



STOTFOLD TOWN COUNCIL
CCTV CODE OF PRACTICE 2026
VERSION 2.0

Contents

1.	INTRODUCTION AND OBJECTIVES	2
1.2	Statement in Respect of Human Rights Act 1998	2
1.3	Objectives of the System.....	2
1.4	System Review	3
2.	STATEMENT OF PURPOSE AND PRINCIPLE	3
2.1	Purpose.....	3
2.2	General Principles of Operation.....	3
2.3	Copyright.....	3
2.4	Monitoring and Recording Facilities	3
2.5	Processing and Handling of Recorded Material	3
2.6	Changes of this Code of Practice	3
3.	PRIVACY AND DATA PROTECTION	4
3.1	Data Protection Legalisation.....	4
3.2	Request for Information – Subject Access Request	4
4.	ACCOUNTABILITY AND PUBLIC INFORMATION	4
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.....	5
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. Principals for Release.....	7
4. Process of Disclosure.....	Error! Bookmark not defined.
5. Media Disclosure.....	Error! Bookmark not defined.
6. Principles.....	Error! Bookmark not defined.
Appendix 2 - Subject Access Request Form	10

1. INTRODUCTION AND OBJECTIVES

- 1.1 This Code of Practice is updated to reflect the Data Protection Act 2018, UK GDPR, and the Surveillance Camera Code of Practice (2021). The Council is registered as a data controller with the Information Commissioner's Office (ICO).

This Code of Practice applies to all CCTV cameras operated and managed by Stotfold Town Council at the following sites:

- The Greenacre Centre
- Riverside Multi Use Games Area

The system owner and Data Controller is Stotfold Town 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 Town 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 Council recognises its obligations under the Human Rights Act 1998, particularly Article 8, which provides for the right to respect for private and family life. The operation of the Council's CCTV system will be conducted in a manner that is lawful, necessary, and proportionate, with due regard to the impact on individuals' privacy. The Council will ensure that any interference with this right is justified by a legitimate aim, such as public safety, the prevention and detection of crime, or the protection of property, and that such interference is kept to the minimum necessary to achieve that aim.

1.3 Objectives of the System

The primary objective of the CCTV system is to protect Town Council owned property and increase the safety of the users of our facilities. 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 regularly 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 the principles of the Data Protection Act 2018 and UK GDPR, and the Surveillance Camera Code of Practice (2021). 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 sites mention in this code, will be stored as follows:

The Greenacre Centre – stored on site.
Riverside – stored locally.

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 Data Protection Act 2018 and UK GDPR provide individuals with rights regarding their personal data. The Council is committed to the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality, and accountability as set out in the UK GDPR:

- 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.

Subject Access Requests (SARs) can be made electronically and must be responded to within one month. No fee is chargeable. Data subjects have the right to erasure, rectification, and restriction of processing.

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 Schedule 2, Part 1, Paragraph 2 of the Data Protection Act 2018, personal data processed for the prevention or detection of crime, or the apprehension or prosecution of offenders, may be exempt from certain data subject rights (including subject access) to the extent that the application of those rights 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.

In responding to Subject Access Requests, the Council will undertake reasonable and proportionate searches for personal data, considering the information provided by the requester, the scope and nature of the request, and the impact on the rights and freedoms of others. Where a request is unclear, excessively broad, manifestly unfounded or excessive, or where compliance would involve a disproportionate effort, the Council may seek clarification, narrow the scope of the request, or refuse the request in whole or in part, in accordance with the Data Protection Act 2018, UK GDPR, and the Data (Use and

Access) Act 2025. Any such decision will be documented and communicated to the requester.

4. ACCOUNTABILITY AND PUBLIC INFORMATION

The Council will publish this Code of Practice and its privacy notice on its website, in line with the requirements of the Data Protection Act 2018 and UK GDPR.

5. ASSESSMENT OF THE SYSTEM

A Data Protection Impact Assessment (DPIA) will be conducted for any new or changed CCTV deployment.

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 using 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 to identify offenders or potential witnesses. In all cases this will need the permission of the Data Controller.

Any sharing of CCTV footage with third parties will be in accordance with the Data Protection Act 2018 and UK GDPR.

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.

Retention and destruction of CCTV footage will comply with the Data Protection Act 2018 and UK GDPR. Secure storage and access controls are in place.

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.

Version History

Version No	Date Approved/ Reviewed	Author/ Owner	Summary Of Changes	Responsible Committee	Review Date
1	January 2024	Town Clerk	Adopted	Buildings Management	January 2026
2	January 2026	Town Clerk	Reviewed and extensively updated with relevant legislation changes NB Not adopted by Town Council until July 2026.	Building Management	July 2028

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. Principals for Release

- All requests for the release of CCTV images will be considered in accordance with the Data Protection Act 2018, UK GDPR, and the Surveillance Camera Code of Practice (2021).
- Images will only be released where there is a clear lawful basis, and the release is necessary and proportionate.
- Images will not be released for commercial or entertainment purposes.
- An audit trail will be maintained for all disclosures.

2. Requests from the Police or Statutory Authorities

- Requests from the police or other statutory authorities must be made in writing and specify the legal basis for the request.
- The Council will only release images where satisfied that the request is lawful and necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders.
- All such disclosures will be documented, and the images released will be limited to what is strictly necessary for the stated purpose.

3. Requests for Civil Proceedings

- Images will only be released for use in civil proceedings where a court order or subpoena is provided.
- The Council will ensure that any such disclosure is lawful and proportionate, and that the rights of third parties are protected.

4. Disclosure to Individuals (Subject Access Requests)

- Individuals have the right to request images of themselves captured by the CCTV system.
- Requests can be made electronically and must be responded to within one month. No fee is chargeable.
- Only images of the requester will be disclosed. Images of third parties will be obscured unless consent is given or it is otherwise lawful to disclose.
- The Council may refuse a request if disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, in accordance with Schedule 2, Part 1, Paragraph 2 of the Data Protection Act 2018.

5. Requests from the Media

- Requests from the media must be made in writing and will only be considered where there is a clear public interest.
- Any images released will be edited to protect the identities of individuals unless there is a lawful basis for disclosure.
- The Council will always seek to minimise the risk of accidental identification of individuals.

6. General Safeguards

- All disclosures will be reviewed for compliance with the Data Protection Act 2018, UK GDPR, and the Surveillance Camera Code of Practice (2021).
- An audit trail will be maintained for all disclosures, including the date, recipient, purpose, and legal basis for release.

Notes

- (1) The release of data to the police is not restricted to the civil police but may include, for example, British Transport Police, Military Police, Ministry of Defence Police, etc. All requests must be made in writing, specify the legal basis, and be documented. Special arrangements may be put in place in response to local requirements.
- (2) Aside from criminal investigations, data may be of evidential value in civil proceedings or tribunals. In such cases, a solicitor or authorised representative of the tribunal must provide relevant information in writing prior to a search being granted. Release of data will only be facilitated on the instructions of a court order or subpoena. Any charge for this service must be reasonable and reflect actual costs incurred.
In all circumstances, data will only be released for lawful and proper purposes, in accordance with the Data Protection Act 2018 and UK GDPR.
- (3) There may be occasions when an enquiry by a plaintiff, accused person, defendant, or defence solicitor falls outside the terms of disclosure or subject access legislation. For example, the investigation of an alibi. Such requests will be considered on a case-by-case basis, ensuring compliance with the Data Protection Act 2018, UK GDPR, and the Human Rights Act 1998.
- (4) The Data Controller shall decide which (if any) other agencies may be permitted access to data. Such access will only be permitted in compliance with this Code of Practice and relevant legislation.
- (5) Under the Data Protection Act 2018 and UK GDPR, individuals have the right to access personal data of which they are the data subject, provided:
 - The request is made in writing (including electronically).
 - No fee is chargeable.
 - Sufficient information is provided to confirm the identity of the requester.
 - Sufficient and accurate information is provided about the time, date, and place to enable the Data Controller to locate the information (within one hour of accuracy is reasonable).
 - Only information relevant to the requester will be disclosed, and third-party data will be obscured unless consent is given or it is otherwise lawful to disclose.

Requests must be responded to within one month. The Data Controller may refuse a request if insufficient or inaccurate information is provided, or if an exemption applies (e.g., where disclosure would prejudice the prevention or detection of crime, as per Schedule 2, Part 1, Paragraph 2 of the Data Protection Act 2018).

- (6) A 'secondary' request is any request not falling into the category of a primary request. Before complying, the Data Processor must ensure:
 - The request does not contravene, and compliance would not breach, current legislation (e.g., Data Protection Act 2018, Human Rights Act 1998).
 - Any legislative requirements have been complied with.

- Due regard has been taken of any relevant case law.
- The request would pass a disclosure of 'public interest' test.

If material is to be released for crime prevention, written agreement should be obtained from a police officer not below the rank of Inspector, with personal knowledge of the circumstances and understanding of the CCTV Code of Practice.

(7) Requests from the media must follow the procedures for secondary requests. If material is to be released:

- A signed release document must state the purpose and limits for use.
- The receiver must process data as prescribed by the Data Controller (e.g., specific identities/data not to be revealed).
- Proof of editing must be provided to the Data Controller for approval before use.
- The release form is a contract and must be signed by both parties.
The Council will always seek to minimise the risk of accidental identification, as highlighted in the Peck case.

(8) Recorded material shall be processed lawfully and fairly, used only for the purposes defined in the Code of Practice, and access/release shall only occur in accordance with this standard and Code of Practice. Release for commercial or entertainment purposes is prohibited.

Appendix 2 - Subject Access Request Form

Stotfold Town Council CCTV System

Data Protection Act 2018 and UK GDPR

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. The law is set out in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). Further information is available from the Information Commissioner's 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 supply is not possible, would involve disproportionate effort, or if you agree otherwise. The Council will only provide that information if it is satisfied as to your identity. If release of the information would 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, 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 law 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 (see Data Protection Act 2018, Schedule 2, Part 1, Paragraph 2).

Fee

No fee is chargeable for a subject access request. However, the Council may charge a reasonable fee if a request is manifestly unfounded, excessive, or for additional copies of the data.

The application form

When you have completed and checked this form, please send it together with the required TWO identification documents (see below) to:

Town Clerk, Stotfold Town Council, Greenacre Centre, Valerian Way, Stotfold, Beds SG5 4HG
Or by email to: enquiries@stotfoldtowncouncil.gov.uk

STOTFOLD TOWN COUNCIL
CCTV SURVEILLANCE SYSTEM

DATA PROTECTION ACT 2018 AND UK GDPR

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	
Birth 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
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

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: <table border="1"> <tr> <td>a) View the information and receive a permanent copy</td> <td></td> </tr> <tr> <td>b) Only view the information</td> <td></td> </tr> </table>	a) View the information and receive a permanent copy		b) Only view the information	
a) View the information and receive a permanent copy				
b) Only view the information				

Section 4 – To help us find the information												
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.												
Were you (tick box below)												
<table border="1"> <tr> <td>Victim of an offence</td> <td></td> </tr> <tr> <td>A witness to an offence or incident</td> <td></td> </tr> <tr> <td>Other – please explain</td> <td></td> </tr> <tr> <td>Date(s) and time(s) of incident</td> <td></td> </tr> <tr> <td>Place incident happened</td> <td></td> </tr> <tr> <td>Brief details of incident</td> <td></td> </tr> </table>	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	
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 <table border="1"> <tr> <td>The information that I have supplied in this application is correct and I am the person to whom it relates.</td> <td></td> </tr> <tr> <td>Signed by</td> <td></td> </tr> <tr> <td>Date</td> <td></td> </tr> </table>	The information that I have supplied in this application is correct and I am the person to whom it relates.		Signed by		Date	
The information that I have supplied in this application is correct and I am the person to whom it relates.						
Signed by						
Date						