



CCTV MANAGEMENT POLICY

As re-adopted at a meeting of Stondon Council on 27th May 2026

DOCUMENT CONTROL

Organisation	Stondon Parish Council
Title	Closed Circuit Television (“CCTV”) Management Policy
Version	2.0
Creator	Sian van der Merwe – Clerk
Adopted	April 2025
Last review Date	April 2025
Owner	Clerk
Next Review date	May 2028

Note – Review date is indicative and will depend on changes in Legislation or best practice

DOCUMENT AMENDMENT HISTORY

Revision No.	Originator of change	Date of change	Change Description
V1.1	Clerk	Apr 2025	New policy
V2.0	Clerk	27/05/2026	Change to Clerk details, amendment to policy in line with need for additional system managers.

Contents

INTRODUCTION	4
LEGISLATIVE REQUIREMENTS.....	5
ROLES AND RESPONSIBILITIES.....	6
ACCOUNTABILITY.....	7
POLICY COMPLIANCE WITH SURVEILLANCE CAMERA CODE OF PRACTICE 2013	7
APPENDIX A: STONDON PARISH COUNCIL: CCTV SYSTEM ANNUAL REVIEW	10
APPENDIX B: SUBJECT ACCESS REQUEST FORM	11
APPENDIX D: CCTV DATA LOG	14

INTRODUCTION

The purpose of this policy is to provide **Stondon Parish Council** (the “Council”) with guidance in order to comply with relevant legislation relating to the use of Closed Circuit Television (“CCTV”) in the Community.

It will enshrine within the Council’s practices the surveillance camera code of practice and data protection code of practice for surveillance cameras and personal information to ensure the Council meets its statutory obligations, and to ensure that individuals and the wider community have confidence that surveillance cameras are deployed to protect and support them rather than spy on them.

This Policy is designed to control the management, operation, use and confidentiality of the CCTV systems at the Community Centre. A list of camera locations is held by the Council Clerk.

The definition of CCTV in this policy is “equipment used to capture and store images, potentially including those of persons”.

The purpose of the CCTV installed by the Council is to provide a safe and secure environment for the benefit of those who might visit, work or live in the area. The system will not be used to invade the privacy of any individual, except when carried out in accordance with the law. The scheme will be used for the following purposes:

- to monitor the security of premises or equipment;
- to ensure public safety;
- to reduce the vandalism of property and to prevent, deter and detect crime and disorder;
- to assist the Police and other local enforcement bodies in the identification, detection, apprehension and prosecution of offenders by examining and using retrievable evidence relating to crime or public order;
- to deter potential offenders by publicly displaying the existence of CCTV, having cameras clearly sited that are not hidden and prominent signs on display; and
- to assist all emergency services to carry out their duties.

CCTV will only be installed at publicly accessible premises owned or administered by the Council in the first instance.

The Council shall comply fully with the requirements of relevant legislation and guidance in the consideration and possible use of CCTV.

<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>
<https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

The Council accepts the principles of that data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with these purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in accordance with individuals’ rights; and
- held securely;

Responsibility for the overall management of the CCTV will lie with the Council. The following people and organisations are covered by this policy:

- (a) Data controller and data owner – meaning the Council

- (b) System manager – meaning an Officer or Councillor or appointed representative of Council.
- (c) System user – meaning such councillors, officers, or other individuals from designated bodies authorised to use the surveillance equipment
- (d) Data subject – meaning any such individual whose personal information is captured by the surveillance equipment

LEGISLATIVE REQUIREMENTS

Local Government and Rating Act 1997 s.31: The power for the Council to install CCTV and other surveillance equipment: :

- (1) A parish council or community council may, for the detection or prevention of crime in their area –
 - (a) install and maintain any equipment,
 - (b) establish and maintain any scheme, or
 - (c) assist others to install and maintain any equipment or to establish and maintain any scheme.

Crime and Disorder Act 1998 s.17: The Council also has a duty to consider crime and disorder implications of their functions:

- (1) ...It shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonable can to prevent:
 - (a) crime and disorder in its area (including anti-social and other behaviour adversely affecting the local environment); and
 - (b) the misuse of drugs, alcohol and other substances in its area; and
 - (c) re-offending in its area

The Council shall comply with all legislation and resultant codes, apply to the gathering and use of data.

The Parish Council recognises that images captured by CCTV may have to be released following a request made under the **Freedom of Information Act 2000** ("FOIA") and receipt of a completed subject access request form.

Data Protection Act 2018 (DPA 2018) & UK General Data Protection Regulation (UK GDPR): The Council is committed to processing personal data captured by CCTV in a lawful, fair, and transparent manner. CCTV footage will only be used for specific purposes, including the prevention of crime, public safety, and supporting law enforcement.

Surveillance Camera Code of Practice: Issued under the **Protection of Freedoms Act 2012**, the Council adheres to this Code to ensure that the use of CCTV is proportionate, necessary, and transparent. The Council follows the 12 guiding principles set forth in the Code.

Human Rights Act 1998: The Council ensures that the use of CCTV respects the rights to privacy under Article 8 of the European Convention on Human Rights. CCTV monitoring is carried out in a way that minimally interferes with individuals' privacy.

ROLES AND RESPONSIBILITIES

Day-to-day maintenance and operational responsibility rests with the Council via the Clerk and a nominated Councillor.

A CCTV installation and service maintenance company is appointed to carry out regular checks of the CCTV equipment and will be able to access the system to carry out essential maintenance repairs when requested by the Clerk and/or the Police.

The CCTV system is securely located at the Community Centre, and this is to prevent unauthorised persons from having access to view any recordings.

Any breach of this policy shall be investigated by the Clerk to the Council and reported to the Council.

A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender. Any relevant digital evidence must be in an acceptable format for use at Court hearings. This policy must be read and understood by all persons involved in this scheme, and individual copies of this policy will, therefore, be issued for retention. A copy will also be available for reference with the recording equipment.

Only those appointed by the Council may access the cameras, monitors and associated systems. The following points must be understood and strictly observed by those persons:

- they must act with due probity and not abuse the equipment or change the pre-set criteria to compromise the privacy of an individual;
- the position of cameras and monitors have been agreed following consultation with the Police and other relevant bodies;
- no public access will be allowed to the monitor except with the express approval of the Clerk and with a written and justified reason;
- the Police and other enforcement bodies will be permitted access to recording media if they have reason to believe that such access is necessary to investigate, detect or prevent crime. Any visit by an enforcement body to view images or retrieve evidence will be logged;
- the accuracy of the date/time displayed will be checked on each occasion that the system is accessed.
- Digital records and images shall be securely stored to comply with data protection and should only be handled by specifically designated persons. Records and images will normally be erased after a certain period but may be retained for longer because of a known incident and required for the apprehension or prosecution of offenders;
- Digital records or images shall not be supplied to the media, except on the advice of the Police. Such a decision will be taken by the Council.
- As records may be required as evidence in a court of law, each person handling a digital record may be required to make a statement to a Police Officer and sign an exhibit label. Any extracted data that is handed to a Police Officer should be signed for by the Police Officer and information logged to identify the recording, showing the Officer's name and police station. The log should also show when such information is returned and/or the outcome of its use;
- any event that requires checking of recorded data should be clearly detailed in the log book of incidents, including crime numbers if appropriate;
- any damage to equipment or malfunction discovered should be reported immediately to the Clerk who will contact the CCTV Contractor responsible for maintenance, and the call logged showing the outcome. When a repair has been made, this should also be logged, showing the date and time of completion.

- any request by an individual member of the public for access to their own recorded image must be made on an 'Access Request Form' and is subject to a standard fee. If there is any doubt concerning the legitimacy of any request, then the Clerk will seek advice from the Information Commissioner's Office and/or the Surveillance Camera Commissioner.

ACCOUNTABILITY

Copies of this policy are available in accordance with the Freedom of Information Act, as will any reports that are submitted to the Council, providing that does not breach security needs. The Police and other local enforcement bodies will be provided with a copy of this policy.

Any written concerns or complaints regarding the Council's use of the system will be considered under the Council's existing complaints policy.

The CCTV system installed and used by the Council does not require it to be registered with the Information Commissioner due to its static nature. The Council is registered with the Information Commissioner as a data handler for the processing of the data collected.

One or more signs shall be displayed in the vicinity of where the CCTV is deployed. Notices shall be erected providing the following information:

- Purpose of the CCTV
- Who manages the CCTV
- Contact details for the organisation(s) responsible should anyone want to find out more about the scheme or request access to their CCTV images.
-

This policy, together with the continued need for CCTV usage, will be reviewed by the Council on a biennial basis.

POLICY COMPLIANCE WITH SURVEILLANCE CAMERA CODE OF PRACTICE 2013

In accordance with the Surveillance Camera Code of Practice 2013 the Council has adopted the following 12 principles:

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.*

The specified purpose of the CCTV system is for the prevention and detection of crime and antisocial behaviour within the Parish of Stondon and the safe management of the sites covered. The systems shall not be used for any other purpose, and there shall be a prohibition on the monitoring of the lawful movements of any individual.

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.*

There are varying and subjective expectations of privacy, and the Council shall not:

- (a) deploy surveillance camera systems in public places where there is a high expectation of privacy, including toilets and changing rooms;
- (b) use any forms of audio recording in a public place, other than for the recording of Council and committee meetings
- (c) use any form of facial recognition or other biometric characteristic recognition system

The Council shall also undertake a privacy impact assessment for any new form of surveillance it wishes to undertake, and shall regularly review such assessments alongside this policy.

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.*

The Council shall ensure that sufficient signage is in place in all areas covered by any surveillance system, and that the Council's privacy policy, CCTV and surveillance policy, complaints policy, and other relevant documents are published on its website.

4. *There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.*

The Data Controller and Data Owner shall have overall ownership of records and data for and from the surveillance systems in place, with the Clerk and nominated CCTV Councillor having responsibility for ensuring that proper governance arrangements are in place, and ensuring that such arrangements are communicated to and adhered to by any system users.

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.*

The Clerk and nominated CCTV Councillor will ensure that all system users are aware of the contents of this policy and have sufficient training to safely and securely use the equipment.

6. *No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.*

As a default, all images captured shall be deleted without review, unless the system manager is satisfied beforehand that there is a legitimate reason, under Principle 1, for it being accessed and viewed and/or a written request has been received from a designated body to preserve evidence.

CCTV images are stored on a DVR for a period of up to 30 days, following which they are automatically overwritten.

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 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.*

Access to all images by any permitted users is solely for the purposes set out in Principle 1 above. Access to stored images is restricted to the Clerk, nominated CCTV Management Councillor and the Council Chairman.

Where footage is extracted for the purposes of passing this to a third party (e.g. the Police or a school for the identification of an offender) the Council shall ensure this complies with any data protection legislation, and any stipulations in its Data Retention Statement and Privacy Policy. The Council shall also take reasonable steps to ensure the third party has in place practices and procedures to comply with data protection regulations.

Where another third party, such as a person whose property has been damaged, requests the disclosure of images, such requests will be approached with care and in accordance with the **Human Rights Act 1998**, and with a view to the guidance set out in para. 4.7.4-4.7.6 of the **Surveillance Camera Code of Practice 2013**.

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.*

The System Manager shall ensure that all CCTV follows British Standard BS7958 on the operation and management of CCTV, and that all surveillance equipment meets any such additional standards as made available by the Surveillance Camera Commissioner.

9. *Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.*

The Clerk and nominated Councillor shall follow the guidance as outlined in Data protection code of practice for surveillance cameras and personal information 2017. All CCTV DVRs and SD cards used to capture images shall be password protected and/or encrypted.

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.*

The Data Controller shall review this policy and privacy impact assessments, along with the number and positioning of all surveillance cameras, in line with the **Surveillance Camera Code of Practice 2013**.

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 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.*

The Data Controller shall ensure that the quality and positioning of any surveillance equipment is such so as to achieve the highest quality and most useful images, including the use of HD cameras and IR night vision. Where images are to be used for law enforcement and criminal proceedings, the Council will ensure that there is an audit trail of all images used, and that such images are available in a readily exportable format without the loss of forensic integrity.

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.*

The Council will not use facial and biometric recognition technology. In addition, the Council does not have, nor has no intention of using, a reference database for the purposes of matching data captured from its surveillance systems.

I have read the above policy and agree to abide by these instructions and the information contained within it. I will discuss any concerns with the Clerk and/or Chairman at any time.

Signed

Print Name

Date/...../.....

(Operators are issued with their own copy of this policy and shall sign to confirm receipt and compliance.)

APPENDIX A: STONDON PARISH COUNCIL: CCTV SYSTEM ANNUAL REVIEW

This CCTV system and the images it produces are controlled by the Council, who are responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose. The Council has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of the public and users of its facilities. It will not be used for other purposes.

The Council will conduct an annual review of the use of CCTV.

	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting specific premises or locations.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
An incident log is kept and all access to the system is reported including the date, time, reason, by whom and the outcome			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			
The Council has reviewed the use of the system, its management, policies and procedures and its overall appropriateness for continued use			

APPENDIX B: SUBJECT ACCESS REQUEST FORM
Subject Access Request Form – Stondon Parish Council CCTV

This form is intended to support individuals requesting access to images of themselves captured by CCTV cameras on the Council CCTV network. Please note: CCTV footage is only normally retained for a maximum of 28 days.

To enable us to respond to your request promptly, please ensure that you provide us with:

- The relevant date, location and approximate time
- A description of what is happening in the footage
- A detailed description of what you were wearing/carrying at the time;
- A recent full-length colour photograph of you

The completed form should be sent to the Clerk at Stondon Parish Council using the details provided at the end of the form. If you need further assistance, please e-mail clerk@stondon-pc.gov.uk You are not required to complete this form; however, it may help you set out your request.

1. Your details

Name:	
Address:	
Postcode:	
Telephone number:	
Email address:	

1. Are you the Data Subject (the individual whose personal data is being requested)?

Yes:	Please provide proof of your identity, for example a photocopy of a valid passport or photocard driving licence; We may also request proof of address, if required.. Please go straight to section 5 of this form
No:	Are you acting on behalf of the Data Subject with their explicit consent, or with the appropriate legal authority? If so, this must be evidenced in writing and enclosed with this form. You must also enclose proof of the Data Subject's identity and address as described above. Please ensure that you complete sections 3 and 4 of this form

2. Details of the Data Subject (If different to those provided in section 1)

Name:	
-------	--

Address:	
Postcode:	
Telephone number:	
Email address:	

3. **Legal status in relation to the Data Subject** (If you are not the data subject please briefly describe your relationship with them (e.g. legal adviser, spouse, parent, carer, etc) and explain why you are making this subject access request on their behalf)

--

4. **Personal information required** (Please describe as precisely as possible the nature of the images you are requesting; providing details of the exact date and location involved, together with an approximate time. Please also describe your appearance and what you were doing at the time you believe your image was captured. Please continue on a separate sheet if necessary)

--

5. **Submitting your request**

Please email your completed copy marked 'Private and Confidential' to clerk@stondon-pc.gov.uk

Or send the completed copy of this form in a securely sealed envelope marked 'Private and Confidential' to the following address:

Stondon Parish Council
Stondon Community Centre, The Pastures, Upper Stondon SG16 6QB

Remember to include:

- Proof of your identity (or, if you are not the Data Subject: proof of the Data Subject's identity and address; and any relevant documents which give you the legal authority to make this request)

- A recent full-length colour photograph of you

I understand that it may be necessary for me to provide additional information in order for Stondon Parish Council to confirm my identity (or that of the Data Subject) and/or locate relevant personal information. The statutory response period of one month specified in data protection legislation will not commence until Stondon Parish Council is satisfied in this regard and has received any additional information it has requested in order to process this request.

..... (signature) date of signature

APPENDIX D: CCTV DATA LOG

Date/Time	Location		Name/Signature of Viewer	Action Taken (Crime Ref Number)	Date/Time of Viewing	Result/Action	Reference No