Creative Works CCTV Policy

Last updated: July 2025
Next review due: October 2027
Policy Owner: NS

1. Introduction

Creative Works (CW), operated by Big Creative Community CIC, uses a Closed Circuit Television (CCTV) system to enhance the safety and security of its staff, clients, visitors, and premises. The system also supports property protection, behavioural oversight, and operational management.

CCTV is considered personal data under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. This policy sets out the lawful use, management, and responsibilities associated with the system. It reflects guidance from the **ICO's CCTV Code of Practice** (latest version at: https://ico.org.uk).

All CCTV operations must uphold individuals' privacy rights under the **Human Rights Act 1998** and comply with CW's internal data protection and privacy policies.

---

2. Purpose of CCTV

CW uses CCTV to:

- Protect buildings and assets against unauthorised access, vandalism, or damage
- Safeguard staff, clients, and visitors by deterring and documenting potential threats
- Support the police in preventing and investigating criminal activity
- Aid in the identification of individuals involved in disciplinary or safeguarding incidents
- Monitor communal areas to ensure adherence to fair usage and conduct policies
- Provide operational oversight and contractor compliance reporting
- Support building usage and event management

---

3. System Overview

- The system comprises fixed and dome cameras positioned in strategic internal locations
- Coverage includes entrances/exits, communal areas, and workspaces
- Cameras operate continuously, switching to motion detection mode overnight
- Signage is displayed prominently at site entry points, in line with ICO standards
- The system includes digital video recorders and secure access controls
- Third-party monitoring partners may view live feeds when an alarm is triggered, but are never granted access to historical footage

Limitations: The CCTV system does not cover all areas and cannot guarantee detection of every incident.

---

4. Management and Operation

- **Data Controller:** Creative Works
- **System Owner:** Big Creative Community CIC
- **Policy Lead:** Director of Operations (DOO)
- **Daily Operation:** Head of Operations and Communications (HOC)

The system is registered with the **Information Commissioner's Office (ICO)** and operates in full compliance with the **UK GDPR**.

Live and recorded footage may only be accessed by authorised personnel (see section 6). PTZ (pan-tilt-zoom) cameras must not be used to focus on individuals or private property without proper authorisation unless responding to an active incident.

Prohibited Use:

- No footage may be used for commercial purposes

- No footage may be viewed or released for entertainment or social media

---

5. Accessing Footage

5.1 Live Monitoring

Authorised staff may view live footage for operational or safety reasons.

5.2 Image Search and Downloads

Access is strictly controlled. A **CCTV Release Form** must be submitted and approved before footage can be reviewed or downloaded. All actions are logged.

Authorisation required:

- **Client/public incidents:** Approved by HOC
- **Staff incidents:** Approved by DOO or MD

Authorised personnel include:

- Managing Director
- CW Community Manager
- BCE Facilities Manager
- Security staff
- IT staff (for technical access only)
- CW Reception staff

Conditions for download:

- Must be approved in writing
- Shared only via password-protected physical media

- Must be returned for secure deletion after use
- Never emailed, shared via cloud services, or posted online
- Only released to the police upon receipt of a valid **CCTV Release Form** and a **warrant card**

---

6. Subject Access Requests (SARs)

Under the **Data Protection Act 2018**, individuals can request access to CCTV footage in which they are identifiable.

Requests must be:

- Submitted in writing to the **DOO**
- Accompanied by proof of identity
- In line with this guidance: gov.uk CCTV SAR advice

CW will respond within 30 calendar days where possible.

---

7. Third-Party Requests

Third parties (excluding data subjects) have no automatic right to CCTV footage.

Requests may be granted only if made by:

- Law enforcement (as part of a criminal investigation)
- Prosecution agencies
- Insurers or legal representatives (with valid cause)

Conditions for access:

- Submission of the external **CCTV Request Form** (available at http://www.bigcreative.education/cctv-external/)

- Full details including time, date, camera location, reason, and proof of identity

All decisions (approved or declined) will be recorded. If declined, reasons will be provided in writing.

---

8. Retention and Disposal

- Recordings are automatically deleted after 30 days unless retained as part of an investigation
- Downloads are securely stored, monitored, and destroyed following investigation closure
- Still images and hard copies are treated as confidential waste and disposed of accordingly

---

9. Installation of New Cameras

Prior to installation of any new cameras:

- A formal privacy impact assessment must be completed
- Justification for use must be documented in line with **ICO Part 4 guidance**
- Responsible persons for compliance must be clearly assigned

---

10. Complaints

Complaints about the CCTV system should follow the standard CW Complaints Procedure.

---

11. Breaches and Misuse

Unauthorised interference with CCTV equipment (e.g., unplugging, tampering, or obscuring cameras) is a disciplinary matter.

Violations of this policy may lead to disciplinary action under CW's internal procedures.

Date Updated	To Review	Responsibility
July 2025	Jul 2027	EG