BILLINGBOROUGH PARISH COUNCIL

CCTV CODE OF PRACTICE

Management of the System

Normal operational responsibility of the scheme will be by nominated Councillors as per the published Councillor Roles. In the absence of these nominated councillors, responsibility will revert to the Chairman and the Clerk.

A CCTV Maintenance Company (such as mp cabling network services who carried out the installation), can access the system to carry out maintenance checks or essential repairs under the supervision of a nominated Councillor or the Clerk.

The CCTV system is located in a locked cabinet in the Pavilion. One set of Keys is held by the Clerk and one set by a nominated Councillor, who resides separately from the Clerk.

Breaches of this policy will be investigated by the Clerk and reported to the Parish 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 acceptable format for use at court hearings. This Policy, along with the Council's Privacy Notice, must be read and understood by all persons involved in this scheme and individual copies of the policy will therefore be issued for retention. A copy will also be available for reference in the CCTV system cabinet, on the Parish Council website and from the Clerk.

Control and Operation of the Camera, Monitor and System

In addition to the requirements of the Data Protection Policy and Privacy Notice, the following points must be strictly observed by all operators:

1. Authorised operators must act with due probity and not abuse the equipment or change the pre-set criteria to compromise the privacy of an individual.

2. The position of the camera and monitor have been agreed following consultation with the Police and security consultants in order to comply with the needs of the public.

3. No public access will be allowed to the monitor except for lawful, proper and with sufficient reason. Advance written approval must be granted by the Clerk on behalf of the Council. Access is arranged through a nominated Councillor or the Clerk

4. The Police are permitted access to recording media if they have reason to believe that such access is necessary to investigate, detect or prevent crime. Access is arranged through a nominated Councillor or the Clerk

5. The Police are permitted to visit the secure recording area to review and confirm the Parish Council's operation of CCTV arrangements. Any visit by the Police to view images to be logged by the Clerk, or nominated Councillor, whoever is in attendance. Access is arranged through a nominated Councillor or the Clerk.

6. Operators should carry out a monthly check on the accuracy of the date/time display on the CCTV system. The check should be recorded in the CCTV Log Book.
7. Digital records should be securely stored to comply with data protection and should be handled by the minimum number of essential persons for the minimum period necessary. In the case of vandalism or crime, images will be erased after a maximum period of 6-months or on completion of the investigation, whichever is the latter.

8. Digital images will not be supplied or shared with the media or social media, unless it is deemed to be in the public need and on the written advice of the Police. The Clerk or nominated Councillor will inform the Council as soon as possible, or Chairman in the event of an emergency.

9. Digital records may be required as evidence at Court. Such 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 officer and entered into the CCTV Log Book, with sufficient detail to identify the recording and Police Officer's name and Station. The log should also show when such information is returned to the Parish Council by the Police and/or the outcome of its use.

10. Any event that requires checking of recorded data should be clearly detailed in the, CCTV Log Book of incidents, by the nominated Councillor, or Clerk, whoever is in attendance including crime numbers if applicable, and the Council notified at the next available opportunity.

11. Any damage to equipment or malfunction discovered by the nominated councillor or Clerk should be reported immediately to the Council and Clerk and the details logged; Clerk to arrange repairs. When repaired, the details should be logged showing the date and time of completion.

12. Any request by an individual member of the public for access to their own recorded image must be made on the 'Access Request Form' detailed at Annex A and is subject to the standard fee in-line with the Council's Data Protection Policy Publication Scheme (Annex D). Forms are available from the Clerk and will be submitted to the Council for consideration and reply, normally within 40 calendar days of receiving the request.

Accountability

The Council's Policy and Code of Practice are based on the guiding principles of the Surveillance Camera Code of Practice 2013. A copy of the guiding principles is detailed at Annex B.

Copies of the CCTV Policy are available in accordance with the Freedom of Information Act 2000 and the Council's Data Publication Policy. Providing it does not breach security needs, responses will be actioned within 20 working days from receipt of the request.

The Police have been informed of the installation of the CCTV System and provided with a copy of this CCTV Policy.

Any written concerns or complaints regarding the use of the system will be considered by the Parish Council, in line with the existing complaints policy.

This CCTV Code of Practice was adopted by the Council in July 2017 and last reviewed at a general meeting on 10 March 2026.

ANNEX A

BILLINGBOROUGH PARISH COUNCIL
CCTV IMAGES ACCESS REQUEST FORM

<table>
<tr><td>Date of recording</td><td colspan="2">Time of recording</td><td>Place of recording</td></tr>
<tr><td colspan="2">Applicants name and address

Post Code

Telephone

Email</td><td colspan="2">Description of applicant and any distinguishing features (e.g. clothing) plus a recent photograph to aid identification, if necessary.</td></tr>
<tr><td colspan="2">Signature of applicant</td><td colspan="2">(or parent/guardian if under 18)</td></tr>
<tr><td>Received by</td><td>Clerk/Councillor signature</td><td>Date received</td><td>Time received</td></tr>
<tr><td>Fee charged</td><td>Fee paid</td><td>Request approved by Parish Council

YES / NO</td><td>Date applicant Informed</td></tr>
</table>

ANNEX B

SURVEILLANCE CAMERA CODE OF PRACTICE 2013

Guiding Principles
These are the guiding principles of the Surveillance Camera Code of Practice 2013. System operators should adopt the following 12 guiding 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.

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.

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.

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

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.

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.

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.

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.

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

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.

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.

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.