policy

CCTV

Responsible Officer:	Director of Legal and Governance
Approved:	Senior Leadership Team June 2018
Review Date:	June 2021
Ratification:	June 2013
Version:	2
Regulatory Code:	Neighbourhood + Communities Standard Home Standard
Scope:	Group Wide

CCTV Policy

1.0 Introduction

1.1 The use of Closed Circuit Television cameras (CCTV) for surveillance has become a common feature in the UK and has become a part of everyday life for most people. Incommunities aims to provide decent homes and communities in which people will want to live and thrive and recognises that the use of CCTV can assist the business in meeting this objective.

1.2 Incommunities is committed to protecting its staff, tenants, visitors and assets from damage, crime and anti-social behaviour and will use CCTV as an appropriate and accountable means, as part of a range of mechanisms, to improve safety and security. Incommunities recognises that both covert and overt surveillance may be a useful and effective tool for protecting its customers and staff and recognise that it's use must be proportionate.

1.3 As well as providing important safeguards, the use of CCTV also enhances public confidence, assists policing in their detection and investigation of crime and allows for the recording, storing and retrieval of information over an extended period of time. The prominence of CCTV can also act as a deterrent to criminal and anti-social behaviour.

1.4 Incommunities understands that the use of CCTV requires adherence to English laws and regulations, standards and good practice. Images captured by CCTV are covered by the Data Protection Act 1998 (DPA) and all citizens have a right to privacy under the Human Rights Act 1998 (HRA). When implementing and utilising CCTV systems, Incommunities will seek guidance from the Information Commissioners Office (ICO) CCTV Code of Practice and implement the recommended mechanisms within the Code where relevant and appropriate.

2.0 Policy Statement

2.1 This policy defines the roles, responsibilities and mechanisms for the effective and controlled use of CCTV located on or at land and/or premises owned, utilised or managed (whether wholly or solely in relation to CCTV) by Incommunities.

2.2 The policy will:

- Provide clear and unambiguous information on the use of CCTV recording equipment used by Incommunities;
- Provide a framework of instructions for the use, retention, handling and disclosure of CCTV recordings;
- Meet the requirements of the DPA;
- Consider any relevant guidance issued by the ICO;
- Promote a safer working and living environment for staff, tenants and any other persons who may come into contact with the CCTV recording system used by Incommunities.

3.0 Organisational Responsibilities

3.1 The Chief Executive is ultimately responsible for the Group's compliance with the DPA and other relevant legislation and will ensure that the Board is provided with effective assurances of compliance with such legislation. These responsibilities will be delegated to nominated Directors and Managers responsible for Information Governance and CCTV within their portfolio.

3.2 The Director(s) and Manager(s) responsible for CCTV must make sure that the mechanisms set out in this policy are implemented through their management structures and that staff are aware of the requirements of this policy.

3.3 The structure in relation to CCTV is as follows:

Director of Legal & Governance responsible for:

- The strategic direction of the CCTV Service.
- Liaise with the Executive Management Team and Boards in terms of business development and resource allocation.
- Development of CCTV and associated security policies.
- Ensure compliance of the Group with policy and legislation.
- Authorising requests for rapid deployment and covert cameras.
- Risk assessments of Incommunities assets and producing guidance on security.
- Seek new business within the CCTV, Door Entry and Security industries.

CCTV Team Leader is responsible for:

- Administration of the CCTV system.
- Training, development and accreditation of the CCTV Operators and any other appropriate persons.
- Development of partnering arrangements with external agencies such as the emergency services and the Local Authority.
- Assess technologies, their use and integration into the CCTV Control Room.
- Ensuring that the CCTV Control Room is appropriately staffed.
- Assist with the development and welfare of CCTV Operators.

CCTV Operatives are responsible for:

- Monitoring CCTV and Door Entry Systems.
- Completing electronic logs to evidence incidents.

- Reviewing and production of evidence in accordance with the DPA (subject to an appropriate authorisation).
- Ensuring legitimate visitors to the control room have signed the visitor's book and preventing access by unauthorised persons.
- Placing copies of recordings on portable devices in a secure location and placing tampering seals.
- Any other tasks appropriate to their skills and abilities

Specialist Electrical Manager – CCTV and Access Control is responsible for:

- Ensuring the CCTV and Door Entry Systems are technically operational.
- Cameras are installed or deployed in accordance with Tenancy Enforcement Managers instructions.
- Offering the CCTV Team Leader technical guidance on the infrastructure of the CCTV and Door Entry systems.

Director of Legal & Governance is responsible for:

- Ensuring compliance by the Group with the DPA and associated policies.
- Authorising requests for rapid deployment and covert cameras.
- Processing Subject Access Requests and authorising disclosure of CCTV requests.

The Specialist Electrical Team is responsible for:

- Stand-alone CCTV systems

3.4 The Data Controller will be appointed and the relevant notification will be made to the Information Commissioners Office (ICO).

3.5 All Incommunities employees are required to comply with this policy and report any concerns or incidents relating to CCTV and its use within Incommunities to their line manager. These reports must then be passed immediately to the CCTV Team Leader. Where such reports identify a potential breach of the DPA, the Data Protection Officer must be notified immediately.

4.0 Objectives

4.1 The purpose of the CCTV system is to monitor the assets, including land, owned by Incommunities (or their clients) in order to:

4.1.1 Assist in the detection of crime and/or anti-social behaviour;

4.1.2 Act as a preventative measure in order to deter crime and/or anti-social behaviour

4.1.3 Reduce the fear of crime and/or anti-social behaviour in and around Incommunities' properties and on their land;

4.1.4 To assist the Neighbourhood Housing Teams and Tenancy Enforcement Team in relation to cases of nuisance and/or anti-social behaviour, harassment, damage and/or any other situation as deemed appropriate

4.1.5 Assist the Police (and any other relevant external agency) with evidence of criminal behaviour and acts of public disorder.

4.1.6 To assist in enforcing the obligations of tenants under our tenancies

5.0 Security and Premises

5.1 The CCTV monitoring system is located in a central CCTV Control Room (the 'Control Room') which is located at the 'Hillam Road'. The location of the Control Room may change from time to time.

5.2 Access to the Control Room is restricted to authorised personnel as identified in Schedule 1.(list of people allowed into the building) No one else is permitted access to the Control Room or CCTV monitoring systems unless authorised by the CCTV Team Leader or the Director of Legal and Governance .

5.3 Access to the Control Room is by fob. Fobs will be issued only to personnel who require access to the Control Room as part of their day-to-day role. Authorised personnel must keep fobs secure and are not permitted to pass this fob to other personnel, whether or not they are employed by Incommunities.

5.4 The Control Room will be staffed by authorised personnel at all times. Should the Control Room have to be left unattended due to unforeseen circumstances, the CCTV Team Leader must be made aware immediately and the alarm set.

5.5 A log book will be maintained at the Control Room logging the details of all personnel entering and exiting the Control Room. Any person entering or leaving the Control Room, whether employed or not by Incommunities, must record their details, including the time and purpose of their visit, in the log book.

5.6 Visits to the Control Room must be by prior arrangement and with authorisation from the CCTV Team Leader, or in her absence, a nominated person. In cases of emergency only, Emergency Services personnel (Police, Fire Service, and Ambulance Service) may be permitted entry to the Control Room. Where such emergency access is granted, a log of the persons entering and the reason for their entry should be recorded in the log book located at the Control Room.

6.0 Data Protection & Confidentiality

6.1 All staff are required to complete mandatory Incommunities data protection training as part of their induction and regular refresher training. Those staff who are identified as having access to CCTV and other monitoring systems

will be required to complete and pass a Security Industry Authority (SIA) approved qualification in Public Space Surveillance (or equivalent) which will provide appropriate staff with enhanced data protection training.

6.2 All staff with access to the Control Room and/or any monitoring systems will be required to sign a 'declaration of confidentiality' to confirm that they will only record and/or disclose CCTV images or any other monitoring information as part of their legitimate duties and that they will abide by the provisions of the DPA at all times. The duty of confidentiality and the expectation that staff will abide by the DPA will apply whether or not the declaration has been completed and signed.

7.0 Camera Operation

7.1 The use of CCTV and other monitoring systems will be for the objectives outlined in section 4 of this policy only. Any person observing the use of CCTV or any other monitoring equipment which is not in accordance with this policy, or is otherwise inappropriate, must report such use to the CCTV Team Leader immediately. In the absence of the CCTV Team Leader the use should be reported to the Director of Legal and Governance. Where such use may constitute a breach of the DPA, this must be reported to the Data Protection Officer.

7.2 Overt and Covert cameras should only be used directly to record particular groups or individuals if this is justified by reference to the purpose of the system as outlined in section 4 of this policy. Groups and individuals should not be target recorded unless there is a legitimate reason and an authorisation has been obtained from the Director of Legal and Governance. Nothing however in this clause shall prevent a CCTV Operative from targeting a group or individual(s) on a live feed during an incident or suspected incident or when observing suspicious behaviour.

8. Incident Logging

8.1 The Control Room must maintain an electronic log of significant events or incidents. Operators must log these events and incidents in a manner which is sufficient to identify and retrieve the recording without unnecessary delay. The log shall contain a report of the incident.

8.2 Reports must be factual statements of what the Operator has witnessed. These reports must be made without delay.

8.3 Examples of what constitute an incident include (but are not limited to):

- Criminal damage
- Assault
- Urinating in a public place
- Graffiti
- Drug use and/or dealing

- Arson
- Public disorder (rowdy, drunken, abusive behaviour, etc.)
- Illegal or unacceptable use of any vehicle(s)
- Dog fouling
- Fly tipping
- Prostitution

8.4 Operators should be mindful that significant events may lead to or indicate incidents. As a result, all significant events must be logged.

8.5 Examples of what constitute a significant event include (but are not limited to):

- Dogs in flats
- Large numbers of people coming and going from a property/area
- Gangs
- Vulnerable individuals acting in a strange manner
- Suspicious behaviour such as loitering

8.6 Incident logs must be dealt with as follows:

8.6.1 An electronic copy of the incident report shall be saved in a clearly marked file saved on the secure and encrypted servers within the Control Room.

8.6.2 An electronic copy shall be sent to the CCTV Team Leader, Neighbourhood Housing Team, and the Tenancy Enforcement Team immediately upon completion.

8.7 Incident reports are restricted documents and must be treated accordingly. Any individual who has access to such documents must keep their contents confidential, unless released in the legitimate course of their business.

8.8 When completing incident reports Operators must be mindful that these may be used in court proceedings and must therefore be completed in a clear, concise and professional manner.

8.9 Where facial recognition technology is in use, Operatives must manually check any matches to ensure the system has correctly identified an individual before passing on such information to any other person, whether internal or external.

9.0 Management of Recorded Material-Overt

9.1 The system records digital images of a particular place at any given time. Recordings are made constantly from each live camera feed onto a digital hard drive. The digital hard drives are located at a local level along with the camera and must be kept secure at all times.

9.2 Any breaches or potential breaches of security of the hard drive must be reported to the CCTV Team Leader immediately. In the absence of the CCTV

Team Leader, reports should be made to the Director of Legal and Governance. Where such breach may amount to a breach of the DPA, a report must also be made to the Data Protection Officers.

9.3 Recordings are retained on the hard drive for a period of 28 days (or any other such period as recommended by the Home Office or Police) following which they are automatically deleted by being "over-recorded" by the system. The Data Protection Officer may agree to recordings being kept for a longer or shorter period of time.

9.4 No person shall have access to the recorded material, save in accordance with the procedure set out in section 10 below.

10.0 Access to Recordings

10.1 Recorded material should be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded on the CCTV system are protected and that the material can be used as evidence in court where appropriate.

10.2 Access to recorded material will only be granted for the purpose for which the system was established (as outlined in section 4 of this policy) and in accordance with the provisions of the DPA.

10.3 Recorded images must be viewed in a restricted area, such as in the Control Room or in a designated secure office, and must only be viewed by authorised persons in the legitimate course of their work.

10.4 Subject to section 10.5 below, requests for copies of recordings must be made to the Data Protection Officer. Recordings must not be released unless an authorisation has been evidenced and this must be recorded in one or more CCTV Release Register(s).

10.5 From time to time Police Officers or other law enforcement agencies may request footage to be released in relation to the prevention or detection of crime and/or disorder. The officer should be asked to complete an Enforcement CCTV Release Form (as identified at Appendix 2). Again this release must be recorded in a CCTV Release Register and be authorised by the Data Protection Officer.

10.6 Where requests for CCTV are made and provided, a master copy should be made and retained by Incommunities in a secure location.

10.7 Any request for CCTV by an individual shall be treated as a Subject Access Request. Subject Access Requests will be processed in line with the Data Protection Policy.

11.0 Responsibilities

11.1 Signs must be displayed notifying individuals that CCTV is in operation in areas where CCTV surveillance is being carried out. This will be advertised by using prominently placed signs at the entrance of the CCTV zone and reinforcing this with further signs inside the area. The number of signs displayed shall be dependant and commensurate to the prominence of the system, i.e. where the system is not clearly visible, more signs will be displayed.

11.2 Signage shall be:

- Clearly visible and readable;
- Identify that Incommunities operate the system (unless this should be obvious due to the location);
- Provide basic contact details such as a telephone number, website address or address;
- Where the purpose of the use of the CCTV is not obvious, provide basic details of the use or an address or website where these details can be found.

11.3 CCTV equipment will be regularly checked by the Specialist Electrical Team to ensure that the system is maintained in a good and effective working order. These checks will include (but are not limited to):

- Ensuring that live as well as recorded pictures produce good clear pictures;
- The compressions settings are appropriate for the CCTV recording;
- The recording medium is set up in such a way to prevent corruption;
- The date and time stamp are correct;
- The location of the CCTV cameras are appropriate;
- Where automatic facial recognition technology is used, cameras are placed in areas where facial images are clearly captured;
- Where a wireless transmission system is used, sufficient safeguards are in place to prevent interception.

11.4 Regular reviews of the CCTV system will be undertaken by the CCTV Team Leader, or a person nominated by her, in order to confirm that there is a necessity for the system and that the quality of the system is satisfactory.

12.0 Retention of Recordings

12.1 Records must only be kept for as long as is necessary and must be destroyed when no longer needed. For guidance on periods of retention, the Data Retention Policy should be referred to or advice taken from the Data Protection Officers.

12.2 As a matter of course, CCTV recordings shall be retained on the CCTV system for a period of 28 days before being automatically deleted by way of over-recording.

12.3 Where recordings have been transferred onto playable media (such as DVDs), they must be kept in a secure location. No person is permitted to gain access to this storage location without authorisation from Data Protection Officer.

13.0 Installation and maintenance of CCTV cameras- Overt

13.1 CCTV Cameras (whether temporary or permanent), must only be installed with the prior authorisation of the Director of Legal and Governance

13.2 The installation of cameras will be in line with good practice guidance as set out by the Information Commissioners Office and reflect the risks to that particular location.

13.3 For all new CCTV systems (whether temporary or permanent), Specialist Electrical Team will provide advice in relation to the appropriateness of the location of the cameras, their capabilities and the technology used to record and transmit captured images securely. CCTV systems should not be installed without authorisation of the Director of Legal and Governance

13.4 CCTV cameras, network hardware and digital recorders will undergo annual cyclical checks to ensure that they are operating effectively. The Specialist Electrical Team shall be responsible for such checks.

14.0 Deployable Cameras

14.1 Deployable CCTV cameras are mobile closed-circuit television camera's which can be quickly deployed in appropriate locations to evidence and reduce Anti-Social Behaviour and Crime within the district of Bradford. These cameras are capable of transmitting live footage to the Control Room via a mobile phone signal.

14.2 Any requests for the deployment of mobile cameras will be made in line with the Deployable Cameras Protocol attached at Appendix 3.

14.3 The CCTV Team Leader will review the request and provide advice in relation to the availability of the cameras and any other relevant logistical considerations.

14.4 Should a third party power supply be used for benefit of the deployment; Incommunities will compensate for the energy used at the appropriate rate.

14.5 The retention, access and storage of all deployable CCTV recordings and images will be in accordance with the relevant sections of this Policy.

15.0 Stand Alone CCTV Systems

15.1 Incommunities has a number of sites that benefit from CCTV cameras but are not connected to the CCTV Control Room. Captured images are recorded securely on site.

15.2 All stand-alone systems will be maintained on a day to day basis by the Specialist electrical Team.

15.3 The Specialist Electrical Team will review the suitability, quality and any cyclical works required to stand alone CCTV systems on a regular basis.

16.0 Authority / Licences

16.1 All necessary licences will be obtained for the operation of CCTV cameras from the Security Industry Authority (SIA) and any other regulatory body that may from time be responsible for the issue of public space licences in accordance with the Private Security Industry Act 2001.

16.2 It will be the responsibility of the CCTV Team Leader to ensure that all necessary licences are obtained for the organisation and its employees.

17.0 Breaches of Policy

17.1 Any breaches of this CCTV policy may be considered as a form of misconduct and disciplinary action may be taken against any relevant individuals.

18.0 Monitoring and Review

18.1 The overall operation of the policy will be monitored by the Director of Legal & Governance

18.2 The CCTV Team Leader and Tenancy Enforcement Manager will conduct an annual review of compliance with this policy and report the number of authorisations granted in the preceding year to the Director of Legal and Governance.

18.3 This policy will be reviewed every three years.

19.0 Associated Policies, etc.

- Covert Surveillance Policy
- Anti-Social Behaviour & Hate Crime Policy
- Data Protection Policy
- Hate Crime Policy
- Witness Support Statement
- Deployable camera protocol

APPENDIX 1

Authorised Personnel

Persons authorised to access Control Room:

- CCTV Team Leader
- CCTV Operatives

All other persons must sign in to the Control Room as a visitor.

Appendix 2

Incommunities CCTV

Request to review & burn CCTV
Data Protection Act 2018, Schedule 2, part 1, paragraph 2

Unique Reference number: | Incoms - |

Section A – Request details

Requesting Officer:

Organisation & position/rank:

Contact details:

Date of Request:

Date and time of incident:

Exact location of incident:

Crime No./Incident Log No

Reason for request: Prevent/detection of crime ☐ ASB ☐

Apprehension or prosecution of offenders ☐ Other ☐ Please specify

Details of incident, suspects, vehicles or information required from CCTV:

Section B – Production details

CCTV Operator:

Date & time:

Review ☐ Burn ☐ Stills ☐

Master CD exhibit no:
Copy CD exhibit no:
Still picture(s) exhibit no's:

Incommunities CCTV

Request to review & burn CCTV
Data Protection Act 2018, Schedule 2, part 1, paragraph 2

Notes / Details:

Signatories:

Burning off or producing officer:

Print name

Signature Date

Reviewing or collecting officer:

Print name

Signature Date

Appendix 3

OVERT CAMERAS PROTOCOL

Deployable CCTV cameras are mobile closed-circuit television camera's which can be deployed in appropriate locations in order to tackle local issues. This procedure is intended to ensure that the use of the mobile CCTV camera is in accordance with the CCTV Code of Practice issued by the Data Protection Commissioner. In the event of any doubt or ambiguity refer to that Code and Incommunities CCTV Policy for clarification.

Incommunities occasionally deploy cameras in order to assist partner agencies in line with objectives outlined in section 4 of this policy.

In order to ensure that the cameras are deployed to the most appropriate location/places in need, Incommunities has established an application process for the deployment of the cameras.

Before each deployment of the CCTV cameras an assessment of the reasons for using the system and the appropriateness of its use must be carried out and the result documented. This means considering and recording what the problem is which the deployment is intended to address. Identifying that there is already prima facie evidence of that problem, demonstrating why this surveillance is necessary to secure further evidence and that the intrusion of surveillance is proportionate to the level of the problem. This must be a purpose within Schedule 2 and Schedule 3 of the Data Protection Act 1998.

Should officers believe that there is a need for the deployment of Overt CCTV cameras, they should complete the application form attached at appendix and forward this to the CCTV Manager in accordance with the procedure below:

Stage 1

The Tenancy Enforcement Manager (TEM) will discuss the request with the TEO and decide whether the deployment request should be accepted after considering all the relevant facts.

When making this decision the following will be considered:

- Nature of the problem
- Length of time the issue has been ongoing
- Actions taken to try and combat issue
- Effect on local residents, businesses, visitors, etc
- Number of people affected
- Any vulnerability factors
- Any legal issues

Where there is more than one request for the cameras to be deployed, the TEM will make a decision as to which request (if any) should be treated as the most urgent.

The TEM will report their decision to the CCTV Team Leader

Stage 2

Before any application for the deployment of CCTV cameras is made, the TEO should make enquiries with the CCTV Team Leader and Specialist Electrical Team in order to ascertain whether the deployment is available from a location/logistical perspective. Due to the size and design of the units, some locations will not be appropriate for the deployment of mobile CCTV cameras.

The application form (attached as appendix 1) should be completed by the relevant Tenancy Enforcement Officer (TEO), then reviewed and authorised by the Tenancy Enforcement Manager (TEM). Once authorised by the TEM the TEO should send the application to the Team Leader.

Stage 3

The Specialist Electrical Team and TEO will carry out a site visit to determine the most appropriate location and advise of the availability of the cameras and any other relevant logistical consideration

The location of any proposed deployment must be carefully considered and must comply with the first data protection principle. Cameras must be sited in such a way as to monitor only those spaces which are intended to be covered by the equipment. If domestic areas such as gardens border the area which is intended to be covered then the equipment should be restricted so as to avoid recording those areas or operators directed to recognise the privacy implications of such spaces being covered.

If the Specialist Electrical Team considers that the deployment of the camera is not appropriate in light of the above, he should notify the Tenancy Enforcement Manager.

Stage 4

Before the cameras are deployed an initial check should be made by the Specialist Electrical Team to ensure that the images which will be recorded are adequate for the purpose of the deployment, for example to ensure that if the purpose of the deployment is to detect anti-social behaviour and crime that the images are of sufficient quality to enable the perpetrators to be identified for the purpose of Court action. Further, signs should be placed so that the public are made aware that they are entering an area which is covered by surveillance. The signs must be clearly visible and legible to members of the public and shall contain the following information:

- The identity of the organisation
- The purpose of the scheme
- The contact details of the organisation.

Stage 5 (disputes)

Where a request for deployment is refused, the relevant officer does have a right of appeal. Should an officer wish to appeal they should put their appeal in writing to the Director of Legal and Governance clearly outlining the reasons for their appeal. This will then be passed to the TEM who will review their decision based upon the appeal reasons and report back to the CCTV Team Leader as to whether the appeal is upheld or not. CCTV Team Leader will then take action as appropriate.

If officers are unsure as to whether the deployment of mobile cameras could assist a particular issue that they are facing they should seek advice from the Tenancy Enforcement Team.

Miscellaneous

The retention, access and storage of all CCTV recordings and images will be in accordance with the Incommunities CCTV Policy.

Monthly review/spreadsheet/removal

APPENDIX 1 - DEPLOYABLE CAMERA PROTOCOL
CCTV Deployment Application Form

Name…….

Location/office ……..

Position/Rank…….

Location of deployment

……

……

……

……

Current Issues at location

……

……

……

……..

……

……

……..

……

……

Who is/are effected by the issues (include approx. numbers)

……

……

……

……

……

……

What has already been done in order to tackle the issue(s)

……..
……
……
……
……
……
……

What is hoped to be achieved by deployment (e.g. evidence for ASBI, crime deterrent, public confidence)

……
……
……
……
……
……
……
……..

Signed…… Date……

Line Manager Authorisation to confirm agrees with and support application

Signed…… Date……

Print name……Rank/Position……

Date passed to TEM ……..

For completion by TEM

Date received……

Decision: Deployment Authorised / Not Authorised

Date ……

Reasons……
……
……
……
……
……
……
……
……..

Priority (if applicable):

- Immediately
- Next available
- Other (details)

……

Authorised by:

- TEM
- DL&G

Signed…….

Date ……..

Signed…….

Date ……..

For completion by CCTV Team Leader

Date received……..