Rotherham Metropolitan Borough Council

Appendix A: CCTV Policy and Guidance (Overt Surveillance)

CCTV Policy and Guidance (Overt Surveillance)

Version	Author	Approved By	Date	Published	Review
0.2	Lewis Coates/ Supported by Marie Buxton		April 2018	-	-
0.3	Marie Buxton		25/04/2018	-	-
0.4	Lewis Coates		8th May 2018		
0.5	Neil Concannon		25th May 2018		
0.6	Neil Concannon and Lewis Coates		13th June 2018		
0.7	Neil Concannon and Lewis Coates		9th July 2018		
0.8	Tom Smith and Lewis Coates		10th July 2018		
0.9	Neil Concannon and Lewis Coates		11th July 2018		
0.10	Tom Smith		20th July 2018		

Contents

1. Introduction

1.1 The following policy relates to surveillance camera equipment and the gathering, storage, use and disposal of Closed Circuit Television (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 word video camera equipment, and automatic number plate recognition . In this policy such devices shall be referred to as 'CCTV Systems'.

1.3 The policy covers all CCTV systems used by Rotherham Metropolitan Borough Council but does not cover Rotherham schools.

1.4 This policy should be read in conjunction with the following codes of practice for surveillance cameras:

https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/561520/NSCS_Strategy_FINAL.pdf

2. Overlap with Regulation of Investigatory Powers Act 2000 (RIPA)

2.1 All 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

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

2.3 Directed Surveillance is defined as:

2.4 Any covert surveillance that is not intrusive.
2.5 Carried out for the purposes of a specific investigation or operation.
2.6 Likely to result in the obtaining of private information about a person.
2.7 Not an immediate response to events or circumstances where it would not be practical to seek an authorisation.

2.8 Covert surveillance is defined as:
2.9 Surveillance is covert if, and only if, it is 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.

2.10 It is important to understand that concealed cameras are not necessarily the same as covert; 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 that 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.

3. Objectives

3.1 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 the CCTV system has been introduced and what the cameras should and should not be used for.

3.2 Each CCTV system will have its own site objectives, these could include some or all of the following:

3.2.1 Protecting areas and premises used by Council officers and the pubic
3.2.2 Deterring and detecting crime and anti-social behavior
3.2.3 Assisting in the identification of and apprehension of offenders
3.2.4 Deterring violent or aggressive behaviour towards Council officers
3.2.5 On-site traffic and car park management
3.2.6 Monitoring traffic movement
3.2.7 Identifying those who have contravened parking regulations
3.2.8 Assisting in traffic regulation enforcement
3.2.9 Protecting Council property and assets
3.2.10 Assisting in grievances, formal complaints and investigations
3.2.11 Surveying buildings for the purpose of maintenance and repair

3.3 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.

4. Policy Statement

4.1 This policy statement and the following guidance must be complied with at all times on all Council premises.

4.2 Management must ensure that there is reasonable justification before CCTV is used. (CCTV Approval Form – Appendix A)

4.3 All schemes require an assessment of impact on people's privacy (Surveillance Camera Privacy Impact Assessment – Appendix B)

4.4 A designated manager will have responsibility for compliance with the schemes operational process and procedures.

4.5 The intended use of the CCTV will be documented and the system must not be used for anything other than this purpose (CCTV Policy – Appendix C)

4.6 Each system must have procedures for administration, which will include:

4.6.1 Ensuring the scheme is in accordance with the CCTV policy
4.6.2 Right to be Informed eg signage and privacy notice
4.6.3 Procedures for handling images.
4.6.4 Record keeping of access requests, use of images procedures
4.6.5 Monitoring of the scheme to ensure compliance, whilst at the same time protecting personal data of others.
4.6.6 Control of recorded material
4.6.7 Retention and Destruction

4.7 Regular training to ensure operators are kept up to date with the procedures.

4.8 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.

4.9 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.

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

4.11 The equipment used must be maintained to give reliable quality.

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

4.13 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.

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

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

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

4.17 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.

4.18 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.

5. Legislation and Guidance

5.1 CCTV systems are subject to legislation under:

5.1.1 Data Protection Act 1998 (DPA)
5.1.2 European Data Protection Legislation (GDPR)
5.1.3 Human Rights Act 1998 (HRA)
5.1.4 Freedom of Information Act 2000 (FOIA)
5.1.5 Regulation of Investigatory Powers Act 2000 (RIPA)
5.1.6 Protection of Freedoms Act 2012
5.1.7 Criminal Procedures and Investigations Act 1996

5.2 Twelve guiding principals of the Surveillence Camera Code of Conduct which the Council will adhere to are:

5.2.1 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.
5.2.2 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.
5.2.3 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.
5.2.4 There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5.2.5 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.
5.2.6 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.
5.2.7 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.

5.2.8 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.

5.2.9 Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

5.2.10 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.

5.2.11 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.

5.2.12 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.[1]

6. Responsibilities

6.1 CCTV Manager (RMBC SPOC)

6.1.1 The role will be undertaken at a Head of Service level such as Head of Service Regulation and Enforcement or equivalent.

6.1.2 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.

6.1.3 The CCTV Manger 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

6.1.4 The CCTV Manager will review the CCTV policy annually

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

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

6.1.7 The CCTV Manager will comply with the roles and responsibilities as set out by the Surveillance Commissioner for organisation Single Point of Contact (SPOC) for CCTV

6.1.8 The CCTV Manager will authorise the deployment of all CCTV systems

6.1.9 The CCTV Manager will ensure that all authorisations and PIAs are submitted to the Information Management team and Legal Services for reference. It is incumbent on the CCTV Manager

[1] Home Office, Surveillance Camera Code of Practice, June 2013, pp 10 - 11

where any application raises concerns, to seek Legal advice before authorizing the application.

6.2 Designated Manager (The Operational Manager)

6.2.1 The role will be undertaken at a service operational manager level such as Community Protection Manager or equivalent.

6.2.2 This will be a minimum M2 graded Manager who is liable for the deployment of CCTV and its legality.

6.2.3 The Manager liable for the actions of the Nominated and Investigating Officers

6.3 Nominated Officer (Supervising Officer or System Operator responsible to the Designated Manager)

6.3.1 The role will be undertaken at a service principal officer/team leader level such as Principal Community Protection Officer or equivalent.

6.3.2 The day-to-day operational responsibilities for each CCTV system rests with the nominated officer.

6.3.3 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

6.3.4 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.

6.3.5 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

6.3.6 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.

6.3.7 The responsible officer shall investigate any reported misuse of a CCTV system and report it immediately to the CCTV Manager. It will be the responsibility of the CCTV Manager to refer any misue of CCTV to the relevant immediate line manager.

6.3.8 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.

6.4 Investigating Officer (System User)

6.4.1 The role will be undertaken at an operational officer level such as Environmental Health Officer, Enforcement Officer, or equivalent.

6.4.2 Person or persons who have access to live or recorded images or other information obtained by virtue of such system.

6.4.3 Person or persons who are trained to burn images and deal with access requests.

7. Process

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/AUDIT
- COMPLAINTS

EACH TEAM MAY HAVE THEIR OWN PROCESS IN PLACE FOR IDENTIFYING DEPLOYMENT LOCATIONS AND INTERNAL AUTHORISATION, PRIOR TO FORMAL AUTHORISATION AT DIRECTORATE LEVEL.

7.1 CCTV Approval

The procedure covers overt surveillance. 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 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.

6.1.1 Approval Procedure

a) It is required that to ensure compliance with the above requirements, the CCTV Policy, the CCTV Approval Form (Appendix A) and CCTV Policy document (Appendix B) are completed. These should be drawn up between the Investigating Officer and the Nominated/Supervising Officer.

b) No officer, unless they have attended suitable training and are deemed competent by the CCTV Manager, shall take a lead role as an Investigating Officer, Nominated/Supervising Officer or Designated Manager.

c) Despite being an overt surveillance operation there may be a risk of intrusion into people's privacy and a risk of collateral intrusion. To address this with regard to the; necessity, proportionality and collateral intrusion, the CCTV Approval Form (Appendix A) should, under

'Storage and Retention', detail such issues as; how long we intend to have the camera in place for and how regularly we will review the recordings. If necessary an addendum can be added to ensure full provision (although concise) of information to allow a decision to be taken.

d) All applications for authorisation to deploy overt CCTV will be accompanied by a Privacy Impact Statement (PIA) (Appendix C). No application will be authorised without a PIA

6.1.2 Guidance Points for CCTV Approval Form (Appendix A):

In addition to the information provided in the CCTV Policy document (Appendix B), the following shall be included:

a) Column 1 – **'Property'** – Property where CCTV camera is located

b) Column 2 - **'Purpose of CCTV Camera**' – Should identify the purpose of the installation such as primarily for security purposes/in order to ensure the safety and security of staff and visitors/ prevention and/or detection of crime.)

c) 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.

d) Column 4 – '**Nominated Officer'** – this should include the responsibilities and names of the Nominated/Supervising Officer, Designated Manager and Investigatory Officer(s)

e) 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.

f) For purposes of approval the whole document should be read in conjunction, including the appendices which are likely to contain detail and supporting information to the entries made in the form.

6.1.3 Submission of Application

a) The Designated Manager shall ensure that the surveillance and associated documentation is CCTV Policy compliant. Appendix A, Appendix B and the PIA at Appendix C shall be submited direct to the CCTV Manager who is the SPOC for the purpose of this policy. Only

applications submitted according to this process will be deemed as a valid application.

b) In the absence of the CCTV Manager, the Regulation and Enforcement Principal Officer for Community Protection (North Team), will have delegated authority to authorise applications

6.1.4 Authorisation

a) The CCTV Manager will review and authorise on satisfaction of compliance with the CCTV & Guidance policy.

b) On approval authorisation will be confirmed via email including named officers and also a copy will be forwarded to the Data Protection Officer Information Management Team, Riverside House, Rotherham. That email will provide;

i. a confirmatory statement that the application is authorised
ii. the Appendix A, Appendix B and Appendix C documentation
iii. the naming of the Designated Manager, Supervising Officer and/or Investigating Officer taken from the Appendix A and section 3 of the Appendix B (also cc'ing these in the email).

c) The team deploying the CCTV shall keep a documented record of each deployment together with location, supervising and investigating officers. The record will be maintained as a live document and updated appropriately.

d) The CCTV Manager will maintain a master record of all deployed CCTV within the Regeneration and Environment directorate.

6.1.5 Changes to equipment, times and other parameters from the original application

a) Parameters contatined within an application might change prior to deployment or during the lifetime of deployment, these would include, but not exclusively:

i. Change of surveillance times
ii. Change of equipment
iii. Breakdown and repair of equipment
iv. Adjustment of location
v. Vandalism and theft of signs
vi. Vandalism and theft of cameras

b) In all such circumstances the CCTV Manager must be informed immediately and a reviewed and apdated application presented to the CCTV Manager for authorisation.

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

7.2 Purchasing and Deployment (PIA) and (Policy)

6.2.1 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.

6.2.2 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 standards. The Council information governance standards which can be found at: http://rmbcintranet/Directorates/FCS/CIDS/IM/default.aspx

6.2.3 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 al 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 Privacy Impact Assessment template can be found on the Surveillence Commissioner's website at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/634894/Privancy_Impact_Asessment_1.docx . A Privacy Impact Assessment must be completed for each CCTV system in use.

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

6.2.5 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.

6.2.6 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.

7.3 Handling / Monitoring

6.3.1 Where CCTV monitors providing live monitoring for security or other Council officers, 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.

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

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

7.4 Access to Images

Access to images must follow one of the following routes:

7.4.1 Subject Access Request

a) 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.

b) CCTV access requests can be made via the Council's website 'Right to Access'.

c) The Information Management Team will verify the request and identity of the individual and send onto the CCTV Manager.

7.4.2 Police, Other Council's etc

a) 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. Access will only be granted when a formal request has been received.

b) Formal requests will be in the format of a Data Protection exemption form sometimes known as a section 29, CIDS49.

c) The Information Management Team will verify the request and identity of the individual and send onto the CCTV Manager.

7.4.3 Solicitors/Insurances

a) 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. Access will only be granted when a formal request has been received.

b) Formal requests will be in the format of a Data Protection exemption form sometimes known as a section 35, or a court order.

c) The Information Management Team will verify the request and identity of the individual and send onto the CCTV Manager.

6.4.4 Any complaints relating to the use of CCTV must be logged via the Council's complaints procedure.

7.5 Signage and Privacy Notice

6.5.1 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.

6.5.2 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.

6.5.3 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.

6.5.4 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 visible at all times 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 was worn.

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

6.5.6 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. Guidance on the content of Privacy Notices can be found on the Information Management Team intranet site at: http://rmbcintranet/Directorates/FCS/CIDS/IM/default.aspx .

7.6 Storage and Retention

6.6.1 CCTV system images will only be stored for a maximum of six weeks and then overwritten, subject to legal proceedings or ongoing investigations.

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

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

6.6.4 All recorded images are the property and copyright of the Council

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

6.6.7 Where recordings are placed onto discs they will have a unique reference number

6.6.8 All images will be time and date stamped

6.6.9 All images and media wil be confidentially disposed of when no longer needed

7.7 Monitoring/Inspections

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

- CCTV Manager
- Relevant Head of Service
- Members of the Information Management team
- Members of the Corporate Complaints team
- Members of the senior management team
- Members of the Information Commissioner's Office

7.8 Complaints

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

Appendix A – CCTV Approval Form

CCTV APPROVAL FORM

Please complete the following:

Property (Property 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 Principle 1 of the Data Protection Act 1998 (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 B – CCTV Policy

1. Purpose

1.1 The CCTV system installed at the [LOCATION] will be used for the prevention/detection of crime.

1.2 The CCTV system will monitor activity at [LOCATION] A Map of the location to attached to the 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 Principle 1 of the Data Protection Act 1998 (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 signage in situ 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 Principle 5 of the Data Protection Act 1998, 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 practibcable.

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 C – Privacy Impact Assessment

The template for the Privacy Impact Statement can be found at:

http://rmbcintranet/Directorates/FCS/CIDS/IM/Privacy%20By%20Design/PIA_CCTV_Only_Template.pdf