



Stratfield Mortimer Parish Council

CCTV Policy

Introduction

- 1 This is the CCTV (Closed Circuit Television) Policy of Stratfield Mortimer Parish Council and adopts the definitions in the Council's Policy Guidance and Glossary.
- 2 CCTV (also referred to as a 'surveillance camera system') has been installed by the Council with the primary purpose of reducing the threat of crime generally, protecting Council premises and helping to ensure the safety of users, the general public and staff, consistent with the respect for the individual's privacy.
- 3 This Policy includes (within the Policy and/or as Appendices) processes for individuals and organisations to request or be provided with access to data, and a Data Privacy Impact Statement.

Processing of personal data

- 4 The lawful basis for processing an individual's personal data is that of a legitimate interest:
 - 4.1 processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
 - 4.2 under data protection legislation, we are permitted to use your information this way because we have a legitimate interest in securing our premises and reducing complaints against our staff;
 - 4.3 CCTV may capture more sensitive information about individuals - this processing is necessary for reasons of substantial public interest, for the prevention or detection of unlawful acts and to carry out a key function as set out in law (s.163, Criminal Justice and Public Order Act 1994).

System

- 5 The CCTV system ("the System") comprises four fully functional deployable cameras located on two poles above the tennis court westside fence at The Fairground, The Street, Mortimer, RG7 3RD. Camera images are not monitored but are recorded locally on the site where they operate, and access is only available to limited people. Images are captured 24 hours a day, seven days a week and are kept securely on encrypted cloud-based storage. If images are downloaded, they are stored on password-protected Council hardware.
- 6 Signs are prominently placed at strategic points to inform members of the public that the System is in use.

- 7 Although every effort has been made to guarantee the effectiveness of the System, it is not possible to guarantee the System will detect every incident taking place within the area of coverage.
- 8 The Council has followed the CCTV guidelines produced by the Information Commissioner's Office ("ICO").

Purposes

- 9 The System will be used for the following purposes:
 - to create a safer community;
 - to reduce the fear of crime;
 - to reduce the vandalism of property;
 - to prevent, deter and detect crime and disorder;
 - to gather evidence by a fair and accountable method;
 - to assist the council, and the police and other law enforcement agencies with the identification, detection, apprehension, and prosecution of offenders, by examining and using retrievable evidence relating to crime, public order or contravention of the law;
 - to deter potential offenders by publicly displaying the existence of CCTV: having cameras clearly sited that are not hidden and signs on display;
 - to assist the emergency services to carry out their lawful duties.

Access to images

- 10 Access to images will be restricted to those that need to have access in accordance with the purposes of the System. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the System and is limited to the following:
 - police and other law enforcement agencies where the images recorded could assist in a specific criminal enquiry and / or the prevention of terrorism and disorder;
 - prosecution and safeguarding agencies;
 - relevant legal representatives;
 - individuals whose images have been recorded and retained (unless disclosure would prejudice criminal enquiries);
 - parents/appropriate adults connected to an incident under review and involving someone aged under 18.
- 11 All requests for disclosure should be documented. If disclosure is denied, the reason should be recorded.

Retention

- 12 All footage can be exported if needed to be retained for as part of an investigation.

- 13 Otherwise, stored images on the System are retained for 30 days - this allows sufficient time and chance to come back to an event that has occurred.
- 14 CCTV footage is not backed up so, unless exported, it will be overwritten by more recent coverage.

Individuals' access rights

- 15 The Data Protection Act 2018 ("the 2018 Act") and the UK General Data Protection Regulation (UK GDPR) give individuals the right to access personal information about themselves, including CCTV images:
 - 15.1 subject to certain exemptions, individuals have a right to be told whether any personal data is held about them;
 - 15.2 they also have a 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 they agree otherwise - the Council will only give that information if it is satisfied as to the individual's identity;
 - 15.3 if the information would disclose information relating to (an)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 information; or
 - it is reasonable in all the circumstances to comply with the request without the consent of the other individual(s).
- 16 An application form for accessing personal information is at Appendix 1.

The Council's rights

- 17 The Council may deny access to information where the Act allows - the main exemptions relate to information held on the System are where the information may be held for the prevention and detection of crime or the apprehension and prosecution of offenders, and the release of the data would potentially prejudice those purposes.

Data Privacy Impact Assessment

- 18 The Council's Data Privacy Impact Assessment ("DPIA") is at Appendix 2.
- 19 The purpose of a DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It is recommended in The Surveillance Camera Code of Practice, issued by the Surveillance Camera Commissioner in June 2013 in accordance with s.30(1)(a), Protection of Freedom Act 2012, ("the Code").
- 20 The Code provides guidance, including 12 guiding principles, on the appropriate use of surveillance camera systems by local authorities and the police.
- 21 Guidance is based on the ICO's DPIA Handbook, and the four areas highlighted by the ICO as potential areas for loss of privacy in relation to personal data are:
 - the privacy of personal information;
 - the privacy of the person;
 - the privacy of personal behaviour; and

- the privacy of personal communications.
- 22 'Personal data', as defined by s1, 2018 Act, means data which relates to a living individual who can be identified from:
- 22.1 that data; or
- 22.2 that data and other information, which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

DPIA - Responsible Person contact details

- 23 The person qualified to respond to questions regarding the Council's DPIA is the Clerk to the Council, Stratfield Mortimer Parish Council, 27 Victoria Road, Mortimer, Reading, RG7 3SH (the.clerk@stratfield-mortimer.gov.uk).

Appendix 1 - Application form for accessing personal information

REQUEST FOR ACCESS TO DATA

SECTION 1 - About You

The information requested below is to help us (a) satisfy ourselves as to your identity and (b) find any data held about you.

PLEASE USE BLOCK LETTERS

Title (<i>tick as appropriate</i>)	Mr		Mrs		Miss		Ms	
Other Title (<i>Dr, Rev, etc</i>)								
Surname								
First Name(s)								
Address								
Postcode								
Tel								

SECTION 2 - Proof of Identity

Please provide (or produce to the Parish Office for inspection) two official documents (or certified copies) that, between them, clearly show (a) photo proof of your ID (eg passport or driving licence), and (b) proof of your current address (eg recent bank statement or utility bill).

SECTION 3 - Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form – do you wish to (please delete as necessary):

- View the information and receive a permanent copy [Yes] / [No]
- Only view the information [Yes] / [No]

SECTION 4 - Details

To assist us in finding the information please complete the following:

I am (please tick or complete):

A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	
Other – please explain:	

Details of the incident:

Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident:	

SECTION 5 - Declaration

The information I have supplied in this application is correct and I am the person to whom it relates.

Signed: _____ Date: _____

Warning: a person who impersonates or attempts to do so may be guilty of an offence

SECTION 6 - Submission

When you have completed, checked, signed and dated this form, please send or deliver it, together with the required identification documents/certified copies to: **Stratfield Mortimer Parish Council, 27 Victoria Road, Mortimer, RG7 3SH.**

If you have any queries regarding this form, or your application, or any complaint or enquiry about the day-to-day operation of the system please email the.clerk@stratfield-mortimer.gov.uk.

Appendix 2 – Privacy Impact Assessment

1	Why a Privacy Impact Assessment is Required	
1.1	What is the aim of the surveillance system?	Providing Stratfield Mortimer Parish Council and Thames Valley Police with evidence to take criminal and civil action in the Courts.
		Reducing the fear of crime and providing reassurance to the public.
		Aiding in the detection and prevention of crime (including countering terrorism).
		Assisting with the maintenance of public order.
		Deterring or reducing the incidence of vandalism, graffiti, and other environmental crime.
		Deterring persons from committing crimes and to enhance the opportunities for detecting those who do.
		Improving the safety and security of residents, visitors, and the business community.
		Discouraging anti-social behaviour including alcohol and drug-related elements.
1.2	Who takes legal responsibility under the Data Protection Act?	Stratfield Mortimer Parish Council is the Data Controller at the point of images being recorded. However if any images are released to any of the authorised organisations, then the legal responsibility will be transferred to that organisation in relation to the images that have been released.
1.3	What organisations will have access to CCTV images?	Stratfield Mortimer Parish Council will be the main user of the CCTV system.
		However, Thames Valley Police, other Police Forces and other agencies such as Fire and Rescue Service will be granted access to images from the system if a legitimate request is received.
1.4	What are the benefits to be gained from the system and who will benefit?	Residents, visitors, and businesses will benefit from improved public safety, and reductions in crime.
		CCTV is a proven tool in detecting crimes, and the perpetrators of it. Using CCTV can significantly

		reduce the time and cost on the Police service in investigating allegations.
		It is known that false allegations are made, and CCTV is also useful in disproving some allegations.
		CCTV captures actual events and is not influenced by interpretation, or events, as seen by people who are under the influence of alcohol or drugs.
1.5	Can CCTV realistically deliver these benefits?	Yes, and consistently so.
2	Information Flow	
2.1	How is information collected?	The system captures video pictures, which are transmitted from cameras positioned on the Fairground, Stratfield Mortimer.
		The transmissions are received via Parish Council hardware. Access is via a web link and log in/password. The cameras are equipped with pan, tilt and zoom facilities.
2.2	Where are the real-time images from the camera displayed?	Real-time images will be accessed and displayed via Parish Council hardware.
		Third parties can be granted access to the images via the web link and log in/password, but it is not envisaged that this will be used.
2.3	Who has operational access and ability to move the CCTV camera?	Stratfield Mortimer Parish Council Clerk.
		Thames Valley Police can access live video streams and use of cameras under the Regulation of Investigatory Powers Act. This is controlled by the Parish Council Clerk.
2.4	How are the images recorded?	Each camera signal will be continuously recorded by way of a Digital Video Recorder.
2.5	Where are the recorded images stored?	On hard drives in a locked cabinet.
2.6	How is information used?	Information is used to monitor public safety and prevent and detect crimes.
		Evidence is provided for investigation and enforcement.

		Individuals can request copies of CCTV data which contains their personal information.
		Disclosure of data is covered by internal processes which are fully compliant with relevant legislation and codes of practice.
2.7	How is access gained to the recorded images?	Password controls are in place on the system. Hard copy requests for images will be required.
2.8	How long are the images retained?	30 days on the system. Images from an 'incident' may be stored for longer.
2.9	How is information deleted?	The data management system will automatically delete information after 30 days
2.10	When data is downloaded, or copied for release to a third party how is information recorded?	Memory stick or secure, encrypted cloud-based exchange.
2.11	What processes are in place to ensure that data protection responsibilities are understood by persons receiving the data?	Each request for data by the public must be requested via a signed data release form.
3	Data Protection Act	
3.1	Can less privacy intrusive solutions achieve the same objectives?	CCTV is a good solution to achieve the objects set out in 1.1.
3.2	Are images of identifiable individuals required or could the scheme use other technology not capable of identifying individuals?	The system must be capable of identifying individuals, as footage from the system could be used in both criminal and civil court cases.
		If the system did not have this capability, it would not be fit for purpose.
3.3	Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?	The service will remain a 24-hour service for the foreseeable future.
3.4	What future demands may arise for wider use of images and how will you address these?	The benefits of additional cameras will be considered as and when required.

3.5	What are the views of those under surveillance?	The general feeling is that people who are not involved in crime are happy to be in an area that is monitored by CCTV cameras. There are some members of society both law abiding and those who are not, who have issues with being in areas covered by CCTV cameras. By abiding with current legislation, the aim is to show that the CCTV system is only used for crime reduction/ detection purposes and those activities that assist the public.
4	Human Rights Act	
4.1	Is the system established on a proper legal basis and operated in accordance with the law?	The system has been established on a proper and legal basis to comply with the Data Protection Act, Human Rights Act and Regulations of Investigatory Powers Act.
4.2	What could we do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?	Regular reviews of camera performance shall be undertaken to justify their need.
4.3	Is CCTV justified in the circumstances?	Yes. Violence, theft, and anti-social behaviour are key areas to address which in turn will reduce the fear of crime thereby creating a safer environment.
4.4	Is it proportionate to the problem that it is designed to deal with?	Yes. CCTV is used to detect crime and complies with the current legislation.
5	Surveillance Code of Practice	
5.1	Do you regularly review the system against its objectives?	Yes.
5.2	Is the system being used for any other purpose other than those specified?	No.
5.3	Does signage exist highlighting the use of surveillance cameras?	Signage is installed.
5.4	Does the signage highlight the point of contact?	Signage highlights the point of contact.
5.5	Are all staff aware of their responsibilities?	Yes.

5.6	Can a member of the public request footage?	<p>The procedure for a Data Subject Access requests forms part of this Policy and is set out in Appendix 1. It is also available in hard copy should it be requested.</p> <p>CCTV footage can only be supplied for 30 days from the date and time of an incident, after which time the images are automatically overwritten.</p>
6	Risks	
6.1	Is the data shared with other organisations?	Yes, for investigation and enforcement.
6.2	Is the system operated in full compliance with: DPA requirements; ICO codes of practice; SCC codes of practice; and Human Rights Act?	Yes.
6.3	Do you have procedures in place to manage risks associated with the use of CCTV cameras	Yes – see the remainder of this Policy.
7	Privacy Solutions	
7.1	Have you identified solutions to address any risks?	As set out in this Policy, the system is operated in line with relevant identified legislation and codes of practice.