

Lydiard Millicent Parish Council

CCTV System Policy and Code of Practice

CONTENTS

1. INTRODUCTION
2. KEY OBJECTIVES OF THE CCTV SYSTEM
3. MANAGEMENT OF THE SYSTEM
4. ACCOUNTABILITY
5. PRIVACY AND DATA PROTECTION
6. VIEWING OF THE RECORDED/LIVE IMAGES
7. SITING OF CAMERA AND SIGNAGE
8. ACCESS REQUESTS
9. RETENTION OF IMAGES
10. COMPLAINTS
11. CODE OF PRACTICE

1. Introduction

- 1.1 Following the installation of a Closed-Circuit Television (CCTV) system (the System). The purpose of this Policy and Code of Practice is to regulate its management, operation and use. Also, to ensure that the community has confidence that surveillance cameras are deployed to protect and give support. The aim is to ensure that the System is not abused or misused and that it is correctly and efficiently installed, managed and maintained.
- 1.2 The System comprises wireless dome cameras, located in prominent positions around the Jubilee Club House and Recreation Field. Images are not monitored continuously. The Parish Council securely stores images recorded by the System for a limited period. Access to images is restricted to Network Connections UK Ltd t/a RedHand and Council Staff. Access is also authorised for the Police and with their prior written consent, images may be released to the media via the Police for the purpose of crime detection.
- 1.3 The Parish Council is committed to the need for the System to comply with the Data Protection Principles set out in the Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act, Regulation of Investigatory Powers Acts 2000 (if applicable) The Home Office Surveillance Camera Code of Practice.
- 1.4 This Policy and Code of Practice will be subject to review, to include consultation with interested parties where appropriate.
- 1.5 Lydiard Millicent Parish Council (the Data Controller) controls the System and the images recorded by it. The Council is responsible for how the System is used and for notifying the Information Commissioner about the System and its purposes. This is a legal requirement of the Data Protection Act 1998.
- 1.6 The Parish Council's Data Protection Officer is the Parish Clerk.
- 1.7 Ownership of the recorded material and copyright in the recorded material will remain with the Parish Council.

2. Key objectives of the CCTV System

- i) To prevent or reduce incidents of property crime and offences against the person.
- ii) To protect Lydiard Millicent Parish Council property and assets.
- iii) To support the Police in a bid to deter and detect crime.
- iv) To assist the Police in identifying and providing evidence in the prosecution of offenders.

The System will not be used for the covert recording of images.

3. Management of the System

- 3.1 Overall management of the system will be the responsibility of the Parish Clerk on behalf of the Parish Council.
- 3.2 Day to day operational control of the system including technical management and training will be the responsibility of Network Connections UK Ltd t/a RedHand
- 3.3 Routine daily operating checks will be carried out by Network Connections UK Ltd t/a RedHand.
- 3.4 Liaison with the Police should take place through the Parish Clerk or nominated representative.
- 3.5 This Code of Practice and Policy will be adhered to by Parish Council Staff and Members.
- 3.6 The Parish Clerk will advise Members and the public as to this Policy and Code of Practice and the performance of the facility together with any recommendations as to changes that should be made, as necessary.

4. Accountability

- 4.1 Copies of this Policy and Code of Practice shall be available for inspection at the Parish Council Office, based at the Jubilee Club House, and made available on the Parish Council website.

5. Privacy and Data Protection

- 5.1 Legitimate public concerns exist over the use of CCTV – this is mainly over matters pertaining to the processing of information (data) and what happens to the material that is obtained.
- 5.2 All personal data obtained by the CCTV shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the CCTV. In processing personal data, there will be total respect for everyone's right to his or her private and family life. The storage and security of the data shall be strictly in accordance with the Data Protection Act 1998 and additional locally agreed procedures.
- 5.3 All data will be processed in accordance with the 7 principles of the General Data Protection Regulation (GDPR) adopted as part of the Data Protection Act in 2018.

6. Viewing of the Recorded/Live Images

- 6.1 Monitors displaying images of areas under surveillance will be located so that only authorised personnel have access.
- 6.2 Access to the recorded images will be restricted to those authorised. The Parish Clerk will decide whether to allow requests for access by third parties in accordance with the Parish Council's disclosure policy.
- 6.3 The viewing of recorded images must take place in a secure area to which the general public will have no access. Unauthorised persons will not have access to that area whilst viewing is taking place.
- 6.4 Removal of the medium on which the images are recorded e.g. USB for viewing purposes must be documented as follows.
- Name(s) of Police Officer(s) viewing the images
 - The purpose of the viewing
 - Date and time of viewing
 - Action taken (if any)
- 6.5 Police requests to view images and information relating to the viewing and copying of images at the request of the Police must be recorded on an appropriate form. The following information must be recorded on the log:
- The reason for the viewing
 - The date and time of removal.
 - The name of the person removing the images.
 - The name(s) of the person(s) viewing the images. If this includes third parties, this should include the organisation of the third party, e.g. Wiltshire Police.
 - The outcome, if any, of the viewing
 - The date and time the images were returned to the System or secure place, if they have been retained for evidential purposes.

7. Siting of Camera and Signage

- 7.1 The CCTV System will be sited in such a way that it only monitors those areas intended to be covered by the equipment. (Only in areas where the Parish Council, the Police or other appropriate agencies have a public duty – e.g. Jubilee Club House, Car Park, the Recreation Field, and vulnerable areas).

7.2 Signs will be placed so that the public are aware that they are entering a zone that is covered by surveillance equipment. The signs should be clearly visible and legible to members of the public.

7.3 The signs must contain the following information.

- The identity of the organisation responsible for the scheme.
- The purpose of the scheme.
- Details of whom to contact regarding the scheme.

8. Access Requests

8.1 Under the Data Protection Act, individuals whose images are recorded have a legal right to view the images of themselves and to be provided with a copy of the images if requested.

They do not have the right of instant access. Access to images must be granted within 40 calendar days of receiving a request.

8.2 The Parish Clerk is the Officer responsible for dealing with requests under the Data Protection Act from members of the public requesting to view images of themselves.

8.3 A fee of £20 will be charged to cover administration and material costs for subject access requests.

8.4 A request to view recorded images may also be made under the Freedom of Information Act 2000 (FOI). The Parish Council must respond within 20 working days from receipt of a written request for information under the Act. However, if the images are those of the person requesting the information then that information is exempt from the FOI and should be treated as a data protection subject to access request as referred to in 8.1 above. If the requested images are of other people who are individually identifiable, these images would not normally be released. This is because the person requesting the information could potentially use the images for any purpose. This could constitute unfair processing in contravention of the Data Protection Act.

8.5 An applicant requesting information must provide sufficient information for the requested images to be identified, i.e. the location, date and approximate time the images are believed to have been recorded.

9. Retention of Images

9.1 Recorded images will be kept for a period of 30 days, after which the recording will be destroyed, unless a longer period is authorised by the Parish Clerk. In some circumstances it may be necessary to retain images for longer e.g. at the request of the Police for investigation purposes or to comply with a data subject access request under the Data Protection Act. These images will be destroyed when they are no longer required.

9.2 If images are retained for evidential purposes, they must be stored in a secure place to which there is controlled access i.e. the Parish Council safe.

9.3 If the retained images are released for use in legal proceedings, the following information must be recorded:

- The date on which the images were removed from the System for use in legal proceedings.
- The reason they were removed from the System
- To whom the images were released e.g. if the images were handed to a Police Officer, the name and station of that Police Officer must be recorded and the images signed for by the Police Officer
- Any crime incident number to which the images may be relevant
- The location of the images.

10. Complaints

10.1 Complaints relating to the use of the CCTV system will be dealt with under Lydiard Millicent Parish Council's existing complaints procedure.

Background papers: Data Protection Act 1998, Freedom of Information Act 2000.

Reference documents: CCTV Code of Practice, revised Edition 2013, (a publication of the Information Commissioner's Office).

11. Code of Practice

The following principles are to be adopted together with this policy:

- Use of a surveillance camera system (SCS) must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a SCS must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a SCS as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all SCS activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a SCS is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a SCS, and such images and information should be deleted once their purposes have been discharged.
- 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.
- SCS 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.
- SCS images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice.
- When the use of SCS 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.
- Any information used to support a SCS which compares against a reference database for matching purposes should be accurate and kept up to date.