



LONDON COLNEY PARISH COUNCIL

CCTV CODE OF PRACTICE 2018

Contents

1. INTRODUCTION AND OBJECTIVES	3
1.2 Statement in Respect of Human Rights Act 1998	3
1.3 Objectives of the System	3
1.4 System Review	3
2. STATEMENT OF PURPOSE AND PRINCIPLE	4
2.1 Purpose	4
2.2 General Principles of Operation	4
2.3 Copyright	4
2.4 Monitoring and Recording Facilities	4
2.5 Processing and Handling of Recorded Material	4
2.6 Changes of this Code of Practice	4
3. PRIVACY AND DATA PROTECTION	4
3.1 Data Protection Legalisation	4
3.2 Request for Information – Subject Access Request	5
4. ACCOUNTABILITY AND PUBLIC INFORMATION	5
5. ASSESSMENT OF THE SYSTEM	5
6. MANAGEMENT OF RECORDED MATERIAL	5
6.1 Guiding Principles	5
6.2 National Standard for Release of Data to a Third Party	6
6.3 Footage and Recorded Material – Retention	6
6.4 Register and Release of Recorded Material	6
6.5 Prints of Recorded Material	6
Appendix 1 - National Standard for the release of Data to Third Parties	7
1. Primary Request to View Data	7
2. Secondary Request to View Data	8
3. Individual Subject Access under Data Protection Legislation	9
4. Process of Disclosure	9
5. Media Disclosure	10
6. Principles	10
Appendix 2 - Subject Access Request Form	11
Document Revision History	14

1. INTRODUCTION AND OBJECTIVES

- 1.1 This code of practice has been written in accordance with the Information Commissioner's CCTV Code of Practice and the National Surveillance Commissioner's CCTV Code of Practice.

This Code of Practice applies to all CCTV cameras operated and managed by London Colney Parish Council at the Caledon Community Centre and Napsbury Sports Pavilion.

The system owner and Data Controller is London Colney Parish Council. They are responsible for the ownership of the system with overall responsibility for ensuring this Code of Practice is adhered to and the system is properly maintained. The Parish Clerk is the Data Processor, responsible for the day to day management of the system including data processing and management of the code of practice.

1.2 Statement in Respect of Human Rights Act 1998

The system owners have considered the obligations imposed by the above legislation and consider that the use of cameras in the locations mentioned above is necessary proportionate and a suitable tool to help prevent and detect crime and disorder.

The system will be operated with respect to all individuals, without any discrimination on the grounds of gender, race, colour, language, religion, political opinion, national or social origin or sexual orientation.

1.3 Objectives of the System

The primary objective of the CCTV system is to protect Parish Council owned property and increase the safety of the users of our facilities. To object this, the system will be used and data processed for the following purposes only:

- To prevent and detect crime, providing evidential material for criminal proceedings.
- To deter and detect incidents of anti-social behaviour, providing evidential material for criminal proceedings.
- To assist with other civil proceedings such as insurance claims.

The need to assist with personal safety will override any other requirements.

1.4 System Review

The system will be reviewed annually to ensure it remains necessary, proportionate and effective.

2. STATEMENT OF PURPOSE AND PRINCIPLE

2.1 Purpose

The purpose of this document is to state how the Owners and System Manager intend to use the system to meet the objectives and principles outlined in Section 1.

2.2 General Principles of Operation

The system will be operated in accordance with this Code of Practice and the Data Protection Act 1998 at all times. The system will be operated in due deference to the general right to respect for an individual and regard for their private and family life.

The public interest in the operation of this system will be safeguarded by ensuring the security and integrity of operational procedures.

2.3 Copyright

Copyright and ownership of all material recorded on the system, will remain with the Data Controller.

2.4 Monitoring and Recording Facilities

The images from the cameras located at the Caledon Community are stored on a PC located in the Parish Council offices.

The images from the cameras located at the Napsbury Sports Pavilion are stored securely within the sports pavilion on a hard drive which can only be accessed by the Data Processor.

2.5 Processing and Handling of Recorded Material

No record material, whether digital, analogue, hard copy or otherwise will be released by the Data Processor unless it is in accordance with this Code of Practice.

2.6 Changes of this Code of Practice

All changes to this Code will be agreed by the Owners of the system.

3. PRIVACY AND DATA PROTECTION

3.1 Data Protection Legalisation

The operator of the system has been notified to the Office of the Information Commissioners in accordance with the current Data Protection Legalisation. Data will be processed in accordance with the Data Protection Act 1998, summarised as:

- All personal data will be processed fairly and lawfully.
- Personal data will be obtained only for the purposes specified.
- Personal data held will be accurate, relevant and not excessive in relation to the purpose for which the data is processed.

- Steps will be taken to ensure personal data is up to date.
- Personal data will be held for no longer than is necessary.
- An individual will be allowed to access their data in accordance with the relevant legalisation.
- Procedures will be implemented to prevent unauthorised access to, alteration, disclosure or loss of, or destruction of information
- Information shall not be transferred outside of the European Economic area unless the rights of individuals are protected

3.2 Request for Information – Subject Access Request

Any request from an individual for disclosure of personal data which they believe is recorded by virtue of the system will be directed in the first instance to the Data Processor and should be treated as a Subject Access Request.

Any person making such a request should use the form included as Appendix 2 including the fee of £10 and must be able to provide sufficient information to prove their identity and enable the data to be located.

If the relevant footage shows third parties and the provision of such could involve an unfair intrusion into their privacy of the third party, the footage will not be disclosed unless all third parties have provided written agreement of the relevant footage can be obscured.

In accordance with Section 29 of the Data Protection Act 1998, personal data processed for the prevention of crime and/or the apprehension or prosecution of offenders is exempt from the subject access provisions, to the extent to which the application of the provisions to the data would be likely to prejudice these matters.

A request from an individual for footage for themselves is exempt from the provisions of the Freedom of Information Act. Instead this request should be treated as a data protection subject access request as explained above.

4. ACCOUNTABILITY AND PUBLIC INFORMATION

This Code will be made available on the Council's website and upon request to the Data Processor.

5. ASSESSMENT OF THE SYSTEM

The operation of the system will be audited on an annual basis to check for compliance with this Code of Practice and to ensure the system meets the objectives specified in section 1.

6. MANAGEMENT OF RECORDED MATERIAL

6.1 Guiding Principles

For the purposes of this Code, 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of this system; this specifically includes images recorded digitally or on other media including still prints.

Every recording made by the use of the system has the potential for containing material that may need to be admitted in evidence at some point during the period of its retention.

Members of the public must have total confidence that information recorded will be treated with due respect for private and family life. It is therefore imperative that all recorded is treated strictly in accordance with this Code of Practice until the final destruction of the material.

Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice only.

Recorded material will not be copied, sold or otherwise released or used for commercial purposes or otherwise made available for any use incompatible with this Code of Practice.

6.2 National Standard for Release of Data to a Third Party

Requests from the Police for footage for the prevention and/or detection of crime and disorder will be submitted to the Data Processor.

In complying with the National Standard it is anticipated, as far as is reasonably practicable, to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in the Code.
- Access to recorded material will only take place in accordance with the National Standard and this Code.

Subject to compliance with this Code, the Police and other agencies with a Statutory Authority to investigate and/or prosecute offences, may release details of recorded information to the media only in an effort to identify offenders or potential witnesses. In all cases this will need the permission of the Data Controller.

6.3 Footage and Recorded Material – Retention

Images are recorded by cameras are retained on the system for 28 days. After this time, the footage is erased.

When footage is released as recorded material a master copy is made and retained securely. This is retained for 7 years after which it is securely destroyed.

6.4 Register and Release of Recorded Material

Every item of recorded material that is produced is managed using specific software which provides a clear audit trail.

6.5 Prints of Recorded Material

Prints will be treated in the same manner as other recorded material and in accordance with this Code of Practice and the National Standard.

Appendix 1 - National Standard for the release of Data to Third Parties

All requests for the release of data shall be processed in accordance with this standard and the Code of Practice. All Police requests for footage needed for the prevention and/or detection of crime and disorder shall be dealt with by the Data Processor. Data to day responsibility for the operation of the CCTV system lies with the Data Processor.

1. Primary Request to View Data

- a) Primary requests to view data generated by a CCTV system are likely to be made by third parties for any one or more of the following purposes:
 - i. Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Crime Procedures and Investigations Act 1996, etc).
 - ii. Providing evidence in civil proceedings or tribunals
 - iii. The prevention of crime
 - iv. The investigation and detection of crime (may include identification of offenders).
 - v. The identification of witnesses
- b) Third parties, which are requested to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
 - i. Police (see note 1)
 - ii. Statutory (enforcing) authorities with powers to prosecute (e.g. Custom & Excise, Trading Standards etc).
 - iii. Solicitors (see note 2)
 - iv. Plaintiffs in civil proceedings (see note 3)
 - v. Accused persons or defendants in criminal proceedings (see note 3)
 - vi. Other agencies, according to purpose and legal status (see note 4)
- c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:
 - i. Not unduly obstruct a third party investigation to verify the existence of relevant data.
 - ii. Ensure the retention of data which may be relevant to the request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.
- d) In circumstances outlined in note (3) below, (requests by plaintiffs, accused persons or defendants), the Data Controller or nominated representative shall:
 - i. Be satisfied that there is no connection with any existing data held by the Police in connection with the same investigation.
 - ii. Treat all such enquiries with strict confidentiality.

Notes

- (1) The release of data to the Police is not to be restricted to the civil Police but could include (for example), British Transport Police, British Military Police, Ministry of Defence Police etc. Special arrangements may be put in place in response to local requirements.
- (2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases, a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such

release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred.

In all circumstance, data will only be released for lawful and proper purposes.

- (3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legalisation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.
- (4) The data controller shall decide which (if any) 'other agencies' might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.
- (5) The Data Controller can refused an individual request to view if sufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest half hour).

2. Secondary Request to View Data

- a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the Data Processor shall ensure that:
 - i. The request does not contravene and that compliance with the request would not breach current legislation (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Just and Public Order Act 1994 etc.)
 - ii. Any legislative requirements have been complied with (e.g. the requirements of the Data Protection Act 1998).
 - iii. Due regard has been taken of any known case law (current or past) which may be relevant
 - iv. The request would pass a disclosure of 'public interest' (see note 1).
- b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before releasing the material:
 - i. In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV Code of Practice.
- c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale or for entertainment purposes.

Note

- (1) 'Disclosure in the public interest' could include the disclosure of personal data that:
 - i. Provides specific information which would be of value or interest to the public well being.
 - ii. Identifies a public health or safety issue.
 - iii. Leads to the prevention of crime.
 - iv. The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request (see 3 above)

3. Individual Subject Access under Data Protection Legislation

- a) Under the terms of the Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
 - i. The request is made in writing
 - ii. A specified fee is paid for each search
 - iii. The Data Controller is provided with sufficient information to suffice him/herself as to the identity of the person making the request
 - iv. The person making the request provides sufficient and accurate information about the time, date and place to enable the Data Controller to locate the information which that person seeks (it is recognised that a person making a request may not know the precise time. Under these circumstances, it is suggested that within one hour of accuracy would be a reasonable requirement).
 - v. The person making the request is only shown information relevant to that particular search and which contains personal data of him/herself only, unless all other individuals who may be identified from the same information have consented to the disclosure.
- b) In the event of the Data Controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied (all other personal data which may facilitate the identification of any other person should be concealed or erased).
- c) The Data Controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however, every effort should be made to comply with subject access procedures and each request should be treated on its own merits.
- d) In addition to the principles within the Data Protection legislation, the Data Controller should be satisfied that the data is:
 - i. Not currently and as far as can be reasonably ascertained, not likely to become part of a 'live' criminal investigation.
 - ii. Not currently or as far as can be reasonably ascertained, not likely to become relevant to civil proceedings.
 - iii. Not the subject of a complaint or dispute which has not been actioned
 - iv. The original data and that an audit trail has been maintained
 - v. Not removed or copied without proper authority
 - vi. For individual disclosure only (i.e. to be disclosed to a named subject)

4. Process of Disclosure

- a) Verify the accuracy of the request
- b) Replay the data to the requestee only (or a responsible person acting on their behalf).
- c) Only data relating to the request will be shown.
- d) It must not be possible to identify any other individual from the information being shown
- e) If a copy of the material is requested and there is no one site means of editing out other personal data, then the material should be sent to an editing house for processing prior to being sent to the requestee.

Note: The Information Commissioner's Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.

5. Media Disclosure

- a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted.
 - i. The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits for its use.
 - ii. The release form shall state that the receiver must process data in a manner prescribed by the data controller e.g. specific identifies/data that must not be revealed.
 - iii. It shall require that proof of any editing must be passed back to the Data Controller either for approval or final consent, prior to its intended use by the media (protecting the position of the Data Controller who would be responsible for any infringement of Data Protection legislation and the System Code of Practice).
 - iv. The release form shall be considered a contract and signed by both parties (see note 1)

Note: In the well case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck (QBD, November 1997), the judge concluded that by releasing the video footage the Council had not acted lawfully. A verbal reassurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid future accidental broadcasts. Attention is drawn in this respect, detailed in her Code of Practice summarised above.

6. Principles

In adopting a national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

- a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the system.
- b) Access to recorded material shall only take place in accordance with this standard and Code of Practice.
- c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix 2 - Subject Access Request Form

London Colney CCTV System

Data Protection Act 1998

How to apply for Access to Information Held on the CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV system. These notes are only a guide. The law is set out in the Data Protection Act 1998. Further information is obtainable from the Information Commissioners Office www.ico.org.uk

Your Rights

Subject to certain exemptions, you have the right to be told whether any personal data is held about you. You also have the right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise.

The Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to other individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless:

- The other individual has consented to the disclosure of the information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s).

The Council's Rights

The Council may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV system are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques to be made payable to 'London Colney Parish Council' or BACS payment to:

Account name: London Colney Parish Council
Sort Code: 08-92-99
Account Number: 65180305
Reference: CCTV – *Your name*

The application form

When you have completed and checked this form, take or send it together with the required TWO identification documents, photography and fee to:

The Parish Clerk, London Colney Parish Council, Caledon Community Centre, Caledon Road, London Colney AL2 1PU

LONDON COLNEY PARISH COUNCIL

CCTV SURVEILLANCE SYSTEM

DATA PROTECTION ACT 1998

Section 1 – About Yourself	
The information requested below is to help the Council a) Satisfy itself as to your identify and b) find any data held about you. Please use BLOCK capitals	
Title (Mr/Mrs/Miss/Dr etc	
Surname/Family Name	
First Name	
Maiden name/former names	
Sex (Male or Female)	
Height	
Date of Birth	
Place of Birth (Town & County)	
Your current home address	
	Post Code:
Telephone Number	

If you have lived at this address for less than 10 years, please give your previous addresses for the period

Previous Address(es)	
Date of Occupancy (From/To)	
Previous Address(es)	
Date of Occupancy (From/To)	

Section 2 – Proof of Identity	
<p>To help establish your identify your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address For example, a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address. Also a recent, full face photograph of yourself Failure to provide this proof of identify may delay your application</p>	

Section 3 – Supply of Information	
You have a right, subject to certain to exceptions, to receive a copy of information in a permanent form. Please tick the box that applies.	
Do you wish to:	
a) View the information and receive a permanent copy	
b) Only view the information	

Section 4 – To help us find the information	
<p>If the information you have requested relates to a specific offence or incident, please complete this section. Please complete a separate box in respect of each different categories/incidents/involvement. Continue on a separate sheet in the same way if necessary. If the information you require relates to a vehicle, property or other type of information, please complete the relevant section overleaf.</p>	
Were you (tick box below)	
Victim of an offence	
A witness to an offence or incident	
Other – please explain	
Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident	

Section 4 – Declaration	
Declaration to be signed by the applicant	
The information that I have supplied in this application is correct and I am the person to whom it relates.	
Signed by	
Date	

Document Revision History

Date	Version No	Revision
9 March 2018	1	Adopted by Council