# AMBERLEY PARISH COUNCIL

# CCTV POLICY AND CODE OF PRACTICE

## Introduction

Closed circuit television (CCTV) is installed at the village car park for the purpose of security. A camera is located on the green electricity kiosk, and images from the cameras are recorded.

The use of CCTV falls within the scope of the Data Protection Act 1998, the General Data Protection Regulation and the Data Protection Act 2018. In order 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

## Data Protection Statement

1. Amberley Parish Council are the Data Controllers under the Act.
2. CCTV is installed for the purpose of security.
3. Access to stored images will be controlled on a restricted basis within the Council (as agreed by the Clerk/RFO as Data Protection Officer).
4. Use of images, including the provision of images to a third party, will be in accordance with the Councils Data Protection registration.
5. CCTV may be used to monitor the movements of vehicles whilst in the car park and when entering and leaving.
6. External signage is displayed in the car park stating the presence of CCTV.

## Retention of Images

Images from the camera are stored locally onto a secure hard disk ('the recordings'). Recordings are retained for 25 days.

## Access to Images

Access to, and disclosure of, images recorded by the CCTV is restricted and carefully controlled by the Data Protection Officer, 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.

## Access to Images by Council Staff

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

Viewing of images must be documented as follows:

- The name of the person accessing the hard disk storage, or otherwise accessing, the recordings
- The date and time of removal 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
- The date and time of replacement of the recordings

CCTV images can also be accessed via a cloud connection on the clerk's and chairman's phone, but these are not stored or recorded.

## Removal of Images for Use in Legal Proceedings

In cases where recordings are removed from the hard disk storage for use in legal proceedings, the following must be documented:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The reason for removal
- Specific authorisation of removal and provision to a third party
- Any crime incident number to which the images may be relevant

- The place to which the recordings will be taken
- The signature of the collecting police officer, where appropriate
- The date and time of replacement into secure storage of the recordings

## Access to Images by Third Parties

Requests for access to images will be made using the 'Application to access to CCTV images' form (which is at **Appendix 1**).
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)

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

## Disclosure of Images to the Media

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.

If the CCTV system does not have the facilities to conduct 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 controllers
- The written contract makes the security guarantees provided by the editing company explicit

## Access by Data Subjects

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 (which is at **Appendix 1**). 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.

## Procedures for Dealing with an Access Request

All requests for access by Data Subjects will be dealt with by the Clerk/DPO. 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.

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.

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 conduct 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 controllers

- The written contract makes the security guarantees provided by the editing company explicit

The Data Controller will provide a written response to the data subject within **30** days of receiving the request setting out the data controllers' decision on the request.

A copy of the request and response should be retained.

## Complaints

Complaints must be in writing and addressed to the 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.

# Appendix 1 Data Protection Act/General Data Protection Regulation - Application for CCTV Data Access

***ALL Sections must be fully completed***. Attach a separate sheet if needed.

| | |
|---|---|
| Name and address of Applicant | |
| Name and address of "Data Subject" – i.e., the person whose image is recorded | |
| If the data subject is not the person making the application, please obtain a signed consent from the data subject opposite | Data Subject signature……. |
| If it is not possible to obtain the signature of the data subject, please state your reasons | |
| Please state your reasons for requesting the image | |
| Date on which the requested image was taken | |
| Time at which the requested image was taken | |
| Location of the data subject at time image was taken (i.e., which camera or cameras) | |
| Full description of the individual, or alternatively, attach to this application a range of photographs to enable the data subject to be identified by the operator | |

| | |
|---|---|
| Please indicate whether you (the applicant) will be satisfied by viewing<br>the image only | |

On receipt of a fully completed application, a response will be provided as soon as possible and in any event within **30** days.

| **COUNCIL USE ONLY** | **COUNCIL USE ONLY** |
|---|---|
| Access granted (tick) | |
| Access **not** granted (tick) | Reason for not granting access: |
| Data Controller's name:<br><br>Signature:<br><br>Date: | |