CCTV Policy

Responsibility: Full Council

Review Cycle: Every three years, or earlier in the event of legislative changes.

Date of Adoption / Renewal	Resolution Number
12the March 2024	10457

CCTV Policy

1. Introduction

1.1 Closed circuit television (CCTV) is installed at the Council premises for the purpose of staff and premises security. Cameras are located at various places on the premises, and images from the cameras are recorded.

1.2 The use of CCTV falls within the scope of the Data Protection Act 1998, the General DataProtection Regulation, and the Data Protection Act 2018. To comply with the requirements of the law, data must be:

- Fairly and lawfully processed.
- Processed for limited purposes and not in any manner incompatible with those purposes.
- Adequate, relevant, and not excessive
- Accurate
- Not kept for longer than is necessary.
- Processed in accordance with individuals' rights.
- Secure

2. Data Protection Statement

2.1 The Operations Manager is the Data Controller for the Town Council under the Act.

2.2 CCTV is installed for the purpose of Health and Safety, Security of staff and or premises, crime prevention and or detection.

2.3 Access to stored images will be controlled on a restricted basis by the Data Controller.

2.4 Use of images, including the provision of images to a third party, will be inaccordance with the Councils Data Protection Registration.

2.5 CCTV may be used to monitor the movements and activities of staff and visitors whilst on the premises.

2.6 CCTV images may be used where appropriate as part of staff disciplinary procedures.

2.7 External and internal signage are displayed on the premises stating of the presence of CCTV and indicating the names of the system owner being the Town Council and a contract number during office hours for enquiries.

3. Retention of Images

3.1 Images from cameras are recorded on a secure hard drive ("the recordings"). Where recordings are retained for the purposes of security/ investigation of staff and premises, these will be held in secure storage, and access controlled. Recordings which are not required for the purposes of security of staff, and premises, will not be retained for longer than is necessary **(28-day *retention period)*.**

3.2 In the event of a failure of an automatic power backup facility (which may operate in the event of a main supply power failure) images may be irretrievable.

4. Access to Images

4.1 It is important that access to, and disclosure of, images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes.

5. Access to Images by Council Staff

5.1 Access to recorded images is restricted to the Data Controller, who will decide whether to allow requests for access by data subjects and/or third parties (see below).

5.2 Viewing of images must be documented as follows (**Appendix B**):

- The name of the person viewing, or otherwise accessing, the recordings.
- The date and time of viewing of the recordings
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties)
- The reason for the viewing
- The outcome, if any, of the viewing

6. Removal of Images for use in legal proceedings

6.1 In cases where recordings are copied/ downloaded from secure storage for use in legal proceedings, the following must be documented (**Appendix B**):

- The name of the person copying/ downloading from secure storage, or otherwise accessing, the recordings.
- The date and time of copying/ downloading the recordings.
- The reason for duplication.
- Specific authorisation from the Town Clerk/ Deputy Clerk in the TC absence for copying/ downloading and provision to a third party.
- Any crime incident number to which the images may be relevant.
- Name of person download handed/ sent too.
- The signature of the collecting police officer, where appropriate

7. Access to images by Third Parties

7.1 Requests for access to images will be made using the 'Application to access to CCTV images' form(**Appendix A**).

7.2 The data controller will assess applications and decide whether the requested access will be permitted. Release will be specifically authorised. Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. For example, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- The press/media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account

- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

8. Disclosure of Images to the Media

8.1 If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of other individuals must be disguised or blurred so that they are not readily identifiable.

8.2 If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editingcompany, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use theimages in accordance with the instructions of the data controllers.
- The written contract makes the security guarantees provided by the editing company explicit.

9. Access by Data Subjects

9.1 This is a right of access under the 1998 Act, the GDPR and the DPA 2018. Requests for access to images will be made using the 'Application to access to CCTV images' form (**Appendix A**). The requestor needs to provide enough information so that they can be identified in the footage, such as a specific date and time, proof of their identity and a description of themselves. Any footage provided may be edited to protect the identities of any other people.

10. Procedures for Dealing with an Access Request

10.1 All requests for access by Data Subjects will be received/ reviewed by the Town Clerk/ or Deputy Clerk in the TC absence. On the request of the Town Clerk, the data controller will locate the images requested. The data controller will determine whether disclosure to the data subject would entail disclosing images of third parties.

10.2 The data controller will need to determine whether the images of third parties are held under a duty of confidence. In all circumstances the Council's indemnity insurers will be asked to advise on the desirability of releasing any information.

10.3 If third party images are not to be disclosed, the data controllers will arrange for the third-party images to be disguised or blurred. If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controller.
- The written contract makes the security guarantees provided by the editing company.

10.4 The Town Clerk will provide a written response to the data subject within 21 days of receiving the request setting out the data controllers' decision on the request.

10.5 A copy of the request and response should be retained.

11. Complaints

11.1 Complaints must be in writing and addressed to the Town Clerk. Where the complainant is a third party, and the complaint or enquiry relates to someone else, the written consent of the data subject is required. All complaints will be acknowledged within seven days, and a written response issued within 21 days.