Surveillance, CCTV and Monitoring Policy

Sample policy template. This is a Verivius-authored template anchored to the statutory regulation and current CQC/professional guidance. Tenants must adapt the operational sections to their own organisation, service type, workforce, premises and professional requirements. Where this template and live law or regulator guidance diverge, the live source wins.

Statutory anchor: Regulation 10 (dignity and respect), Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (SI 2014/2936). This policy also engages Regulation 13 (safeguarding) and Regulation 17 (good governance). **Primary source:** https://www.legislation.gov.uk/uksi/2014/2936/regulation/10 **Non-CQC primary anchors:** Data Protection Act 2018, UK GDPR, ICO video surveillance guidance and CQC guidance on using surveillance. **Last reviewed:** 2026-06-10 **Verivius pack version:** v1, 2026-06-10

Policy owner: Registered Manager. Data protection owner: [DPO / IG lead / responsible person]. **Applies to:** CCTV, video monitoring, audio recording, call recording, vehicle cameras, doorbell cameras, body-worn cameras, remote monitoring, sensor monitoring and any surveillance or monitoring system used by or on behalf of the provider.

1. What the regulation says

> Service users must be treated with dignity and respect. (Reg 10(1): the headline duty)
>
> having due regard to any relevant protected characteristics (as defined in section 149(7) of the Equality Act 2010) of the service user. (Reg 10(2)(c): protected characteristics)
>
> The full text of the regulation is at https://www.legislation.gov.uk/uksi/2014/2936/regulation/10. Where this policy and the regulation diverge, the regulation wins.

2. Plain-English summary

Service users must be treated with dignity and respect. In particular, you have to protect their privacy, support their autonomy, independence and involvement in the community, and have due regard to any relevant protected characteristics under the Equality Act 2010. Surveillance, CCTV and monitoring can support safety, security and incident review, but they also interfere with privacy, dignity, autonomy and trust, so they must be used only where they are lawful,

necessary, proportionate, transparent and properly governed under the Data Protection Act 2018, UK GDPR and ICO and CQC surveillance guidance.

3. Purpose

The purpose of this policy is to make sure that [Service Name] only uses surveillance, CCTV or monitoring systems where they are lawful, necessary, proportionate, transparent and properly governed.

Surveillance can support safety, security and incident review, but it can also interfere with privacy, dignity, autonomy and trust. It must not be used casually or as a substitute for safe staffing, supervision, care planning or good management.

4. Policy warning

The service must not install or use CCTV, audio recording, covert monitoring, vehicle cameras, body-worn cameras, remote monitoring or other surveillance without a documented lawful basis, risk assessment and governance approval.

Surveillance must not be used in bedrooms, bathrooms, treatment areas, changing areas, personal-care areas or other private spaces unless there is an exceptional, lawful, necessary and proportionate reason, supported by specialist advice.

Covert surveillance is high risk and must not be used without senior approval and legal/data protection advice.

5. Scope

This policy applies to:

- fixed CCTV
- temporary CCTV
- vehicle cameras
- dashcams
- patient transport cameras
- body-worn video
- doorbell cameras
- audio recording
- call recording
- remote monitoring
- movement sensors
- falls sensors

- environmental monitoring
- monitoring used in care homes, clinics, vehicles, offices, reception areas or shared spaces
- contractor-managed surveillance systems
- surveillance footage used for incidents, complaints, safeguarding, employment or police matters

6. Principles

The service will ensure surveillance is:

- lawful
- fair
- transparent
- necessary
- proportionate
- limited to a clear purpose
- subject to data protection assessment
- clearly signed where overt
- secure
- access controlled
- retained only as long as necessary
- reviewed regularly
- removed where no longer justified

7. Responsibilities

The provider is responsible for approving surveillance systems and ensuring compliance.

The Registered Manager is responsible for ensuring surveillance does not compromise dignity, safety, safeguarding, confidentiality or care quality.

The Data Protection Officer or information governance lead is responsible for advising on lawful basis, transparency, DPIA, access controls, retention and data subject rights.

Managers are responsible for local use, signage, incident access and audit.

Staff must not view, copy, share, record or disclose surveillance material unless authorised.

8. Lawful basis and purpose

Before any system is used, the provider must document:

- purpose
- problem being addressed
- lawful basis
- whether special category data may be captured
- people affected
- areas covered
- alternatives considered
- why surveillance is necessary
- why less intrusive options are insufficient
- expected benefit
- risks to people's rights and freedoms
- retention period
- access controls
- review date

Possible purposes may include safety, security, crime prevention, incident review or protection of people at risk, but the purpose must be specific.

9. Data Protection Impact Assessment

A Data Protection Impact Assessment must be completed where surveillance is likely to create high risk to people's rights and freedoms.

The DPIA should consider:

- nature of the monitoring
- scale
- location
- whether people expect privacy
- vulnerable people
- children
- staff impact
- audio capture
- continuous monitoring
- remote access
- facial recognition or analytics
- vehicle monitoring

- safeguards
- consultation
- residual risk

High-risk surveillance must not start until the DPIA has been reviewed and approved.

10. Transparency and signage

People must be told about surveillance unless there is a lawful reason not to do so.

The service must provide:

- clear signage
- privacy notice information
- purpose of recording
- data controller identity
- contact details
- retention period or where to find it
- how to request access
- how to complain

Signage must be visible before people enter monitored areas where practicable.

11. Areas where surveillance is prohibited or exceptional

Surveillance must not normally be used in:

- bedrooms
- bathrooms
- toilets
- changing areas
- treatment rooms during intimate care or examination
- counselling or sensitive consultation areas
- staff changing areas
- areas where people reasonably expect high privacy

Any exception must be individually justified, time-limited, documented, risk assessed and supported by specialist advice.

12. Audio recording

Audio recording is more intrusive than video-only monitoring and must be separately justified.

The service must not enable audio recording unless:

- the purpose cannot be met by less intrusive means
- people are clearly informed
- lawful basis is recorded
- privacy impact is assessed
- retention and access are tightly controlled
- staff are trained

Call recording must be clearly explained to callers and managed under the information governance policy.

13. Covert surveillance

Covert surveillance is not routine governance.

It may only be considered where there is a serious concern, a clear lawful basis, no less intrusive way to investigate, senior approval and specialist advice.

Before covert surveillance is used, the provider must document:

- serious concern being investigated
- alternatives considered
- legal advice
- data protection advice
- authorisation
- scope
- duration
- areas covered
- access controls
- review date
- how recordings will be handled
- when surveillance will stop

Covert surveillance must never be used for general staff performance monitoring or convenience.

14. Staff monitoring

Where surveillance may monitor staff, the provider must be transparent and fair.

Staff must be told:

- what is monitored
- why
- when monitoring happens
- who can access recordings
- whether recordings may be used for investigation
- retention period
- rights and complaint route

Surveillance must not be used to replace supervision, management, staffing review or disciplinary processes.

15. Access to recordings

Access must be restricted to authorised people.

The access log must record:

- date
- person accessing
- reason
- footage reviewed
- whether copied or exported
- recipient
- outcome
- deletion or retention decision

Staff must not download, photograph, copy, share or send footage using personal devices or unauthorised systems.

16. Disclosure to police, safeguarding or regulators

Recordings may be shared where there is a lawful basis.

Potential recipients include:

- police
- safeguarding authority
- CQC

- coroner
- insurer or legal adviser
- professional regulator
- employment investigator

The decision must be recorded, including what was shared, why, with whom and under what lawful basis.

17. Retention and deletion

Recordings must be kept only as long as necessary.

The provider must set and document retention periods for each system.

Longer retention may be justified where footage is linked to:

- incident
- complaint
- safeguarding concern
- police matter
- legal claim
- employment investigation
- regulatory concern

Footage not needed must be deleted securely.

18. Subject access requests

People may request access to their personal data captured by surveillance.

The service must handle requests under the Subject Access Request process.

Before disclosure, the service must consider:

- identity verification
- third-party data
- safeguarding risk
- confidentiality
- exemptions
- redaction or blurring
- secure transfer
- response timeframe

Requests must be escalated to the information governance lead.

19. Surveillance in vehicles

Vehicle cameras or dashcams must be assessed separately.

The assessment must consider:

- road safety purpose
- whether passengers are recorded
- whether audio is captured
- signage or privacy information
- driver monitoring
- location tracking
- access controls
- retention
- safeguarding
- incident use

Patient transport services must consider dignity, confidentiality and safeguarding.

20. Remote monitoring and sensors

Remote monitoring, falls sensors or environmental sensors must be used only where lawful, necessary and proportionate.

The record must show:

- purpose
- consent or lawful basis
- capacity assessment where needed
- best-interests decision where needed
- risk addressed
- alerts generated
- who responds
- review date
- impact on privacy and autonomy

Remote monitoring must not become an unjustified restriction or substitute for safe care.

Where surveillance or remote monitoring touches a person who may lack capacity to consent to it, follow the Mental Capacity Act best-interests process. Any question of whether the monitoring amounts to a deprivation of liberty is a separate legal matter; take specialist advice rather than treating it as decided by this policy.

21. Incidents and breaches

The following must be reported:

- unauthorised viewing
- unauthorised disclosure
- lost footage
- footage sent to wrong recipient
- camera covering inappropriate area
- audio enabled without approval
- surveillance used outside approved purpose
- failure to delete footage
- missing signage
- system access by former staff
- surveillance-related complaint

The Data Breach Policy and Incident Reporting Policy must be followed.

22. Audit

The Registered Manager and information governance lead must audit surveillance at least annually.

The audit must check:

- current DPIA
- lawful basis
- signage
- camera locations
- access logs
- retention
- deletion
- disclosures
- staff training

- complaints
- incidents
- continued necessity
- whether a less intrusive option is now available

Systems must be removed or changed where they are no longer justified.

23. Review

This policy will be reviewed annually, or sooner following a surveillance incident, data breach, complaint, safeguarding concern, system change, new technology, ICO guidance update, legal change or CQC finding.

24. Sources and further reading

This template is based on CQC's guidance for providers and managers, the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, and other topic-specific legislation and guidance listed below. It is a starting point for adaptation, not a substitute for legal, clinical, HR, safeguarding or specialist professional advice.

- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, Regulation 10 (https://www.legislation.gov.uk/uksi/2014/2936/regulation/10)
- CQC Regulation 10: Dignity and respect
- CQC Regulation 13: Safeguarding
- CQC Regulation 17: Good governance
- CQC guidance on using surveillance
- Data Protection Act 2018 (https://www.legislation.gov.uk/ukpga/2018/12)
- UK GDPR
- ICO video surveillance guidance, including CCTV
- ICO CCTV self-assessment checklist
- Note: ICO surveillance guidance is under review following the Data (Use and Access) Act 2025; providers must check the live ICO source before adopting.
- Human Rights Act 1998, especially Article 8 (https://www.legislation.gov.uk/ukpga/1998/42)
- Equality Act 2010 (https://www.legislation.gov.uk/ukpga/2010/15)
- CQC Regulation 12: Safe care and treatment
- Mental Capacity Act 2005 where monitoring affects a person who may lack capacity (https://www.legislation.gov.uk/ukpga/2005/9)
- Safeguarding procedures where monitoring is used to investigate or manage risk

25. When to seek further advice

Seek specialist advice where the issue involves serious harm, safeguarding, deprivation of liberty, restraint, children, professional misconduct, controlled drugs, radiation, termination of pregnancy, infection outbreak, water safety, employment dismissal, DBS barring referral, or regulatory enforcement. In particular, seek specialist advice before using covert surveillance, audio recording, bedroom or private-area monitoring, facial recognition, continuous monitoring, staff disciplinary surveillance, monitoring of children, monitoring of people who may lack capacity, or sharing footage with external bodies.

26. Document control

Version	Date	Author	Changes
v1	2026-06-10	Verivius (sample)	Conformed new cross-cutting draft to the Verivius policy standard.

This sample policy template was issued by Verivius. It is a template, not a substitute for legal advice or the tenant's own policy-development process. Where this template and live law or regulator guidance diverge, the live source wins.
