

COLWICH PARISH COUNCIL



PD016 CCTV POLICY

©This document is the property of Colwich Parish Council
Parish Centre, St. Mary's Road, Little Haywood, Staffordshire, ST18 0TX
Telephone: 01889-882665.
It must not be copied, or the contents otherwise used, without the consent of the owner.

CCTV POLICY

CCTV Policy – PD016

Revision history

This document was originally written by:

Name	Position	Date
Michael Lennon	Clerk	April 2018

This document version was reviewed by:

Policy Committee	October 2023
------------------	--------------

This document version was approved by:

Full Council	December 2023
Chairman of Council	Wendy Plant

Document Review Schedule:

Next Mandatory Review by:	December 2024
---------------------------	---------------

Revision History

Version	Issue Date	Document ID	Reason for Change	Section(s) Changed
1	09/2018	PD016	Initial issue	None
2	12/2018	PD016-02	New Chairman	None
3	12/2019	PD016-03	Chairman and new sections	Sections 5-10 added
4	10/2021	PD016-04	Annual review New Chairman	None
5	10/2022	PD016-05	Annual review	None
6	12/2023	PD016-06	Annual review	3.1, 4 & 11

CCTV POLICY

CONTENTS

1	Policy	4
2	Surveillance Commissioner's Code of Practice	4
3	Statement of Purpose	5
4	Roles and Responsibilities	5
5	Procedure for Release of Evidence	6
6	Primary Request to View Data	6
7	Secondary Request to View Data	7
8	Individual Subject Access under Data Protection Legislation	7
9	Process of Disclosure	8
10	Media Disclosure	9
11	Concerns	9

CCTV POLICY

1 POLICY

- 1.1 This policy is to control the management, operation, use and confidentiality of the CCTV system owned and run by Colwich Parish Council at the Jubilee Playing Field, Little Haywood.
- 1.2 This policy has been prepared taking into account current Data Protection advice from the Information Commissioner's Office and to reflect the emerging General Data Protection Regulations specifically:
- The Human Rights Act 1998 article 8
 - The Data Protection Act 1998.
 - The Regulation of Investigatory Powers Act 2000.
 - The protection of Freedoms Act 2012
 - Information commissioners CCTV Code of Practice
 - Surveillance Commissioners, Surveillance Camera Code of Practice

2 SURVEILLANCE COMMISSIONER'S CODE OF PRACTICE

- 2.1 The Parish Council will ensure that the operation of its CCTV system is in line with the 12 principles in the Surveillance Commissioner's Code of Practice:
- 2.1.1 Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- 2.1.2 The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- 2.1.3 There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- 2.1.4 There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- 2.1.5 Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- 2.1.6 No more images and information should be stored than that which is strictly required of the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- 2.1.7 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 as 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.
- 2.1.8 Surveillance camera system 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.

CCTV POLICY

- 2.1.9** Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- 2.1.10** There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- 2.1.11** When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should 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.
- 2.1.12** Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

3 STATEMENT OF PURPOSE

- 3.1** Colwich Parish Council has installed a CCTV system at the Jubilee Playing Field to provide a safe and secure environment for the benefit of residents, staff and other visitors to the Jubilee Playing Field.
- 3.2** The CCTV system will not be used to invade the privacy of any individual, except when carried out in accordance with the law.
- 3.3** Retrieved images may be viewed by Councillors and shared with those parties listed in 6.2 to protect the integrity of the site from fly-tipping, vandalism and other anti-social behaviour.
- 3.4** Downloaded images will **NOT** be shared with members of the public. Data including images, date and time will only be downloaded if an incident is suspected.
- 3.5** The retention of data will be in line with the General Data Protection Regulations. Retained data will be kept until there is a resolution of the incident.

4 ROLES AND RESPONSIBILITIES

- 4.1** Overall responsibility for the system will rest with the Council managed through the Clerk.
- 4.2** Annual audit of retrieved data will be conducted by the Data Protection Officer (DPO) and the findings reported to the Annual Meeting.
- 4.3** The DPO will ensure that the Council sets standards and procedures to manage the CCTV system and that the system complies with legal obligations including individuals' rights of access.
- 4.4** Day to day operational management will be through the Lengthsmen who will receive appropriate training in the operation of the system. The Lengthsmen will download data via a password-protected link to the CCTV system.

CCTV POLICY

4.5 The Clerk will retain retrieved images on a password-protected computer.

4.6 Only the Clerk may share images with relevant partner authorities.

5 PROCEDURE FOR RELEASE OF EVIDENCE

5.1 All requests for the release of data shall be channelled through the Clerk or their nominated representative.

6 PRIMARY REQUEST TO VIEW DATA

6.1 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:

6.1.1 Providing evidence in criminal proceedings

6.1.2 Providing evidence in civil proceedings or tribunals

6.1.3 The prevention of crime

6.1.4 The investigation and detection of crime (may include identification of offenders)

6.1.5 Identification of witnesses

6.2 Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

6.2.1 Police

6.2.2 Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc)

6.2.3 Solicitors

6.2.4 Claimants in civil proceedings

6.2.5 Accused persons or defendants in criminal proceedings

6.2.6 Other agencies, (as agreed by the Clerk and notified to the Information Commissioner) according to purpose and legal status

6.3 Upon receipt from a third party of a bona fide request for the release of data, the Clerk shall:

6.3.1 Not unduly obstruct a third party investigation to verify the existence of relevant data.

6.3.2 Ensure the retention of data which may be relevant to a 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.

6.4 Where requests fall outside the terms of disclosure and Subject Access legislation, the Clerk, or nominated representative, shall:

6.4.1 Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.

6.4.2 Treat all such enquiries with strict confidentiality.

7 SECONDARY REQUEST TO VIEW DATA

CCTV POLICY

- 7.1** 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.
- 7.2** Before complying with a secondary request, the Clerk shall ensure that:
- 7.2.1** The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc);
 - 7.2.2** Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);
 - 7.2.3** Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck); and
 - 7.2.4** The request would pass a test of 'disclosure in the public interest'.
- 7.3** 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 surrendering the material:
- 7.3.1** 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 System Code of Practice.
 - 7.3.2** If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.
- 7.4** 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 of material for training or entertainment purposes.

8 INDIVIDUAL SUBJECT ACCESS UNDER DATA PROTECTION LEGISLATION

- 8.1** Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
- 8.1.1** The request is made in writing;
 - 8.1.2** An appropriate fee is paid for each individual search;
 - 8.1.3** The Clerk is supplied with sufficient information to satisfy their self as to the identity of the person making the request;
 - 8.1.4** The person making the request provides sufficient and accurate information about the time, date and place to enable the Clerk to locate the information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);
 - 8.1.5** The person making the request is only shown information relevant to that particular search and which contains personal data of their self only, unless all other individuals who may be identified from the same information have consented to the disclosure.

CCTV POLICY

- 8.2** In the event of the Clerk 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). Under these circumstances an additional fee may be payable.
- 8.3** The Clerk 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 merit.
- 8.4** In addition to the principles contained within the Data Protection legislation, the Clerk should be satisfied that the data is:
- 8.4.1** Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
 - 8.4.2** Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
 - 8.4.3** Not the subject of a complaint or dispute which has not been actioned;
 - 8.4.4** The original data and that the audit trail has been maintained;
 - 8.4.5** Not removed or copied without proper authority;
 - 8.4.6** For individual disclosure only (i.e. to be disclosed to a named subject).

9 PROCESS OF DISCLOSURE

- 9.1** Verify the accuracy of the request.
- 9.2** Replay the data to the requestee only, (or responsible person acting on behalf of the person making the request).
- 9.3** The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request shall be shown.
- 9.4** It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
- 9.5** If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

10 MEDIA DISCLOSURE

- 10.1** In the event of a request from the media for access to data, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released and is agreed upon by the Council, the following procedures shall be adopted:
- 10.1.1** 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 on its use, and indemnifies the Council against any breaches of the legislation.

CCTV POLICY

- 10.1.2 The release form shall state that the receiver must process the data in a manner prescribed by the Clerk, e.g. specific identities/data that must not be revealed.
- 10.1.3 The release form shall require that proof of any editing must be passed back to the Clerk, either for approval or final consent, prior to its intended use by the media (protecting the position of the Clerk who would be responsible for any infringement of Data Protection legislation).
- 10.1.4 The release form shall be considered a contract and signed by both parties.

11 CONCERNS

- 11.1 Any requests for information, concerns or complaints regarding the operation of the CCTV system at the Jubilee Playing Field should be made in writing and addressed to:

Revd Mr Michael Lennon FSLCC
Parish Clerk
Colwich Parish Council
St Marys Road
Little Haywood
ST18 0TX

Clerk@colwichparishcouncil.gov.uk

Who will ask the DPO to investigate the matter on behalf of, and report direct to, the Parish Council.

SIGNED	
COUNCILLOR WENDY PLANT PARISH COUNCIL CHAIRMAN	