloads/file/294/corporate-complaints-procedure

Appendix 1 – CCTV Approval Form

CCTV APPROVAL FORM

Please complete the following:

Property/Site (Place where CCTV camera is located)	**Purpose of CCTV Camera** (i.e., primarily for security purposes/in order to ensure the safety and security of staff and visitors/ prevention and/or detection of crime.)	**Public Awareness** (In order to comply with Article 5 GDPR (fair and lawful obtaining and processing), individuals should be made aware that a CCTV system is in use. Please advise how this is done – signs displayed etc.)	**Nominated Officer** (The Supervising Officer for the CCTV System)	**Storage and Retention** (Where are images stored, who has access to the images and how long they are kept for?)	**Quality** (i.e., How often are the media changed/if quality not adequate for purpose who will this be reported to? /How long for repair or reinstatement if broken or damaged/Where will maintenance log be kept and who is responsible to check log?) Give Details

Appendix 2 – CCTV System Code of Practice

1. Purpose

1.1 The CCTV system installed at the [LOCATION] will be used for the STATE PURPOSE.

1.2 The CCTV system will monitor activity at [LOCATION] A Map of the location is attached to this application at [APPENDIX] with the location of the camera marked with a [DESCRIBE THE MARK]

2. Public Awareness

2.1 In order to comply with Article 5 GDPR (fair and lawful obtaining and processing), individuals will be made aware that a CCTV system is in use. A number of camera warning signs will be sited around the area. The signs will be clearly visible and legible.

2.2 A photograph(s) of the intended signage position is provided to this application at [APPENDIX] and marked on the map referred to in 1.2 with a [DESCRIBE THE MARK]

3. Nominated Officers

3.1 The supervisory officers for the surveillance CCTV system will be [NAME OF SUPEVISORY/NOMINATED OFFICER]. The system will be used and monitored under the supervision of [NAME OF SUPEVISORY/NOMINATED OFFICER], by investigatory officers [NAME AND RANK OF INVESTIGATORY OFFICERS/SYSTEM USERS].

3.2 The designated manager for the CCTV system will be [NAME OF DESIGNATED MANAGER]

4. Storage and Retention

4.1 Images will be stored [LOCATION OF STORAGE DATA INCLUDING BUILDING AND SYSTEM] and will only be viewed in a secure location by [NAME OF OFFICERS AUTHORISED TO VIEW IMAGES].

4.2 In accordance with Data Protection Act 2018, images will be kept only as long as necessary for the specified purpose. They will, therefore, be retained for [SPECIFY TIME PERIOD FOR RETENTION]. When this period expires the images will be removed or erased.

5. Quality

5.1 The media will be changed every [FREQUENCY OF MEDIA CHANGE] If the quality of images is not adequate for the intended purpose, this will be reported to [SYSTEM PROVIDER

5.2 If a breakdown occurs, the camera will be repaired and reinstated as soon as practicable.

5.3 A maintenance log for the system will be kept at [LOCATION] and will be checked by the Nominated/Supervising Officer [NAME OF OFFICER].

Appendix 3 – Data Protection Impact Assessment

The template for the Data Protection Impact Statement can be found at:

https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras