CCTV POLICY

Necessary surveillance, privacy, secure access and accountable use

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027 | IMPACT AP

1 | SCOPE AND DEPLOYMENT STATUS

Applies to any CCTV controlled by Impact, including live viewing, recording and access through a contractor. This policy does not confirm that a camera is installed or recording at either site. Kate Willis and Kirsty Lampkin must maintain a current system register identifying cameras, controller, purpose, field of view, recording settings, storage and authorised users before operation.

2 | PURPOSE AND LAWFUL BASIS

Document a specific security or safeguarding purpose and why less intrusive controls are insufficient. Establish and record a lawful basis appropriate to Impact's AP status, including a legitimate-interests assessment where used. Do not assume public-task powers or use parental consent as blanket permission for surveillance. Complete a data protection impact assessment where required and consult appropriate advice.

3 | LOCATION AND PRIVACY

Restrict coverage to areas necessary for the stated purpose. Do not record toilets, changing areas, spaces used for intimate care or other private activity. Avoid unnecessary views of neighbouring property, public areas or confidential meetings. No covert monitoring, facial recognition, biometric analytics or audio recording is authorised by this policy. Any proposed exceptional monitoring requires separate legal and privacy assessment.

4 | TRANSPARENCY

Place clear signs before people enter monitored areas, naming the controller, purpose and contact route. Provide an accessible privacy notice explaining use, retention, sharing and rights. Explain arrangements to learners and staff. Do not describe cameras as recording when they are inactive, or imply that surveillance replaces staff supervision and safeguarding practice.

5 | ACCESS AND SECURITY

Allow access only to named, trained users for a documented purpose. Protect equipment, accounts and remote access with appropriate security, updates and access controls. Keep an access/export log. No personal-phone recording of screens, informal sharing or use of footage for entertainment. Contractors must have suitable written data-processing and security arrangements.

6 | RETENTION AND PRESERVATION

Set the shortest justified retention period in the system register before recording starts; there is no universal statutory retention period. Configure deletion accordingly and test it. Preserve only relevant footage when an incident, request or lawful hold requires it, recording the reason and review date. Do not retain whole archives merely because capacity permits.

CCTV POLICY

Necessary surveillance, privacy, secure access and accountable use

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027 | IMPACT AP

7 | INCIDENTS AND LAWFUL DISCLOSURE

Report safeguarding footage through the DSL or independent adult-conduct route. Preserve original material securely and record who handled it. Verify and document requests from police, commissioners or other agencies before necessary lawful disclosure. Redact unrelated personal information where appropriate. Inform the DPO promptly about loss, unauthorised viewing or insecure sharing.

8 | REQUESTS AND RIGHTS

Send requests to see footage or exercise data rights promptly to Kirsty Lampkin. Identify relevant dates and footage quickly to prevent routine deletion. Verify identity, consider others' rights and respond within the applicable legal timescale, normally one month, explaining any lawful extension or restriction. Do not promise unrestricted copies or refuse a request simply because it includes other people.

9 | STAFF AND LEARNER PROTECTIONS

CCTV must not become routine hidden performance monitoring or a substitute for fair investigation. Do not make automatic judgements from a short clip without context. Provide a fair opportunity to respond through the relevant procedure. Respect learner communication needs and the risk that footage reveals sensitive health, family or safeguarding information.

10 | ASSURANCE AND COMPLAINTS

Review camera need, coverage, retention, permissions and security at least annually and after changes or incidents. Record faults, corrective actions and deletion checks. Use Complaints for service concerns and the data-protection route for information handling; explain the right to complain to the ICO. Pause processing that lacks a defensible purpose or necessary safeguards.

11 | POLICY CONTROL AND REVIEW

Policy owner: Kate Willis, Principal and Proprietor. Effective date: September 2026. Scheduled review: September 2027, or sooner after relevant changes, incidents or feedback. Record actual governance approval and implementation decisions and brief staff on their duties. These policy dates do not assert that approval, staff training or operational checks have already occurred. Use the Complaints or independent reporting route for concerns about implementation.

12 | SOURCES AND RELATED DOCUMENTS

ICO: CCTV and video surveillance guidance; UK GDPR and Data Protection Act 2018 as amended.

ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/

Check current versions and apply according to Impact's legal and commissioning status.