CCTV Policy

Reigate & Banstead Borough Council

1st August 2019

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate

1. Introduction 1.1. Reigate and Banstead Borough Council (RBBC) operate CCTV cameras. The use of CCTV cameras by a public authority is a legally regulated activity. CCTV provide both the public and RBBC significant benefits. The use of CCTV must always be balanced against an individual's right to privacy.

1.2. This policy has two purposes. The first, is to set clear guidelines to those within the council on how to manage CCTV in a manner that complies with RBBC's legal requirements. The second, is to provide confidence to the public that CCTV is only operated for set purposes and in a transparent manner.

2. Policy Scope 2.1. This policy applies to any member of staff who is responsible for CCTV within RBBC. Currently, those members of staff fulfil the following roles:

Name	Role
Ross Spanton	Community Safety Officer
Sarah Crosbie	Partnerships Team Leader
George Potter	Building Facilities Surveyor
Morag Williams	Head of Neighbourhood Operations
Ben Murray	Senior Manager for Regulatory Services (JET)
Ian Orrick	Programme Delivery Manager at the Harlequin Theatre
Alison Robinson	Housing Strategy and Projects Manager

2.2. Those fulfilling the roles in the list above are referred to as CCTV Owners in this Policy.

2.3. If you would like to establish the use of CCTV in your service area and are not fulfilling one of the roles listed above, you must first have a consultation with the Data Protection Officer (DPO).

2.4. RBBC are considered the Data Controller of any personal data captured by the CCTV scheme it operates. RBBC are also Joint Controllers with Surrey Police in Reigate for CCTV which falls within the remit of the Public Realm.

3. Definitions

3.1. CCTV 3.1.1. CCTV is the commonly used abbreviation for Closed Circuit Television. CCTV is the use of video cameras to transmit images (and sometimes audio) to a specific place, on a limited set of monitors. CCTV takes many forms. In RBBC, some of these forms include: 3.1.1.1. Pan-tilt-zoom

3.1.1.2. Static Camera

3.1.1.3. Mobile units

3.1.2. CCTV can be used overtly or covertly. Different rules will apply depending on which type is chosen. RBBC only operate overt CCTV.

3.2. Data Controller 3.2.1. The term Data Controller is derived from Article 4 of the General Data Protection Regulation (GDPR). It applies to the party that determines the purposes and means of processing personal data.

3.2.2. In most instances, RBBC will be the Data Controller for any Personal Data captured by cameras that they operate.

3.3. Data Processor 3.3.1. The term Data Processor is derived from Article 4 of the General Data Protection Regulation (GDPR). It applies to the party that processes personal data on behalf of the Data Controller.

3.3.2. RBBC often use third parties to operate as Data Processors. At RBBC this is generally the term applied to the party who have access to the cameras for maintenance purposes.

3.4. Personal Data 3.4.1. Personal Data means data which relates to a living individual who can be identified, either:

3.4.1.1. From that data, or

3.4.1.2. From that data and other information which is in the possession of or is likely to come into the possession of the data controller.

3.4.2. Images or audio captured by CCTV will constitute Personal Data where the individual could be identified.

3.5. Relevant Legislation 3.5.1. The use of CCTV by public authorities requires adherence to the relevant legislation. This includes the Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, and the Protection of Freedoms Act 2012.

3.6. Relevant Guidelines 3.6.1. The Information Commissioner's Office and the Surveillance Camera Commissioner have issued Codes of Practice. Public authorities, such as RBBC, must have regard to this guidance when operating CCTV.

4. Principle – surveillance by consent

4.1.1. CCTV by RBBC must always be characterised by the concept of implied consent from the community. According to the Relevant Guidelines there is a legitimacy in surveillance where there is general public consensus which follows on from transparency about what is happening, a demonstration of integrity and accountability in the act of surveillance.

4.1.2. RBBC will ensure that this characterisation is achieved through following the requirements in this policy, set out below.

4.1.3. This is especially important for RBBC as the use of CCTV has the potential to interfere with a person's right to family and private life. RBBC must therefore follow the appropriate process to ensure adequate safeguards are in place.

5. Establishing CCTV – a checklist

5.1. Any member of staff who is responsible for or who is authorised by the DPO to operate CCTV within RBBC, must only do so after:

5.1.1. Completing a Data Protection Impact Assessment (DPIA)

5.1.1.1. See the RBBC DPIA Policy and Template

5.1.2. Arranging for GIS Mapping 5.1.2.1. Contact the GIS team to enable this to be automated.

5.1.3. Updating relevant privacy notices/ work area specific instructions (also known as CCTV Protocols.

5.1.3.1. These should set out internal processes and safeguards including circumstances in which CCTV may be used and training guidelines.

5.1.4. Reading and being able to confidently meet the requirements of this CCTV Policy.

5.1.5. Updating their Information Asset Registers to make sure the new dataset is accounted for.

5.2. All activities in relation to this checklist should be documented and kept as evidence to support our compliance to the Relevant Legislation and Guidelines.

6. Managing CCTV – Annual Reviews

6.1. The use of surveillance cameras by RBBC must always be so as to provide a proportionate and effective solution that is in pursuit of a legitimate aim and to meet a pressing need.

6.2. The Relevant Guidelines state that a “system operator should review the continued use of a surveillance camera system on a regular basis, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose for deployment.” (Surveillance Code – 4.10.1)

6.3. Therefore, on an annual basis, each grouping of cameras, covered by a Part 1 DPIA, should be reviewed to assess their ongoing justification and given sign off by the CCTV Owner.

6.4. The questions that need a response in the Annual Review are included in the DPIA template form.

6.5. You must always diarise when the next annual review should be completed by.

6.6. The completion of this annual review may be delegated by the CCTV owners to the member of their team they deem most appropriate, or to a third-party, where there is a suitable contract in place. However, the CCTV owner will remain accountable for the quality of the annual review and for sign off, no matter who they select as responsible for its completion.

7. Requests for CCTV Footage

7.1. The Relevant Legislation allows individuals to request copies of their Personal Data from Data Controllers, such as RBBC. CCTV footage constitutes Personal Data and so are in scope of the Relevant Legislation. These requests are known as a Subject Access Request (SAR) or as a Data Subject Access Request (DSAR).

7.2. These requests can be made in any way. They can be verbal or written, made by members of the public, staff, our suppliers. They often are made directly to the Data Protection Officer, but this will not always happen due to the myriad of routes a request can take. Therefore, all staff who work in an environment supported by CCTV may be asked about a DSAR.

7.3. It is the CCTV owner’s responsibility to ensure that all staff who have access to their cameras are aware of what to do if someone makes a DSAR. (They should inform the CCTV owner and immediately contact the Data Protection Officer for further instruction.)

7.4. Nobody should respond to a DSAR without consulting the Data Protection Officer first.

7.5. CCTV owners must ensure that when creating and maintaining CCTV assets, all systems have the relevant infrastructure to be able to provide access to the Personal Data.

8. Removing CCTV

8.1. When there is no longer a case for maintaining the CCTV, for example, the pressing need or purpose no longer stands, or the cameras are not working
well, then there needs to be a clear process in place for the removal and safe disposal of the assets.

8.2. The form of this process will be different depending on the type of CCTV in use. It will be up to the CCTV owner to determine what is most appropriate. They may seek the support of the Data Protection Officer in making this decision.

8.3. When the CCTV has been removed, it is up to the CCTV owner to update all documentation, including:

8.3.1. The DPIA

8.3.2. The GIS Mapping tools

8.3.3. Information Asset Registers

9. Any Questions

9.1. If anything in this Policy is unclear or you have suggestions for aspects to be included in future versions, please contact the Data Protection Officer who will be able to assist you.

9.2. The DPO will also be able to help you find more resources such as the CCTV Codes of Practice, issued by the regulators, and provide Data Protection Impact Assessment Training.

Review and Approval
This policy will be reviewed regularly and may be altered from time to time in light of legislative changes or other prevailing circumstances.

Next Review Date
All policies should be reviewed at least annually or when significant change occurs to the policy subject matter.

The next review date for this policy is 01.08.2020.

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate