HARTLEBURY PARISH HALL

CCTV POLICY

This is a joint policy with Hartlebury Parish Council

1. Provenance

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.

2. Background & Introduction

Under the Protection of Freedoms Act 2012 and Data Protection Act 2018 the processing of personal data captured by CCTV systems is governed (including recordings 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 Hartlebury Parish Council together with the Parish Hall Management Committee adheres to the ICO's Code of Practice.

The system is jointly operated by the Hartlebury Parish Council (Council) and the Hartlebury Parish Hall Management Committee (Hall), referred to collectively as the Controllers.

The Council and Hall are committed to informing its staff, volunteers and service users about the presence of and operation of CCTV. This Policy is available on the Hartlebury Parish Council's website so that all stakeholders are clear about how CCTV is utilised.

Access to personal information recorded through CCTV cameras is restricted solely to the Data Protection Officer appointed by Hartlebury Parish Council and the trained member of the Parish Hall Management Committee (Hall Rep).

3. Objectives and targets

This CCTV Policy explains how the Controllers will operate its CCTV equipment and comply with the current legislation.

The Council and Hall uses CCTV equipment to provide a safer, more secure environment for their staff, volunteers and service users and to combat vandalism and theft. Essentially it is used for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of recordings as evidence in criminal proceedings).
- Safeguarding public, volunteers and staff.
- Monitoring the security of the site.
- To protect members of the public and private property

The Controllers do not use the CCTV system for covert monitoring.

4. Location

Cameras are located in those areas where it has been identified there is a need and where other solutions are ineffective. The CCTV system is used solely for purpose(s) identified and is not used to routinely monitor staff, volunteers, or service users' conduct. Cameras will not be used in areas subject to a heightened expectation of privacy e.g. changing rooms or toilets. Signage alerts individuals to the use of CCTV on entrance to the areas covered.
Static cameras will not focus on private homes, gardens and other areas of private property.

5. Maintenance

The CCTV system is jointly maintained by Hartlebury Parish Council and Parish Hall and includes periodic maintenance inspections.

The Controllers are responsible for:

- Ensuring that it complies with its responsibilities in relation to guidance on the location of the cameras.
- 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 and Hall Rep are trained in the use of the equipment.
- Ensuring that cameras are protected from vandalism in order to ensure that they remain in working order.

6. Identification

In areas of entrance to the Hall, car parks, pétanque court, MUGA and tennis court, the Controllers will ensure prominent signs are in place.

The signs will:

- Be clearly visible and legible.
- Contain details of the organisation operating the scheme, the purpose for using CCTV and who to contact about the scheme.
- Be an appropriate size depending on context.

7. Type of equipment

The standard CCTV cameras record visual images only and do not record sound. The Network Video Recorder (NVR) has rolling storage for 30 days worth of recordings from all cameras.

8. Administration

Hartlebury Parish Council will assign a Data Protection Officer who will have responsibility for the control of the recordings. The Controllers have notified the Information Commissioner's Office of both the name of the Data Controllers and the purpose for which the recordings are used. Only the Data Protection Officer and the Hall Rep will have access to recordings, and are aware of the procedures that need to be followed when accessing the recorded images. They are trained and are aware of responsibilities under the CCTV Code of Practice:
https://ico.org.uk/fororganisations/guide-to-data-protection/encryption/scenarios/cctv/

Access to recorded images is restricted to the Data Protection Officer and Hall Rep. Recordings will be accessed as prescribed by this policy in the event of an incident.

Access to the NVR on which the images are recorded is documented.

9. Image storage, viewing and retention

CCTV recordings will be captured in a way that ensures the integrity of the recording and in a way that allows specific times and dates to be identified. The recording equipment will be located in a locked cabinet within the Parish Hall.

The Controllers reserve the right to use recordings 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 or Hall Rep will retain recordings for evidential purposes in a locked area. Where recordings are retained, the Data Protection Officers will ensure the reason for its retention is recorded, where it is kept, any use made of the recordings and finally when it is destroyed.

The Controllers ensure that recordings are not retained for longer than is necessary. Once the retention period has expired, recordings are removed or erased. The maximum time that any recordings are stored is 30 days unless further retention is requested by an authorised body.

10. Disclosure

Disclosure of the recorded images to third parties can only be authorised by the Controllers in consultation with the ICO.

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.

All data processing also complies with article 10 of the GDPR legislation (2018). Specifically: "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6 shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

11. Subject Access Requests

Individuals whose images are recorded have a right to view recordings of themselves and, unless they agree otherwise, to be provided with a copy of the recordings. If the DPO receives a Subject Access Request under the General Data Protection Regulations 2018 it will comply with requests within 14 days. The Council may charge a fee for the provision of a copy of recordings. If the Council receives a request under the Freedom of Information Act 2000 it will comply with requests within 14 working days of receiving the request.

As a general rule, if the DPO 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 recordings, and for the operator to locate the recordings on the system. Requests for access should be addressed to the clerk.

Refusal to disclose recordings may be appropriate where its release:

- Is likely to cause substantial and unwarranted damage to that individual.
- Has been requested by a law enforcement authority in relation to a suspected crime.

12. Monitoring and evaluation

Hartlebury Parish Council in conjunction with the Hall 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.

13. Period of Review

The efficacy of this Policy will be reviewed biennially by the Controllers. If the Controllers decide to change the way in which it uses CCTV, it will inform the Information Commissioner within 28 days.

14. 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 recordings 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 recordings and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such recordings and information should be deleted once their purposes have been discharged.

7. Access to retained recordings 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 recordings 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 recordings 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.

Adopted
16.10.24
Reviewed and
Accepted