



Bishop Monkton Parish Council

CCTV Policy

SUMMARY

Bishop Monkton Parish Council operates CCTV and traffic-monitoring equipment to support road safety, evidence-based decision-making, and (where appropriate) the prevention of crime and anti-social behaviour.

The system is not used for general surveillance of individuals.

Purpose

Bishop Monkton Parish Council (“the Council”) operates, or may operate, closed circuit television (“CCTV”) and associated traffic-monitoring equipment within the parish.

The purpose of this Policy is to ensure that any such equipment is operated lawfully, fairly, transparently, securely and proportionately with appropriate regard to the privacy and rights of residents, visitors and other persons travelling through the parish and in compliance with the Surveillance Camera Code of Practice and Data Protection Act 2018.

The Council recognises that CCTV and traffic-monitoring equipment may capture information relating to identifiable individuals and vehicles and that such information may constitute personal data.

The Council will therefore ensure that surveillance technology is used only where there is an identified and documented need and where its use is proportionate to the objective being pursued.

Purpose

1. Scope

This Policy applies to surveillance and monitoring equipment operated on behalf of the Council, or with their authority including, where applicable:

- fixed CCTV cameras;
- temporary or mobile cameras;
- traffic-flow monitoring cameras;
- vehicle classification systems;
- Automatic Number Plate Recognition (“ANPR”) equipment;
- cameras capable of recording pedestrians, cyclists, horse riders and other road or path users;
- associated recording, storage and analytical equipment; and
- any contractor or third party processing information obtained from such systems on behalf of the Council.

The Policy applies to recorded images and other information derived from the equipment, including date, time, location, vehicle movements, vehicle registration marks and other information capable of identifying an individual.

2. Objectives of the System

CCTV and traffic-monitoring equipment may only be operated for clearly defined purposes approved by the Council.

These may include:

- 1) monitoring traffic volumes and movements through the parish;
- 2) assessing the type and classification of vehicles using particular roads;
- 3) identifying patterns of traffic movement, congestion or inappropriate routing;
- 4) obtaining objective evidence concerning road safety and traffic conditions;
- 5) monitoring the interaction between motor vehicles and vulnerable road users, including pedestrians, cyclists and horse riders;
- 6) supporting assessments of the use and safety of highways, junctions, crossings, footpaths and bridleways;
- 7) supporting representations to the relevant highway authority, planning authority, police or other public bodies;
- 8) assisting the Council in considering the potential traffic and highway effects of proposed developments;
- 9) supporting evidence-based community and highway-safety initiatives; and
- 10) where specifically approved and lawful, assisting in the prevention or investigation of crime, anti-social behaviour, vandalism or damage to Council property.

The system will not be used for purposes incompatible with those for which it was installed unless the Council is satisfied that the further use is lawful.

3. Governing Principles

The Council will operate its CCTV and monitoring systems in accordance with the following principles:

Lawfulness, fairness and transparency – personal data will be processed lawfully, fairly and transparently.

Purpose limitation – information will only be collected for specified, explicit and legitimate purposes.

Data minimisation – cameras and associated systems will collect no more information than is reasonably necessary.

Accuracy – reasonable steps will be taken to ensure that recorded dates, times and other system-generated information are accurate.

Storage limitation – information will not be retained for longer than is reasonably necessary.

Security – recordings and associated data will be protected against unauthorised access, alteration, disclosure, loss or destruction.

Accountability – the Council will maintain appropriate records demonstrating the reasons for and governance of its surveillance activities.

4. Legal and Regulatory Framework

The Council will have regard, where applicable, to:

- the UK General Data Protection Regulation (“UK GDPR”);
- the Data Protection Act 2018;
- the Data (Use and Access) Act 2025 and amendments to the UK data-protection framework;
- the Protection of Freedoms Act 2012 where applicable;
- ICO CCTV Code of Practice
- Human Rights Act 1998 (Article 8 – Right to Privacy
- Protection of Freedoms Act 2012
- Surveillance Camera Code of Practice (2021 Revision)
- relevant statutory surveillance-camera requirements and codes applicable to the Council;
- guidance issued by the Information Commissioner’s Office (“ICO”); and
- other legislation, statutory guidance or codes applicable to the Council and the particular surveillance activity.

The Council will periodically review this Policy to take account of changes in legislation, regulatory guidance and surveillance technology.

5. Data Controller

For the purposes of applicable data-protection legislation, the data controller is:

Bishop Monkton Parish Council

Contact details:

Data Protection Contact: Miss Sue Reid
Address: Chapel Villas, Dishforth, YO7 3LW
Email: clerk@bishopmonkton-pc.gov.uk
Telephone: 07881 989148

Formal responsibility for day-to-day administration of the system will rest with Proper Officer or approved delegate, subject to the oversight of the Council.

6. Lawful Basis

Before deploying surveillance equipment that processes personal data, the Council will identify and document an appropriate lawful basis for the processing.

Where the Council is performing a function in the public interest or exercising official authority, it will consider whether the processing is necessary for the performance of a task carried out in the public interest.

Where another lawful basis is relied upon, this will be identified and documented.

Consent will not ordinarily be relied upon as the lawful basis for general surveillance of public areas.

7. Data Protection Impact Assessment

Before introducing a new CCTV or traffic-monitoring system, or making a significant change to an existing system, the Council will consider whether a Data Protection Impact Assessment (“DPIA”) is required.

As a matter of good governance, a DPIA should normally be completed where surveillance involves systematic monitoring of publicly accessible areas or where the technology, scale or nature of the proposed monitoring creates an increased privacy risk.

The assessment should consider:

- the purpose and benefits of monitoring;
- whether monitoring is necessary;
- whether less intrusive alternatives are available;
- the location and field of view of cameras;
- categories of individuals likely to be recorded;
- the information collected;
- whether vehicle registration marks will be recorded;
- retention periods;
- access arrangements;
- disclosure arrangements;
- security measures;
- risks to individuals; and
- measures adopted to reduce those risks.

8. Camera Location and Field of View

Cameras will be positioned only where necessary to achieve an approved purpose.

Particular care will be taken to avoid unnecessary recording of:

- private homes and gardens;
- windows or entrances to residential properties;
- areas where individuals would reasonably have a heightened expectation of privacy; and
- land or activities unrelated to the stated monitoring purpose.

Where technically possible, privacy masking or equivalent technology will be used where a camera’s field of view would otherwise capture unnecessary private areas.

Camera locations and fields of view will be reviewed periodically and whenever there is a material change in circumstances.

9. Traffic Monitoring

Where cameras are primarily installed to obtain traffic information, the Council will seek, wherever reasonably practicable, to use aggregated or anonymised information for analysis and reporting.

Traffic reports may include information such as:

- total vehicle numbers;
- direction of travel;
- time and date;
- vehicle category;
- speed information where the equipment is capable of collecting it;
- peak traffic periods;
- pedestrian movements;
- cycling movements;
- horse and rider movements; and
- patterns of use of relevant roads, paths or bridleways.

Published reports should not ordinarily contain images or information identifying individual members of the public or individual vehicles unless there is a lawful and documented reason for doing so.

10. Vehicle Registration Numbers and ANPR

A vehicle registration mark may constitute personal data where it can be linked, directly or indirectly, to an identifiable individual.

The Council will not introduce ANPR or systematic number-plate recording merely because the equipment has the technical capability to do so.

Before activating such functionality, the Council will determine:

- why registration information is required;
- whether the purpose can be achieved without retaining registration numbers;
- the lawful basis for processing;
- the appropriate retention period;
- who will have access;
- the circumstances in which information may be disclosed; and
- whether the DPIA requires amendment.

Where only traffic counts or classifications are required, the Council should configure the system so that unnecessary registration information is not retained wherever reasonably practicable.

11. Audio Recording

Audio recording will be disabled by default.

The Council will not record conversations between members of the public.

Audio recording will only be considered where there is a specific, documented and lawful justification demonstrating that it is necessary and proportionate and that less intrusive means cannot reasonably achieve the identified and purpose subject to formal approval by the Council.

12. Signage and Public Information

Appropriate signs will be displayed where CCTV or other identifiable-person surveillance is taking place.

Signs should, as appropriate:

- be clearly visible;
- indicate that CCTV or monitoring equipment is operating;
- identify the Council as the operator/data controller;
- state the principal purpose of the monitoring; and
- provide contact details or direct individuals to further privacy information.

The Council will also make appropriate privacy information available through its website and/or other suitable means.

13. Live Monitoring

CCTV will not normally be continuously monitored by Council members or members of the public unless specifically justified by the purpose of the system.

Where remote or live access is available, access will be restricted to specifically authorised persons.

The system must not be used by authorised persons to observe individuals out of personal interest, curiosity or for any purpose unrelated to the Council's approved objectives.

14. Access to Recorded Information

Access to recorded footage and associated data will be strictly controlled.

Access may be granted only to persons authorised by the Council and where access is necessary for their role.

Authorised users must:

- maintain confidentiality;
- access information only for an authorised purpose;
- not copy, photograph or distribute recordings without authority;
- not disclose passwords or access credentials;
- comply with the Council's data-protection and information-security requirements; and
- report any actual or suspected security breach immediately.

Where technically available, the Council will maintain an audit trail showing access to, copying of and disclosure of recorded information.

15. Councillors and Members of the Public

The fact that a person is a Councillor, committee member, volunteer or resident does not automatically entitle that person to view CCTV footage.

Requests to view or obtain recordings must be dealt with through the Council's authorised procedures.

Recordings will not be shown at public meetings or distributed through email, social media or other channels unless the Council has established a lawful basis and appropriate safeguards for doing so.

16. Disclosure to Police and Other Authorities

Recorded information may be disclosed to the police, highway authority, planning authority, court, regulator or other public body where the disclosure is lawful, necessary and proportionate.

Requests should normally be made in writing and should identify:

- the requesting organisation;
- the identity of the requesting officer;
- the information required;
- the relevant date/time/location;
- the purpose for which it is required; and
- the legal basis or authority for the request, where appropriate.

The Council will maintain a record of material disclosures.

In urgent circumstances, information may be disclosed without a written request where this is lawful and necessary, provided that the circumstances and reasons for disclosure are subsequently documented.

All requests should come via the Proper Officer of the Council.

17. Disclosure to Third Parties

CCTV images will not routinely be disclosed to private individuals, businesses, developers, campaign groups or other third parties.

Any request will be considered on its individual merits having regard to:

- applicable data-protection legislation;
- the rights of persons shown in the recording;
- confidentiality;
- the purpose for which the recording was obtained;
- the reason for the request; and
- whether redaction or masking is required.

18. Subject Access Requests

Individuals have rights under data-protection legislation in relation to personal data concerning them.

A person who believes that they have been recorded may make a request for access to their personal data.

The Council may require sufficient information to locate the relevant recording, which may include:

- date;
- approximate time;
- location;
- description of the individual;
- description of the vehicle, where relevant; and
- other reasonable identifying information.

Before releasing footage, the Council will consider whether images of other identifiable individuals should be obscured or whether another exemption or restriction applies.

Requests will be handled in accordance with applicable statutory timescales and the Council's data-protection procedures.

19. Retention and Deletion

Recorded information will be retained only for as long as is reasonably necessary for the purpose for which it was obtained.

The Council adopts an appropriate CCTV retention period of 30 days, unless a different period has been documented as necessary for a particular system.

Information may be retained for longer where it:

- relates to a reported incident;
- is required for a police or other authorised investigation;
- is relevant to legal proceedings;
- is required to respond to a data-protection request;
- is required as evidence in relation to a planning, highway or safety matter; or

is otherwise required by law.

Where footage is preserved beyond the standard retention period, the reason for preservation and eventual deletion shall be recorded.

Aggregated or genuinely anonymised statistical traffic information may be retained for longer because it does not identify individuals.

20. Security

The Council will implement appropriate technical and organisational measures to protect CCTV information.

These may include:

- password-protected systems;
- individual user accounts;
- multi-factor authentication where available;
- encryption;
- secure physical storage;
- restricted administrator privileges;
- access logging;
- secure backup arrangements;
- controlled downloading and copying;
- software and firmware updates; and
- secure deletion or destruction.

Default manufacturer passwords must be changed before equipment is placed into operational use.

21. Cloud Storage and External Providers

Where footage or data is stored or processed by an external supplier, the Council will undertake appropriate due diligence.

Contracts with processors will include appropriate data-protection and security provisions.

The Council will establish where information is stored and whether any processing or transfer takes place outside the United Kingdom.

The Council will remain responsible for ensuring that its use of the system complies with applicable data-protection requirements.

22. Contractors

Any contractor installing, maintaining, hosting or operating equipment on behalf of the Council must:

- act only on documented instructions from the Council;
- maintain appropriate confidentiality and security;
- restrict access to authorised personnel;
- promptly report security incidents;
- assist the Council with data-subject rights where required; and
- securely return or delete personal data at the end of the contractual relationship where appropriate.

23. Data Breaches

Any loss, unauthorised disclosure, unauthorised access, cyber incident or other compromise involving CCTV recordings or associated personal data must be reported immediately to the Proper Officer & Data Protection Officer so that the system governance may be reviewed and disciplinary action, of applicable, may be instituted.

The Council will assess the incident in accordance with its personal-data-breach procedures and determine whether notification to the ICO and/or affected individuals is required.

24. Complaints

Questions or complaints concerning the operation of the CCTV system should initially be addressed to:

25. Proper Officer

Complaints will be investigated in accordance with the Council's complaints and data-protection procedures.

Individuals also have the right to raise concerns with the Information Commissioner's Office.

26. Misuse

Unauthorised access to, copying, disclosure or use of CCTV information is strictly prohibited.

Any suspected misuse will be investigated and may result in:

- withdrawal of system access;
- disciplinary or other action;
- termination of a contractor's appointment;
- referral to the Council;
- notification to the ICO; and/or
- referral to the police or another authority where appropriate.

27. Public Reporting

Where surveillance equipment is used for traffic or highway monitoring, the Council may publish statistical reports and analysis.

The default approach will be to publish aggregated or anonymised information rather than identifiable images or vehicle registration information.

Reports may be used to support:

- highway-safety proposals;
- traffic-management measures;
- planning representations;
- Neighbourhood Development Plan evidence;
- discussions with the highway authority;
- assessment of development proposals;
- pedestrian, cycling and equestrian safety initiatives; and
- other legitimate Council functions.

28. Periodic Review

The Council will review each surveillance system periodically, at least on an annual basis, to establish whether:

- the original purpose remains valid;
- surveillance remains necessary and proportionate;
- the cameras remain appropriately positioned;
- the information collected remains relevant and necessary;
- retention periods remain appropriate;
- security arrangements remain adequate;
- access remains appropriately restricted;
- signage and privacy information remain accurate;
- technological changes have introduced additional privacy risks: and in compliance with the 12 Principles of the Surveillance Camera Code (2021 revision specified at para 5, above

Where a system is no longer necessary or proportionate, the Council will consider removing it or modifying its operation.

29. Policy Review

This Policy will be reviewed at least annually and sooner where there is:

- a material change to the CCTV or monitoring system;
- introduction of ANPR, artificial intelligence, facial recognition or other enhanced surveillance technology;
- a significant data-protection incident;
- a change in applicable legislation or regulatory guidance; or
- a material change to the purpose for which monitoring is undertaken.

Version Control

Date	Version	Description
August 2026	1.0	Draft
September	1.1	Draft