



CCTV

Reviewed by: IT Manager

Reviewed: July 2025

Contents

1.0 Policy Statement and Purpose	2
2.0 Legal Framework	2
3.0 Scope of Policy.....	3
4.0 Principles of CCTV Operation	4
5.0 Camera Locations and Coverage	5
6.0 System Management and Technical Specifications	5
7.0 Data Protection and Privacy	6
8.0 System Access Control	7
9.0 Subject Access Requests	9
10.0 Monitoring and Recording.....	10
11.0 Incident Management	10
12.0 Training and Awareness	11
13.0 Review and Compliance	12
14.0 Contact Information.....	13
Appendix A: CCTV Access Request Form	14
Appendix B: Incident Investigation Checklist	14
Appendix C: Camera Location Register Template	14
Appendix D: Privacy Notice Template	14
Appendix E: Data Protection Impact Assessment Summary	14

1.0 Policy Statement and Purpose

1.1 Katharine Lady Berkeley's School is committed to providing a safe and secure environment for pupils, staff, and visitors whilst respecting individual privacy rights and complying with all relevant UK legislation.

1.2 This policy establishes the framework for the lawful, proportionate, and transparent use of Closed Circuit Television (CCTV) systems operated by Verkada. The primary purposes are:

1.2.1 Safety and Security: Protecting pupils, staff, and visitors from harm

1.2.2 Crime Prevention: Deterring criminal activity and antisocial behaviour

1.2.3 Property Protection: Safeguarding school premises and assets

1.2.4 Investigation Support: Providing evidence for incident investigation

1.2.5 Regulatory Compliance: Meeting health and safety obligations

1.3 Scope

1.3.1 This policy applies to all CCTV systems operated by the school, including fixed cameras, mobile devices, and any associated recording equipment provided by Verkada.

2.0 Legal Framework

2.1 This policy complies with the following UK legislation:

2.1.1 UK General Data Protection Regulation (UK GDPR) - governs the processing of personal data

2.1.2 Data Protection Act 2018 - provides the UK framework for data protection

2.1.3 Human Rights Act 1998 - protects the right to privacy under Article 8

2.1.4 Protection of Freedoms Act 2012 - establishes the Surveillance Camera Code of Practice

2.1.5 Children Act 1989/2004 - safeguarding obligations for children

2.1.6 Education Act 2002 - duty of care in educational settings

2.2 Regulatory Guidance

2.2.1 Information Commissioner's Office (ICO) guidance on video surveillance (under review due to Data (Use and Access) Act coming into law on 19 June 2025)

2.2.2 Department for Education safeguarding guidance

2.2.3 Home Office Surveillance Camera Code of Practice

2.3 Lawful Basis for Processing

2.3.1 Under Article 6 of UK GDPR, our lawful basis for processing personal data through CCTV is:

2.3.1.1 Legitimate Interests (Article 6(1)(f)) - for crime prevention, security, and property protection

2.3.1.2 Public Task (Article 6(1)(e)) - fulfilling our statutory duties as an educational institution

2.3.1.3 Legal Obligation (Article 6(1)(c)) - meeting health and safety requirements

3.0 Scope of Policy

3.1 Coverage Areas

3.1.1 External perimeters and entrances

3.1.2 Internal corridors and common areas

3.1.3 Reception areas

3.1.4 Car parks and external grounds

3.1.5 Specialist rooms (science labs, workshops) where justified

3.2 Excluded Areas

3.2.1 Toilets and changing rooms

3.2.2 Private offices (unless specifically justified)

3.2.3 Medical rooms

3.2.4 Counselling rooms

3.2.5 Staff rooms (unless specifically justified and consulted upon)

3.3 System Specifications

3.3.1 The school operates a Verkada cloud-based CCTV system with the following features:

- 3.3.1.1 High-definition digital recording
- 3.3.1.2 Remote access capabilities
- 3.3.1.3 Automated retention management
- 3.3.1.4 Audit trail functionality
- 3.3.1.5 Encrypted data transmission and storage

4.0 Principles of CCTV Operation

4.1 All CCTV usage must be proportionate, necessary, and justified, adhering to:

- 4.1.1 Necessity: CCTV is only used where there is a clear need that cannot be met through less intrusive means
- 4.1.2 Proportionality: The level of surveillance is appropriate to the identified risk or need
- 4.1.3 Transparency: Clear signage and information about CCTV usage is provided
- 4.1.4 Data Minimisation: Only the minimum amount of data necessary is collected and retained
- 4.1.5 Purpose Limitation: Data is only used for the specific purposes identified in this policy
- 4.1.6 Accountability: Clear responsibilities and procedures are established for system management

4.2 Decision-Making Framework

- 4.2.1 Before installing new cameras, the school will conduct a Data Protection Impact Assessment (DPIA) considering:
 - 4.2.2 Specific security risks or needs
 - 4.2.3 Alternative less intrusive solutions
 - 4.2.4 Impact on privacy rights
 - 4.2.5 Stakeholder consultation requirements
 - 4.2.6 Technical and organisational safeguards

5.0 Camera Locations and Coverage

5.1 A comprehensive register of all camera locations is maintained, including:

- 5.1.1 Camera identification number
- 5.1.2 Precise location description
- 5.1.3 Justification for placement
- 5.1.4 Field of view description
- 5.1.5 Privacy impact assessment outcome

5.2 Clear, visible signage is displayed at all monitored areas, including:

- 5.2.1 Notice that CCTV is in operation
- 5.2.2 Purpose of surveillance
- 5.2.3 Data controller contact details

5.3 Regular Review

- 5.3.1 Camera locations are reviewed annually to ensure continued necessity and proportionality.

6.0 System Management and Technical Specifications

6.1 The school's Verkada system provides:

- 6.1.1 Cloud-based storage with UK data residency
- 6.1.2 End-to-end encryption
- 6.1.3 Multi-factor authentication
- 6.1.4 Comprehensive audit logging
- 6.1.5 Automated compliance features
- 6.1.6 Mobile and web-based access

6.2 Technical Safeguards

- 6.2.1 All data transmission is encrypted
- 6.2.2 Access requires strong authentication
- 6.2.3 System maintains comprehensive audit trails
- 6.2.4 Regular security updates are applied
- 6.2.5 Data is stored in UK-based servers

6.3 Data Retention

6.3.1 CCTV footage is retained for a maximum of 365 days, after which it is automatically deleted unless:

6.3.1.1 Required for ongoing investigation

6.3.1.2 Subject to legal proceedings

6.3.1.3 Requested under Subject Access Rights (processed separately)

7.0 Data Protection and Privacy

7.1 A comprehensive Privacy Impact Assessment has been conducted, considering:

7.1.1 Data flows and processing activities

7.1.2 Privacy risks to individuals

7.1.3 Mitigation measures

7.1.4 Stakeholder consultation outcomes

7.1.5 Ongoing monitoring requirements

7.2 Data Subject Rights

7.2.1 Under data protection laws, individuals have rights regarding CCTV footage, including:

7.2.1.1 Right of access to personal data

7.2.1.2 Right to rectification

7.2.1.3 Right to erasure (in certain circumstances)

7.2.1.4 Right to restrict processing

7.2.1.5 Right to object to processing

7.3 Privacy Notice

7.3.1 A comprehensive privacy notice is published, detailing:

7.3.2 What data is collected

7.3.3 Legal basis for processing

7.3.4 How long data is retained

7.3.5 Who has access to data

7.3.6 How to exercise data subject rights

7.3.7 How to make complaints

8.0 System Access Control

8.1 System Access Levels

Access Level	Personnel	Permitted Activities	Circumstances	Authorization Required
Level 1 - Full Administrative	IT Manager IT Technicians	• Live monitoring • Footage review • System configuration • User management • Export footage • Delete footage	• Routine monitoring • Incident investigation • System maintenance • Policy compliance	Self-authorized for routine use
Level 2 - Operational	Designated Safeguarding Lead Senior Leadership Team Site Manager	• Live monitoring • Footage review • Export footage for investigations	• Safeguarding concerns • Security incidents • Health & safety investigations • Emergency situations	Self-authorized for routine use
Level 3 - Limited Monitoring	Reception Staff Security Personnel HOY/Pastoral Assistants	• Live monitoring only • Incident reporting • No recording access	• During designated hours • Emergency situations • Visitor management	Authorized as part of role Cannot access recordings
Level 4 - Emergency Access	Police Officers Other Emergency Services	• Footage viewing/export • Investigation support	• Criminal investigations • Safeguarding emergencies • Court orders/warrants	Legal requirement or court order Headteacher notification required
Level 5 - External Agencies	Social Services Local Authority Officers Ofsted Inspectors	• Specific footage access • Limited to relevant incidents	• Safeguarding investigations • Regulatory inspections • Legal proceedings	Formal request with legal basis Senior Leadership approval Data sharing agreement

8.2 Access Authorization Groups

Requestor Type	Purpose	Approval Required	Documentation Needed	Response Time
Internal Staff	Incident investigation	Line manager + Headteacher	Incident report form	24 hours
Internal Staff	Safeguarding concern	Designated Safeguarding Lead	Safeguarding concern form	Immediate
Police	Criminal investigation	None (legal obligation)	Formal request/warrant	Immediate
Social Services	Child protection	Headteacher approval	Formal written request	48 hours
Parents/Pupils	Subject Access Request	Data Protection Officer	Completed SAR form + ID	30 days
Insurance Companies	Claim investigation	Headteacher approval	Formal written request	5 working days
Legal Representatives	Court proceedings	Headteacher + Legal advice	Court order/legal request	As required by court

8.3 Access Logging and Monitoring

8.3.1 All system access is automatically logged, recording:

- 8.3.1.1 User identity and authentication method
- 8.3.1.2 Date and time of access
- 8.3.1.3 Duration of access
- 8.3.1.4 Actions performed (view, export, delete, etc.)
- 8.3.1.5 Cameras accessed
- 8.3.1.6 Any footage exported

8.4 Regular Access Reviews

- 8.4.1 Monthly review of access logs by IT Manager
- 8.4.2 Quarterly review of user permissions by Headteacher with IT Manager
- 8.4.3 Annual comprehensive access audit by Headteacher with IT Manager
- 8.4.4 Immediate review following any security incident by Headteacher with IT Manager

9.0 Subject Access Requests

9.1 Individuals have the right to request access to CCTV footage containing their personal data, usually provided free of charge within 1 calendar month.

9.2 Request Process

- 9.2.1 Initial Contact: Requests must be made in writing to the Data Protection Officer
- 9.2.2 Identity Verification: Requestor must provide acceptable proof of identity
- 9.2.3 Request Assessment: Determine if the request is valid and footage exists
- 9.2.4 Third Party Considerations: Assess if footage contains other individuals' data
- 9.2.5 Preparation: Edit footage if necessary to protect third-party privacy
- 9.2.6 Response: Provide footage with explanatory information

9.3 Response Timeframes

- 9.3.1 Acknowledgment: Within 3 working days of receipt
- 9.3.2 Full Response: Within 1 calendar month of receipt
- 9.3.3 Complex Cases: May be extended by 2 months with explanation

9.4 Exemptions and Restrictions

9.4.1 Requests may be refused or restricted if:

- 9.4.1.1 Footage would reveal third-party personal data
- 9.4.1.2 Disclosure would prejudice crime prevention/detection
- 9.4.1.3 Footage relates to ongoing legal proceedings
- 9.4.1.4 Request is manifestly unfounded or excessive

10.0 Monitoring and Recording

10.1 Live Monitoring

- 10.1.1 Live monitoring is conducted only when staff are present
- 10.1.2 Monitoring staff receive appropriate training
- 10.1.3 Clear procedures exist for responding to incidents observed
- 10.1.4 Privacy expectations are respected during monitoring

10.2 Recording Parameters

- 10.2.1 Continuous recording during school operational hours
- 10.2.2 Motion-activated recording outside operational hours
- 10.2.3 High-definition quality sufficient for identification purposes
- 10.2.4 Audio recording only where specifically justified and clearly signposted

10.3 Storage and Backup

- 10.3.1 Primary storage on Verkada cloud platform
- 10.3.2 Automatic backup systems in place
- 10.3.3 Encrypted transmission and storage
- 10.3.4 UK-based data residency
- 10.3.5 Automated retention period enforcement

11.0 Incident Management

11.1 Incident Response Procedures

- 11.1.1 When CCTV footage is required for incident investigation:
- 11.1.2 Immediate Actions:
 - 11.1.2.1 Secure relevant footage immediately

11.1.2.2 Log the incident in the CCTV incident register

11.1.2.3 Notify appropriate personnel

11.1.3 Investigation Process:

11.1.3.1 Determine if footage exists and is relevant

11.1.3.2 Assess who needs access to footage

11.1.3.3 Ensure appropriate authorization is obtained

11.1.3.4 Maintain chain of custody for evidence

11.1.4 Documentation:

11.1.4.1 Record all access to footage

11.1.4.2 Document decisions and actions taken

11.1.4.3 Maintain incident investigation file

11.1.4.4 Ensure compliance with retention requirements

11.2 External Agency Cooperation

11.2.1 Full cooperation with police investigations

11.2.2 Formal processes for social services requests

11.2.3 Clear protocols for emergency service access

11.2.4 Legal advice sought for complex situations

11.3 Evidence Handling

11.3.1 Chain of custody maintained for all exported footage

11.3.2 Digital integrity verification procedures

11.3.3 Secure storage of evidence copies

11.3.4 Court-ready presentation formats

12.0 Training and Awareness

12.1 Staff Training Requirements

12.1.1 All staff with CCTV system access must complete training covering:

12.1.2 Data protection principles and requirements

12.1.3 System operation and technical procedures

12.1.4 Privacy rights and responsibilities

12.1.5 Incident response procedures

12.1.6 Professional boundaries and ethics

12.2 Ongoing Training Programme

12.2.1 Annual refresher training for all users

12.2.2 New user induction training

12.2.3 Update training when systems change

12.2.4 Specialized training for different access levels

12.3 Awareness for School Community

12.3.1 Privacy notices displayed prominently

12.3.2 Information in school handbook and website

12.3.3 Parent/pupil awareness sessions

12.3.4 Regular communication about CCTV purposes

13.0 Review and Compliance

13.1 Policy Review Schedule

13.1.1 Annual comprehensive policy review

13.1.2 Bi-annual operational procedures review

13.1.3 Immediate review following significant incidents

13.1.4 Review following legislative changes

13.2 Compliance Monitoring

13.2.1 Monthly technical system checks

13.2.2 Quarterly access and usage audits

13.2.3 Annual Data Protection Impact Assessment review

13.2.4 Regular consultation with stakeholders

13.3 Performance Metrics

13.3.1 Response times to access requests

13.3.2 System uptime and reliability

13.3.3 Incident investigation effectiveness

13.3.4 Compliance with retention periods

13.3.5 Training completion rates

14.0 Contact Information

14.1 Data Protection Officer:	Richie Jackman,	rjackman@klbschool.org.uk
14.2 IT Manager:	Steve Miles,	smiles@klbschool.org.uk
14.3 Headteacher:	Hannah Khan,	hkhan@klbschool.org.uk
14.4 Verkada Support:	+442030 486 050	support@verkada.com
14.5 ICO:	0303 123 1113,	casework@ico.org.uk

This policy complies with UK GDPR, Data Protection Act 2018, and all relevant UK legislation as of September 2025. Regular updates ensure continued compliance with evolving legal requirements.

Appendix A: CCTV Access Request Form

[To be completed with specific form details]

Appendix B: Incident Investigation Checklist

[To be completed with specific checklist items]

Appendix C: Camera Location Register Template

[To be completed with register format]

Appendix D: Privacy Notice Template

[To be completed with privacy notice details]

Appendix E: Data Protection Impact Assessment Summary

[To be completed with DPIA details]

KLB



Katharine Lady Berkeley's School
Wotton-under-Edge, Gloucester, GL12 8LX

Tel: 01453 842227

Mail: info@klbschool.org.uk

www.klbschool.org.uk