

CCTV Compliance Checklist

For the person responsible for a CCTV system. Work through it once, tick what is in place, and act on what is not.

Site / building:	Date completed:
Completed by:	Next review due:

1. Who is responsible

- ☐ We know who the data controller is: the person or organisation that decides why and how the CCTV is used
- ☐ The controller decided to have CCTV, and the reason is written down
- ☐ We know who sees the footage, and the list of people is kept short
- ☐ Someone is named to decide how long footage is kept
- ☐ Someone is named to answer requests for footage
- ☐ Managed or multi-let site: each operator knows which cameras and recordings are theirs *A managing agent can act on the controller's behalf, but the responsibility stays with the controller.*

2. ICO data protection fee

- ☐ We have paid the annual data protection fee to the Information Commissioner's Office (ICO), or we have recorded why we are exempt
- ☐ The renewal date is in the diary
- ☐ The fee tier is correct for the size of the organisation *Check the current figures on the ICO website.*

3. Lawful basis and impact assessment

- ☐ The lawful basis is recorded: legitimate interests for most private organisations, public task for most public bodies
- ☐ We can show the recording is necessary and proportionate
- ☐ A data protection impact assessment (DPIA) was done before installing or significantly changing the system
- ☐ Each camera has a job, and its view covers only what that job needs *Privacy masking helps where a view takes in private areas.*

4. Signage

- ☐ Signs are at every entrance to the recorded area, where people see them before they enter
- ☐ Each sign says who operates the system, why, and how to contact them
- ☐ Signs are legible, undamaged and updated when the operator or contact changes

5. Retention and security

- ☐ A retention period is set, written down and followed *There is no fixed legal period. Keep footage only as long as you need it.*
- ☐ The recorder overwrites or deletes footage when the period ends
- ☐ The recorder is in a locked or access-controlled location
- ☐ Every user has their own login, and default passwords have been changed
- ☐ Remote viewing is limited to people who need it
- ☐ Leavers are removed from the system promptly

6. Requests to see footage

- ☐ We can recognise a subject access request (SAR) when someone asks to see footage of themselves
- ☐ We know the response deadline is normally one month
- ☐ We can export footage in a usable form
- ☐ We can blur or otherwise protect other people in the footage *Check your system can do this before you need it.*
- ☐ Our search for footage is reasonable and proportionate, and we keep a note of what we searched
- ☐ Requests are logged, with the date received and the date answered

7. Complaints

- ☐ We have a written process for data protection complaints *A one-page procedure is enough for most CCTV operators.*
- ☐ Each complaint is acknowledged within 30 days, and the person is told the outcome

8. Review

- ☐ The system, signage and records are reviewed at least once a year
- ☐ The review is repeated whenever cameras are added, moved or removed, or the site changes hands

Anything left unticked is a gap to close. Most can be closed in an afternoon.

Security Adviser · securityadviser.co.uk · [\[Email\]](#)

This checklist gives practical guidance based on ICO publications. It is not legal advice. You stay in control of your compliance.