

IMPACT ALTERNATIVE LEARNING CCTV POLICY – ELITE MASTER VERSION

Principal: Kate Willis

Deputy DSL: Kirsty Lampkin

Reviewed: November 2025 | Review Date: November 2026

1. STATEMENT OF INTENT

Impact Alternative Learning operates a CCTV system to safeguard learners, staff and visitors. The system is designed to deter unsafe behaviour, support safeguarding investigations and provide evidence where required. All use of CCTV is lawful, proportionate and necessary. The system is not used to intrude unnecessarily into private life and is operated transparently with clear signage.

2. LEGAL FRAMEWORK

This policy complies with: • Data Protection Act 2018 • UK GDPR • Human Rights Act 1998 • Protection of Freedoms Act 2012 • Freedom of Information Act 2000 • Keeping Children Safe in Education 2025 It also reflects ICO CCTV Code of Practice guidance.

3. DEFINITIONS

Surveillance: Monitoring behaviour via recording equipment. Overt: Visible CCTV with signage. Covert: Only used in exceptional safeguarding cases with formal approval.

4. ROLES AND RESPONSIBILITIES

Principal: Overall responsibility for CCTV operation. Data Controller: • Manages access and storage • Handles Subject Access Requests • Ensures compliance Staff: • Must not misuse CCTV • Report incidents appropriately Governance: • Monitor effectiveness and compliance

5. PURPOSE AND JUSTIFICATION

CCTV is used to: • Safeguard learners and staff • Deter and detect crime • Support behaviour investigations • Provide evidence to agencies Cameras are never placed in toilets, changing areas or private spaces.

6. DATA PROTECTION PRINCIPLES

Footage is: • Lawfully processed • Used only for intended purposes • Stored securely • Retained only as long as required • Protected against unauthorised access

7. USE OF CCTV SYSTEM

CCTV is used for safeguarding, behaviour monitoring and incident investigation. It is not used for routine staff performance monitoring.

8. SYSTEM OVERVIEW

• Cameras installed in key safety areas • Visible signage across site • Secure login access • Continuous recording with deletion cycle (typically 30 days)

9. PROTOCOLS

System is registered with ICO. Clear signage is displayed. System designed to minimise intrusion. May include approved platforms such as security apps or portals.

10. SECURITY

- Restricted authorised access only
- Password protected systems
- Annual system checks
- Faults addressed immediately

11. CCTV CODE OF PRACTICE

The system operates transparently and fairly. Individuals are informed of CCTV presence. Use is proportionate and justified.

12. ACCESS TO DATA

Individuals may request access via SAR. Requests verified and responded to within one month. Access may be refused if it compromises safeguarding or is excessive.

13. THIRD PARTY ACCESS

Footage may be shared with: • Police • Courts • Social care All disclosures are logged and justified.

14. MEDIA DISCLOSURE

Images released only where necessary. Other individuals anonymised where possible.

15. DATA SUBJECT ACCESS

Individuals can request footage of themselves. Identity verification required. Requests processed in line with GDPR.

16. MONITORING AND REVIEW

Policy reviewed annually. System audited regularly for compliance.

17. COMPLAINTS

Complaints should be directed to the Principal. Escalation available to ICO if unresolved.

APPENDICES

Appendix 1 – CCTV Access Request Form

Name: Address: Date/Time: Location: Reason:

Appendix 2 – CCTV Usage Log

Date	Time	Staff	Reason	Outcome

Appendix 3 – Incident Review Form

Incident: Action: Outcome: Review: