



# CCTV Policy

Policy | 2026-27

|                        |                                           |
|------------------------|-------------------------------------------|
| <b>Policy name</b>     | CCTV Policy                               |
| <b>Version</b>         | 1.0                                       |
| <b>Status</b>          | Live                                      |
| <b>Author</b>          | Gareth Kyle, Academy Business Leader      |
| <b>Approval body</b>   | Resources, Audit & Risk Committee         |
| <b>Date approved</b>   | October 2026                              |
| <b>Review cycle</b>    | Annual                                    |
| <b>Next review due</b> | Autumn 2027                               |
| <b>Published on</b>    | Both (Trust website and National College) |
| <b>Applies to</b>      | Trust-wide                                |

## Revision history

| Version | Date         | Author      | Summary of change                                                                                                                          |
|---------|--------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0     | October 2026 | Gareth Kyle | First Trust CCTV policy, based on The School DPO Service model CCTV policy (May 2025). Submitted to the Resources, Audit & Risk Committee. |

# Index

---

## The Policy

|                                            |   |
|--------------------------------------------|---|
| 1. Aims and scope .....                    | 3 |
| 2. Legislation and guidance.....           | 3 |
| 3. Roles and responsibilities.....         | 4 |
| 4. Location of the cameras and signs ..... | 4 |
| 5. Operation of the system .....           | 4 |
| 6. Covert surveillance .....               | 5 |
| 7. Storage and retention of footage.....   | 5 |
| 8. Access to footage .....                 | 5 |
| 9. Data protection impact assessment ..... | 6 |
| 10. Security.....                          | 6 |
| 11. Complaints.....                        | 6 |
| 12. Monitoring and review .....            | 7 |
| 13. Linked policies and documents .....    | 7 |

## 1. Aims and scope

---

- 1.1** This policy sets out how The Cedars Academy Trust (the Trust) operates, manages and uses its closed circuit television (CCTV) system at Cedars Academy: Low Fell and Cedars Academy: High Heworth. It applies to everyone who works for the Trust, and to anyone who operates the system or handles footage on the Trust's behalf.
- 1.2** The purpose of the CCTV system is to:
- help keep pupils, staff and visitors safe
  - protect pupils, staff and visitors from harm to themselves or to their property
  - deter crime on Trust premises
  - protect Trust buildings and assets
  - help the police to prevent and detect crime
  - find out the cause of accidents
  - help the Trust look into safeguarding concerns and allegations, complaints, and disciplinary and grievance matters
  - help the Trust defend legal claims.
- 1.3** The CCTV system will not be used to:
- intrude on anyone's right to privacy
  - monitor people where they expect privacy, such as toilets, changing rooms and rooms used for intimate care
  - follow particular individuals, unless there is an emergency incident taking place
  - monitor how well staff do their jobs
  - pursue any purpose other than those in 1.2.
- 1.4** Footage, and any information taken from it, will never be used for commercial purposes.
- 1.5** If the police ask for footage to be released to the media, the Trust will agree only when the police have given written authority, and only to help investigate a specific crime.

## 2. Legislation and guidance

---

- 2.1** This policy follows the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, and the Human Rights Act 1998, which protects the right to respect for private life. It takes account of the Information Commission's guidance on video surveillance (March 2022). The Information Commission is still known as the ICO.
- 2.2** The Trust operates CCTV as part of its public task of running a safe school (UK GDPR Article 6(1)(e)). Its privacy notices tell people that CCTV is used. The Trust pays the data protection fee to the ICO.
- 2.3** The Surveillance Camera Code of Practice (2021) applies to the police and local authorities, not to academies. The Trust takes account of its principles as good practice.

### 3. Roles and responsibilities

---

- 3.1 Trust Board.** The Trust Board has overall responsibility for making sure the CCTV system is operated in line with this policy and the law.
- 3.2 Headteachers.** Each site Headteacher is responsible for the day-to-day leadership of the CCTV system at their site, and for making sure staff follow this policy. The co-headteachers decide together on any new or moved cameras, or upgrades to the system, after a data protection impact assessment (section 9) and advice from the DPO.
- 3.3 Academy Business Leader.** As the Trust's internal data protection contact, the Academy Business Leader handles requests for footage (section 8), keeps the disclosure log, makes sure the data protection impact assessment is completed and kept up to date, makes sure everyone with access is trained, and keeps this policy under review.
- 3.4 Data protection officer.** The Trust's data protection officer (DPO), The School DPO Service, advises on data protection impact assessments, requests for footage and disclosures, and monitors compliance. The DPO does not operate the system.
- 3.5 Facilities manager.** The facilities manager looks after the day-to-day operation, maintenance and security of the system at each site. This includes checking for faults, keeping the date and time stamps accurate, and exporting footage when authorised.

### 4. Location of the cameras and signs

---

- 4.1** Cameras are placed only where monitoring is needed to meet the aims in 1.2. At both sites, cameras cover the outside of the buildings, the grounds, and the entrances and gates. There are no cameras inside the buildings.
- 4.2** Cameras are not, and will not be, aimed off Trust grounds into public spaces or at other people's private property.
- 4.3** Signs are displayed wherever cameras are in use, so that people know before they enter the area. The signs say that the Trust operates the system and is the data controller, explain why CCTV is used, and give contact details.
- 4.4** Cameras are positioned to cover as much as possible, but there is no guarantee that every incident will be captured.

### 5. Operation of the system

---

- 5.1** The system operates 24 hours a day, every day of the year.
- 5.2** The system does not record audio.
- 5.3** Recordings carry date and time stamps. The system manager checks these each term and when the clocks change.
- 5.4** Footage should be of good enough quality to identify people, so that it can be used by the police or a court if needed.

## 6. Covert surveillance

---

- 6.1** Covert surveillance means recording people without telling them that they are being recorded. The Trust does not use covert surveillance. The Trust is not a body that can authorise covert surveillance under the Regulation of Investigatory Powers Act 2000. Where a crime is suspected, it is reported to the police.

## 7. Storage and retention of footage

---

- 7.1** Footage is kept for 30 days and is then overwritten automatically, as set out in the Records Retention Schedule (12.1.6).
- 7.2** Footage may be kept for longer only where it is needed for a specific matter: for example, an incident, a safeguarding concern or allegation, a complaint, a request for footage, a police investigation or a legal claim. The Designated Safeguarding Lead, a case manager or the Academy Business Leader may ask the system manager to save footage before it is overwritten. Saved footage is kept only for as long as that matter needs it, and is then securely deleted.
- 7.3** Saved footage is downloaded and encrypted, so that it is secure and its integrity is protected if it is needed as evidence. It is stored only in the Trust's approved systems.

## 8. Access to footage

---

- 8.1** Only authorised people may view footage, and only for the aims in 1.2 or another lawful reason. Everyone who views footage must record their name, the date and time, and the reason in the access log.
- 8.2** Monitors are positioned so that only authorised people can see them.
- 8.3** **Staff access.** The following may view footage: the site Headteacher for their site, the Director of Inclusion, the Academy Business Leader, and the system manager for maintenance and exporting. Anyone else may view footage only with the express permission of the site Headteacher, for a specific purpose.

Footage is viewed only on Trust devices or on the system's own monitors. Everyone with access is trained in using the system and in data protection. Misusing the system may be a criminal offence and will be dealt with under the Disciplinary Policy and Procedure.

- 8.4** **Requests for footage of yourself.** Anyone may ask for a copy of footage of themselves. This is a subject access request and is handled under section 9 of the Data Protection Policy. The Trust responds without undue delay and normally within one calendar month; school holidays do not extend this. A request for footage of a child is handled under section 9.2 of that policy. People asking should give the date, time and place, to help staff find the footage.

Footage often shows other people, including other pupils. Before disclosing it, the Trust will blur or otherwise obscure other people where it can, or ask for their consent. Where it can do neither, the DPO will advise whether all or part of the request can be met, or whether the person can be offered the chance to view the footage instead. A request may be refused in some circumstances, for example where disclosure would prejudice a police investigation.

Footage is disclosed securely, so that only the intended recipient can access it.

- 8.5 Requests from others.** Footage is shared with others only to meet the aims in 1.2, for example to help the police investigate a crime. Requests must be made in writing. They are decided by the site Headteacher and the Academy Business Leader, with advice from the DPO where needed. The Trust will comply with court orders, disclosing only the footage that is needed.
- 8.6** Every disclosure is recorded in the disclosure log kept by the Academy Business Leader. The log records the date, who received the footage and the organisation they represent, and why they needed it.

## 9. Data protection impact assessment

---

- 9.1** The Trust builds privacy into every stage of the CCTV system, including when it is replaced, extended or upgraded. A data protection impact assessment (DPIA) must be completed, with advice from the DPO, covering the system at both sites. It is reviewed when this policy is reviewed, and whenever cameras are added, moved, replaced or upgraded.
- 9.2** The DPIA checks that the system is still justified, necessary and proportionate. People most likely to be affected, including staff, parents and carers, and neighbours, are consulted where appropriate. Any risks found are dealt with as soon as possible.
- 9.3** Any change to how the system is used needs a new DPIA before it starts.

## 10. Security

---

- 10.1** The system manager oversees the security of the system and of footage. In particular:
- the system is checked for faults each term, and faults are reported and repaired as soon as possible
  - access to the system and to footage is password protected, and recording equipment is kept in a locked area
  - footage is stored securely and encrypted wherever possible
  - software and security updates from the manufacturer are applied as soon as possible
  - cyber security measures protect the system, in line with the Online Safety and Acceptable Use Policy.

## 11. Complaints

---

- 11.1** Complaints about how the Trust has handled personal data in CCTV footage are dealt with under section 19 of the Data Protection Policy. Other complaints about the CCTV system are dealt with under the Trust's Complaints Policy.

## 12. Monitoring and review

---

- 12.1** This policy is reviewed each year, with the Data Protection Policy. The review checks whether CCTV is still necessary, proportionate and effective in meeting the aims in 1.2.

**12.2** The Resources, Audit & Risk Committee approves this policy on behalf of the Trust Board.

## **13. Linked policies and documents**

---

**13.1** This policy should be read alongside:

- Data Protection Policy
- Records Retention Schedule
- Privacy notices
- Safeguarding and Child Protection Policy
- Allegations Against Staff and Low Level Concerns
- Disciplinary Policy and Procedure
- Complaints Policy
- CCTV data protection impact assessment