CCTV Policy

Policy Code:	ICT1
Policy Start Date:	September 2026
Policy Review Date:	September 2029

Please read this policy in conjunction with the policies listed below:

- HR5 Acceptable Use Policy
- HR6 Data Protection Policy
- HR6A Data Breach Policy
- HR12 Staff Disciplinary Policy
- HR16 DBS Policy
- HR23 Whistleblowing Policy
- HR24 Allegations of Abuse Made Against Adults Policy
- HR33 Records Management Policy
- HR42 Low-Level Concerns Policy
- SW5 Safeguarding and Child Protection Policy
- SW17 Safeguarding Adults Policy
- CCTV Code of Practice – Information Commissioner's Office

1 Policy Statement

1.1 The purpose of this policy is to regulate and provide guidance for the management, operation and use of the closed-circuit television (CCTV) system at The Priory Federation of Academies' sites.

1.2 References to the Trust or Academy within this policy specifically include all nursery, primary, secondary and special academies within the Trust, as well as Priory Apprenticeships and Lincolnshire ITT.

1.3 This policy does not form part of any member of staff's contract of employment and it may be amended at any time.

2 Roles, Responsibilities and Implementation

2.1 The People, Performance and Operations Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. This committee delegates day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Director of Trust Services.

2.2 This policy is approved by the People, Performance and Operations Committee before being ratified at the next available Trust Board meeting. Approval and ratification is minuted, with records kept by the Clerk to Trustees.

2.2 Leaders and Managers have a specific responsibility to ensure the fair application of this policy and all employees are responsible for supporting colleagues and ensuring its success.

2.3 This document follows Data Protection Act 2018 guidelines. A review of this document will be conducted in the event of significant changes to the CCTV system or legislation. The CCTV system is owned by the Trust. Whilst some external elements of it are maintained by external contractors, only Trust staff have access to footage.

3 Aims

3.1 To set out the purpose for the use of CCTV by the Trust.

3.2 To ensure clarity on how CCTV is managed by the Trust, who can access it, how it will be shared if required and who is responsible for the use of it.

3.3 To increase personal safety of all school/site users, protect the Trust's buildings/ground and assets and reduce the fear of crime.

4 Statement of Intent

4.1 The CCTV system is used following Information Commissioner Guidance under the terms of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2018 and will comply with the requirements both of the Data Protection Act 2018 and the Commissioner's Code of Practice. The Trust will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

4.2 The purpose of CCTV cameras will be to monitor activities within the settings and their grounds in order to:

- identify criminal activity actually occurring, anticipated, or perceived; and
- secure the safety and wellbeing of all Trust users and visitors.

4.3 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Material will not be released to the media and will only be released to the police for the purpose of identification, detection or prevention of crime.

4.4 The planning and design of CCTV systems has endeavoured to ensure that the systems will give maximum effectiveness and efficiency but it is not possible to guarantee that the systems will cover or detect every single incident taking place in the areas of coverage. Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at entry points to the settings and additional strategic locations within the grounds.

4.5 CCTV cameras will be positioned to maintain the dignity and rights of all individuals at all times. For example, CCTV cameras will not be placed in an area where intimate care is taking place, and if placed within communal toilets, will be positioned to film shared areas, e.g., entrances/exits/wash basins.

4.6 As far as reasonably possible, all CCTV cameras will avoid focusing on any private residences neighbouring the academy sites.

5 Responsibilities

5.1 Administration and management of the system is the responsibility of the Trust's IT Team, along with the Director of Trust Services.

5.2 The Headteacher/Head of Setting has delegated responsibility for oversight of CCTV on their individual site.

5.3 The day-to-day management and operation of the CCTV systems will be the responsibility of the IT Team and the Site Team.

6 Operation of the System

6.1 The system comprises of fixed/PTZ cameras located around the sites. In some areas, monitoring stations are set up; however, monitors will be positioned where they cannot be viewed by persons other than those authorised.

6.2 The CCTV system is able to be operated 24 hours each day, every day of the year, and this is the Trust's default operation.

6.3 Any faults in the operating system are sent to the IT Team in an automatic email alert (or through a manual report). A member of the IT Team will submit a ticket through the IT ticket system, and the technician on duty will action the repair.

6.4 Cameras are set to record on motion detection, and are maintained to provide the highest possible levels of coverage.

7 Access to the CCTV system and recorded footage

7.1 The IT Support Team have access to CCTV systems and recorded footage. They are also able to extract footage to show to authorised staff (in line with 7.3). On some sites, additional authorised staff can view live footage, but they are not able to extract footage from the system.

7.2 Video screens displaying live pictures should be kept in access-controlled areas where possible, and must not be viewed in public areas.

7.3 In the event that staff wish to view live pictures, watch playback or receive digital exports, the following must take place:

- An IT ticket must be submitted by a member of the setting's Senior Leadership Team (SLT). If the member of SLT wishes to request the footage for another member of staff to view, they must state this in their request. In the event that a member of SLT wishes to view the footage themselves, they must copy another member of SLT into the IT ticket.
  The IT Team will not release footage if the request is made through a method other than the IT ticket system, if the request comes from an individual who is not a member of the setting's SLT, or a member of SLT requests the footage for themselves without including another member of SLT in the IT ticket.
- In the event that a member of the IT Team has concerns about a request, they can discuss this with their Line Manager and/or the Trust's Designated Safeguarding Lead (DSL).
- A member of the IT Team will upload the selected footage to a secure area of SharePoint, ensuring only those with authorisation have access. If the

request is to view live footage, the member of staff will be able to go to the IT Office to view it with a member of the IT Team.
Footage placed in the SharePoint area will automatically delete after 30 x days, unless a request is made for the footage to be kept for an extended period (in line with Section 10 of this policy).

- The IT Team will keep the ticket request in the ticket system archive.

7.4 There may be occasions when members of the Central Services Team require access to CCTV to perform an aspect of their role. This may include, but is not exclusive to, the Data Protection Officer (DPO), the Director of Safeguarding and the Head of HR. If access to CCTV footage is required, the following must take place:

- An IT ticket must be submitted by the Trust's DPO or Head of HR. If the DPO/ Head of HR wishes to request the footage for another member of staff to view, they must state this in their request. In the event that the DPO/ Head of HR wishes to view the footage themselves, they must copy the Director of Safeguarding or the Director of Trust Services into the IT ticket.
  The IT Team will not release footage if the request is made through a method other than the IT ticket system, if the request comes from an individual who is not the DPO/Head of HR, or the DPO/Head of HR requests the footage for themselves without including the Director of Safeguarding or the Director of Trust Services in the IT ticket.
- If a member of the IT Team has concerns about a request, they can discuss this with their Line Manager and/or the Trust's Director of Safeguarding.
- A member of the IT Team will upload the selected footage to a secure area of SharePoint, ensuring only those with authorisation have access. If the request is to view live footage, the member of staff will be able to go to the IT Office to view it with a member of the IT Team.
  Footage placed in the SharePoint area will automatically delete after 30 x days, unless a request is made for the footage to be kept for an extended period (in line with Section 10 of this policy).
- The IT Team will keep the ticket request in the ticket system archive.

7.5 Authorised ICT support staff may access the system but only in line with 7.3, or to perform maintenance tasks which have been logged on the ticket system.

7.6 Members of the public, including parents/carers, visitors and pupils are not permitted to view CCTV footage. Any requests from a data subject to access their personal data held within the Trust's CCTV system should be submitted as a Subject Access Request (SAR) to the Trust in line with HR6 Data Protection Policy. Each request will be considered on a case-by-case basis but access to footage may be limited to the data subject's personal data alone and

will only be provided if doing so does not impact the rights and freedoms of other data subjects who may also appear in the footage.

7.7 In line with the Data Protection Act 2018 and UK GDPR the Trust will share CCTV footage with law enforcement authorities (for example, the Police) who are discharging their statutory law enforcement functions. This is likely to occur in the following circumstances (although this is not an exhaustive list):

- the Trust reports a crime, and shares footage relevant to the crime report;
- the Trust receives a request from a law enforcement authority for CCTV footage held; and/or
- a court order or another legal obligation compels the Trust to share the footage with a law enforcement authority.

7.8 In the event that a request for CCTV footage is made by a law enforcement authority, a member of the IT Team will seek authorisation from either the Trust's DPO or the Director of Safeguarding. A record will be kept of any footage that is issued to a law enforcement authority through the IT ticket system archive.

7.9 A copy of the required footage will be released to the appropriate law enforcement authority via a secure method, e.g., a CD rom in a sealed envelope, a secure OneDrive link, or an encrypted storage device.

7.10 Footage will only be released to a law enforcement authority on the clear understanding that the footage remains the property of the Trust, and the Trust retains the right to refuse permission for the law enforcement authority to share the footage with any other person/organisation.

7.11 In the event that the law enforcement authority requests that the Trust retains the footage, for possible use as evidence in the future, the Trust will do so in line with Section 10 of this policy.

7.12 Applications received from outside agencies (e.g., solicitors) to view or release footage will be referred to the Trust's DPO. In these circumstances, recordings may be released where satisfactory evidence is produced showing that they are required for legal proceedings, a Subject Access Request (SAR), or in response to a court order.

8 Covert Surveillance

8.1 If covert surveillance is planned, the decision to implement the surveillance will be made by the DPO. All documentation must be retained and no covert surveillance will take place unless all necessary processes and authorisations

have been obtained in advance. Covert surveillance will only be used for the purpose of detecting or preventing a crime.

9 Security

9.1 In line with the requirements of the Data Protection Act 2018 and UK GDPR, the Trust has the following security measures in place to protect the data collected:

- the footage is stored on encrypted data stores;
- only authorised staff have access to the material; and
- the servers are updated in line with Cyber Security guidelines.

10 Retention

10.1 CCTV footage is kept for up to 7 x days in recycled storage.

10.1 CCTV 'extractions'/recordings are retained by the Trust for 30 x days, after which they are deleted.

10.2 In the event that recordings are required to be kept beyond 30 x days, a member of the IT Team, with the agreement of the Trust's DPO (and the Director of Safeguarding if appropriate), will store the required recording in a secure area of SharePoint (with restricted access). The recording will be kept for a further 30 x days, upon which it will be subject to review and a decision will be made as to whether to extend the retention of the recording, or delete it. Recordings may only be retained in order to fulfil the purpose for which they have been made (please see section 4.2), or at the request of a law enforcement authority discharging statutory law enforcement functions.

11 Breaches of the Policy

11.1 Any individual found to be in breach of this policy will be reported to HR, and may be subject to an investigation in line with HR12 Staff Disciplinary Policy.

11.2 Any concerns about an individual's conduct in relation to this policy should be reported to the Trust's DPO. If the concern relates to an adult's conduct with children and young people, it should be reported to the Headteacher/Head of Setting or the Trust DSL. If necessary, individuals can refer to the following policies for guidance:

- HR23 Whistleblowing Policy
- HR24 Allegations of Abuse Made Against Adults Policy
- HR42 Low-Level Concerns Policy

12 Complaints

12.1 Any complaints about the Trust's CCTV system should be addressed to the Trust's DPO for investigation, in line with HR6 Data Protection Policy. Any complainant will be notified of the outcome of the investigation and if they are not satisfied with that outcome, will be provided with information about how to refer the matter to the Office of the Information Commissioner.

13 Policy Change

13.1 This policy may only be amended or withdrawn by The Priory Federation of Academies Trust.