ART· NATURE· CREATIVITY

COMPTON VERNEY

CCTV Policy

Purpose

This policy establishes guidelines for the operation and management of Compton Verney's closed-circuit television (CCTV) system.

The primary objectives and lawful basis for CCTV surveillance are:

- Deter and detect crime
  To discourage and identify criminal activity and anti-social behaviour
- Protect individuals and property
  To safeguard visitors, staff, estate, assets, loaned art works, and the collections
- Facilitate incident investigations
  To aid in the investigation of incidents, crimes, accidents, or breaches of our policies and procedures

Compton Verney House Charity (CVHC) operates a CCTV surveillance system comprising of approximately 85 fixed cameras strategically placed throughout the estate, including perimeters, entrances and exits, car parks, public areas, and gallery spaces.

Our security contractors monitor live CCTV footage from the Control Room to assess and respond to security concerns. Video images are recorded and stored securely onsite for a maximum of 35 days.

The CCTV system does not capture audio and does not employ Automatic Number Plate Recognition, Facial Recognition Technology, or machine learning algorithms.

CVHC is committed to protecting the confidentiality, security, and integrity of personal information collected from its staff, volunteers, trustees, participants, visitors, partners, and other individuals. Images captured by the CCTV system, which include recognisable individuals, constitute personal data and are processed in accordance with our GDPR Policy and Cyber Security Framework.

Scope

This policy applies to all on site CCTV systems operated by CVHC, encompassing both indoor and outdoor areas of the premises. It does not cover the use of conventional cameras for promotional activity or artistic purposes, such as for film making.

Legislation and Guidance

CVHC's CCTV system is registered with the Information Commissioner's Office (ICO) and full details are available on the data protection public register (**www.**ico.org.uk).

This policy complies with the *UK General Data Protection Regulation (UK GDPR)* and the *Data Protection Act 2018*. CVHC processes personal data captured by its CCTV systems in accordance with data protection principles and the *Human Rights Act 1998*, as described in our GDPR Policy.

This policy is based on the *Surveillance Camera Code of Practice* issued under the *Protection of Freedoms Act 2012*.

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. For example, this may include an individual's: • Name (including initials) • Image • Identification number • Location data • Online identifier, such as a username
CCTV	A closed-circuit television or automatic number plate recognition system and any other system for recording or viewing visual images for surveillance purposes.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Roles and Responsibilities

Trustees (Data Controller)

- Approve and review the CCTV Policy annually, ensuring it's compliant, proportionate, and fit for purpose.
- Approve annual budgets for CCTV spending.
- Identify, evaluate, and proactively manage risks associated with the CCTV system.
- Report any serious incidents to the Charity Commission.

Chief Executive Officer (CEO)

- Provides strategic oversight of the CCTV Policy.
- Communicates changes, risks, and opportunities to the board and alerts them to data breaches.
- Reports data breaches to the Information Commissioner's Office (ICO) with the DPO.

Chief Operating Officer (COO)

- Assigns data protection roles and responsibilities.
- Coordinates the implementation of the CCTV Policy across the organisation.
- Reviews and updates the CCTV Policy regularly.
- Reviews and monitors incidents, reporting them to the CEO.
- Reviews and approves CCTV contracts and agreements.
- Monitors exposure to major threats related to the CCTV system.

Data Protection Officer (DPO)

The DPO is CVHC's competent person, trained in data protection, and is responsible for:

- Monitors compliance with data protection law and develops related policies and guidelines.
- Ensures Data Protection Impact Assessments (DPIAs) are carried out for changes to data processing or storage.
- Provides an annual report on data protection activities to the Executive and Trustees.
- Acts as the first point of contact for individuals whose data CVHC processes and for the ICO.
- Responds to subject access requests for access to recorded CCTV footage.

Facilities and Operations Manager

- Oversees the day-to-day maintenance and operation of the CCTV system.
- Ensures images are deleted in accordance with the retention policy.
- Authorises staff to view images when investigating incidents.
- Arranges for periodic maintenance checks by suppliers.
- Trains Facilities & Operations Team members on the CCTV system and data protection compliance.

Security Personnel – Contractor (Data Processor)

- Operate and maintain surveillance equipment.
- Monitor live and recorded footage.
- Report incidents or suspicious behaviour.
- Contact authorities when necessary.

We have written contracts in place that clearly define the responsibilities of organisations that provide processing services for us. We make sure that information is only processed by others in accordance with our instructions, with guarantees about security, storage, and the use of properly trained staff.

CVHC expects all employees to follow this policy and those who misuse the system or cause serious data breaches may face disciplinary action. CVHC will examine each incident on a case-by-case basis and follow the Disciplinary Policy.

Employees, volunteers, or Trustees who are observed to disregard our procedures may face progressive discipline, even if their behaviour hasn't resulted in a data breach.

Failure of contractors, temporary staff, partners, or third-party organisations to comply with this policy may result in termination of contracts and connections, or the suspension of services.

Covert Recording

Covert cameras are not routinely used at Compton Verney and may be used only in very limited circumstances. This requires the written authorisation of the Chief Executive, Chief Operating Officer, and, where this may involve members of staff, the People Manager.

Covert surveillance may be carried out in cases of suspected specific criminal activity only where the objective of making the recording would be seriously prejudiced should the individuals concerned be informed of such surveillance.

Authorisation to use covert surveillance must include:

- a justification of the need to use such methods to obtain evidence of suspected criminal activity in a specific case.
- an assessment of alternative methods of obtaining such evidence.
- a statement of how long the covert monitoring should take place.

The authorisation must be reviewed by the CEO every 28 days, and they will consider whether that should continue or be closed. Any decision to use covert surveillance for any reason must be fully documented and records of such decision retained securely.

Applications to Review CCTV Images

There will be no disclosure of recorded CCTV footage to third parties other than to enforcement authorities such as the Police and other statutory organisations where there is a lawful need to access the footage.

CVHC staff may apply for CCTV footage to be reviewed by security personnel when a crime or incident has occurred and there is a reasonable likelihood that the event or evidence has been recorded on the system. Images may be required as part of criminal or civil court proceedings. Such applications should be made on the Access Request Form, included as Appendix 2.

Images may also be accessed by the relevant Investigating Manager, if necessary, as part of an internal disciplinary investigation. Images may then be disclosed as part of the evidence assembled by the Investigating Manager in the event of a disciplinary hearing or employment tribunal..

Staff submitting applications for a review of the CCTV recordings will be required to provide sufficient information to enable the request to be considered and located.

The Facilities & Operations Manager will then determine, in consultation with the DPO, whether the incident warrants examination of the recording and whether there is a reasonable likelihood that the event or evidence has been recorded on the system.

If the footage contains images of other individuals, then the Facilities & Operations Manager must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained
- Whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

Specialist software may be used to redact visual and audio data of third parties (techniques include blurring, masking, or using a solid fill to completely obscure parts of the footage).

Application by the Authorities

As records may be required as evidence at Court, each person handling a digital record may be required to make a statement to a police officer and sign an exhibit label. Any images that are handed to a police officer should be signed for by the officer and information recorded in the Logbook to identify the recording and showing the officer's name, number, crime number, and police station.

Subject Access Requests (SAR)

All individuals have a right to make a subject access request (SAR) to gain access to personal information that CVHC holds about them.

Anyone who believes that they have been filmed by the CCTV system can request a copy of the recording, subject to any restrictions covered by the Data Protection Act. Individuals also have the right to request that inaccurate data be corrected or erased and to seek redress for any damage caused. CVHC will comply with UK GDPR when considering such a request.

The SAR procedure included in the GDPR Policy must be followed and requests should be directed to the DPO.

Where CVHC is unable to comply with a SAR without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless that individual has consented to the disclosure or it is reasonable, in the circumstances, to comply without the consent of the individual.

CVHC may be unable to provide copies of recorded images where this may prejudice the legal rights of other individuals during a police investigation.

Regular Review

This CCTV policy is reviewed annually to ensure its ongoing compliance with legal and regulatory requirements and to adapt to evolving technological and operational needs.

As detailed in our GDPR Policy, a Data Protection Impact Assessment (DPIA) must be undertaken whenever the development or changes to the surveillance camera system are first considered. This must ensure that the purpose of the system is and remains justifiable, there is consultation with those most likely to be affected, and the impact on their privacy is assessed and any appropriate safeguards can be put in place.

Contact Information

For inquiries related to this CCTV policy or to exercise data protection rights, please contact:

Data Protection Officer

Compton Verney
Warwickshire,
CV35 9HZ

01926 645500

info@comptonverney.org.uk