BARTON UNDER NEEDWOOD
VILLAGE HALL
CROWBERRY LANE, BARTON UNDER NEEDWOOD, BURTON ON TRENT, DE13 8AF
REGISTERED CHARITY NO: 502046
BOOKINGS AND ENQUIRIES: 07568 302247
EMAIL: BARTONVILLAGEHALLBOOKINGS@GMAIL.COM
WWW.BARTONUNDERNEEDWOODVILLAGEHALL.ORG

CCTV Policy

Introduction

This Policy should be read with reference to the Data Protection Act 2018, Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act 2012 (PFA), the Human Rights Act 1998 (HRA), the Secretary of State's Surveillance Camera Code of Practice (SC code) and the Information Commissioner's Office (ICO) CCTV Code of Practice.

This CCTV Policy explains how Barton under Needwood Village Hall Committee will operate its CCTV equipment and comply with the current legislation.

Background

Several factors have informed Barton under Needwood Village Hall Committee's decision to extend their CCTV.

These include:

- Two events in 2025 which saw staff abused and the Hall maliciously vandalised.
- The Terrorism (Protection of Premises) Act, known as Martyn's Law, which is now law and is being developed to ensure the public is better protected from terrorism by requiring certain public premises and events to be prepared and ready to keep people safe in the event of an attack. Barton under Needwood Village Hall is one of those premises.
- Recent events such as the one in Southport.

For the purposes of this Policy:

- Barton under Needwood Village Halll Committee (the Committee) retains overall responsibility for the system.
- the 'Data Protection Officer (DPO)' is responsible for the operational system and for ensuring compliance with this policy and is nominated by the Committee.

The CCTV system has been notified to the Information Commissioner with whom the Committee is registered (Registration Reference ZC141053) as Data Controller.

Under the Protection of Freedoms Act 2012 and Data Protection Act 2018 the processing of personal data captured by CCTV systems is governed (including images identifying individuals). The Information Commissioner's Office (ICO) has issued a Code of Practice on compliance with legal obligations. The use of CCTV is covered by the Act, regardless of the number of cameras or how sophisticated the equipment is, and the Committee adheres to the ICO's Code of Practice.

The Committee is committed to informing its staff, volunteers, hirers, and contractors about the presence of and operation of CCTV. This Policy is available on The Committee's website so that all stakeholders are clear about how CCTV is utilised and signage is displayed throughout the Hall.

Access to personal information recorded through CCTV cameras is restricted solely to the Data Protection Officer appointed by the Committee but only on the authorisation of the Committee.

Objectives

The Committee uses CCTV equipment to:

- provide a safe and secure environment for volunteers, staff, hirers, visitors, and contractors.
- deter, detect, and prevent crime, vandalism, and anti-social behaviour.
- monitor the security of the site.
- ensure use of the Hall is per hiring agreements.
- assist Law Enforcement Agencies to carry out their lawful duties.

This list is not exhaustive, and other purposes may be or become relevant.

The Committee does not use the CCTV system for covert monitoring.

Location

Cameras are located in those areas where it has been identified there is a need and where other solutions have proved ineffective. The locations have been dictated by recent events at the Hall which included abuse and vandalism (2025). The CCTV system comprises of 7 cameras covering the main rooms, the foyer and part of the stairwell.

The CCTV system is used solely for purposes identified and is not used to routinely monitor staff, volunteers, hirers, or contractors conduct. Cameras will not be used in areas subject to a heightened expectation of privacy i.e. the toilets. Signage alerts individuals to the use of CCTV.

Static cameras will not focus on private homes, gardens, and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Recordings will never be released to the media for purposes of entertainment.

Maintenance

The CCTV system is maintained by Burton Aerial Services on behalf of The Committee and includes periodic maintenance inspections.

The Committee is responsible for:

- Ensuring that it complies with its responsibilities in relation to guidance on the location of the camera.
- Ensuring that the date and time reference are accurate.
- Ensuring that suitable maintenance and servicing is undertaken to ensure that clear images are recorded.
- Ensuring that the Data Protection Officer is trained in the use of the equipment.
- Ensuring that cameras are protected from vandalism in order to ensure that they remain in working order.

Identification

In areas where CCTV is located, the Committee will ensure prominent signs are in place.

Type of equipment

The Committee's standard CCTV cameras record visual images only and have been set not to record sound.

The CCTV system operates 24 hours a day, 365 days a year.

Administration

The Committee has responsibility for the control of images and deciding how the CCTV system is used. The Committee has notified the Information Commissioner's Office of both its name as the Data Controller and the purpose for which the images are used. Only the Data Protection Officer will have access to images and is aware of the procedures that need to be followed when accessing the recorded images. He/she is trained and aware of responsibilities under the CCTV Code of Practice: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/cctv/

Access to recorded images is restricted to the Data Protection Officer and recordings will be accessed as prescribed by the Committee in the event of an incident.

Access to the medium on which the images are recorded is documented. All employees are aware of the restrictions in relation to access and security, and disclosure of, recorded images.

Image storage, viewing, and retention

Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified.

The recording system records digital images; all CCTV images held on the hard drive are deleted and overwritten on a recycling basis every 30 days. Images will not be stored on, or transferred to, removable media such as CDs or flash drives unless required as evidence by the Police or other law enforcement agencies. The Committee reserves the right to monitor the CCTV at random intervals.

The Committee reserves the right to use images captured on CCTV where there is activity that cannot be expected to be ignored such as criminal activity, potential gross misconduct, or behaviour which puts others at risk. The Data Protection Officer will retain images for evidential purposes securely. Where images are retained, the Data Protection Officer will ensure the reason for its retention is recorded, where it is kept, any use made of the images and finally when it is destroyed.

The Committee ensures that images are not retained for longer than is necessary, typically 31 days. Once the retention period has expired, images are removed or erased.

Disclosure

Disclosure of the recorded images to third parties can only be authorised by the Committee.

Disclosure of images to third parties will only be made in accordance with the objectives for which the system is used and will be limited to:

1. The Police and other Law Enforcement Agencies, where the images recorded could assist in the:
    a. Prevention or detection of a crime.
    b. Identification and prosecution of an offender.
    c. Identification of a victim or witness.
2. Prosecution agencies, such as the Crown Prosecution Service.
3. Relevant legal representatives.
4. Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders). Note disclosure will only be granted:

    - If its release is fair to all individuals concerned.
    - If there is an overriding legal obligation (e.g. information access rights).
    - If it is consistent with the purpose for which the system was established.

All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented.

N.B Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

Access to recorded images is restricted to the Data Protection Officer nominated by the Committee. Disclosure of information will be controlled and consistent with the purpose(s) for which the CCTV system has been established. Once information is disclosed to a Law Enforcement Agency, they will become data controller for the copy which they hold.

Subject Access Requests

Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If The Committee receives a Subject Access Request under the General Data Protection Regulations 2018 it will comply with requests within 1 month. The Committee may charge a fee for the provision of a copy of images. If the Committee receives a request under the Freedom of Information Act 2000 it will comply with requests within 20 working days of receiving the request.

Generally, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data, and its disclosure is unlikely as a Freedom of Information request.

Those requesting access must provide enough detail to allow the operator to identify that they are the subject of the images, and for the operator to locate the images on the system. Requests for access should be addressed to the Data Controller.

Refusal to disclose images may be appropriate where its release is:

- Likely to cause substantial and unwarranted damage to that individual.
- To prevent automated decisions from being taken in relation to that individual.

The following guidelines will be adhered to in relation to the disclosure of images:

a) The disclosure of images will be in line with the above Objectives and will be controlled under the supervision of the Data Controller;
b) A log will be maintained itemising the date, time(s), camera, person copying, person receiving and reason for the disclosure;
c) The appropriate disclosure documentation from the Law Enforcement Agencies will be filed for future reference;
d) Images must not be forwarded to the media for entertainment purposes or be placed on the internet;
e) Images must not be copied in any way, e.g. photographed, downloaded or printed for use other than described in the objectives;
f) Images will only be released to the media for identification purposes in liaison with the Law Enforcement Agencies;
g) The method of disclosing images should be secure to ensure that they are only seen by the intended recipient; and
h) Images of third parties not relevant to the investigation should be obscured where possible to prevent unnecessary identification.

Monitoring and evaluation

The Committee undertakes regular audits to ensure that the use of CCTV continues to be justified. The audit includes a review of:

- Its stated purpose.
- The location.
- The images recorded.
- Storage length.
- Deletion.

Period of Review

The efficacy of this Policy will be reviewed bi-annually by The Committee. If the Committee decides to change the way in which it uses CCTV, it will inform the Information Commissioner within 28 days.

Guiding Principles

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.

Data Controller: **Barton under Needwood Village Hall Committee**
ICO Registration: ZC141053

Policy Adopted: May 2026
Next Review: May 2027