Policy: Closed-Circuit Television (CCTV)

Author	Premise Manager
Date last reviewed	June 2025
Approval route	College Leadership Team
Date Approved	10th September 2025
Review cycle	Annually
Date Review Due	September 2026
Contractual or Non-Contractual	Contractual / Website
Location of copies	College SharePoint
Policy version	1

FRANKLIN COLLEGE TRUST

1. Introduction

Franklin College Trust is committed to transparency, accountability, and openness in its operations. This Closed-Circuit Television (CCTV) Policy sets out how we will comply with the Data Protection Act and UK GDPR as the lawful basis for CCTV processing includes and is not limited to for legitimate interests and a public task.

Franklin College Trust is a provider, who is responsible for the collection and processing of your personal data, the use of surveillance systems is lawful, fair, transparent and meets the standards set in the data protection law. The Trust is the data controller and/or processor for personal data relating to you.

2. Purpose of the Policy

The purpose of this policy is to:

- Ensure that the Trust complies with the requirements of the Data Protection Act and UK GDPR in relation to CCTV.
- Provide staff, students, and third parties with clear guidance.
- Promote a culture of openness and transparency within the Trust.
- Clarify the responsibilities of staff.

3. Scope of the Policy

This policy applies to the following individuals to follow:

- **Staff:** All employees, Community Governors, Directors, Members contractors, and volunteers working for the Trust.
- **Students:** Individuals enrolled at the Trust, including those on full-time and part-time programmes.
- **Third Parties:** External individuals or organisations making requests from the Trust.

This policy covers all information held by the Trust in relation to CCTV.

4. What information do we hold about you?

- We carry out CCTV recording across the Trust's sites. The Trust is registered with the Information Commissioner's Office (ICO) for this purpose.
- CCTV covers some interiors and exteriors of buildings. If you attend, visit or work at Franklin College Trust we may record moving images of you as you enter and move about Trust sites.

5. Why do we collect this information?

- We have installed CCTV and make recordings to enable us to keep students, staff and visitors safe protecting the Trust's buildings and assets, both during and after Trust hours and to help investigate and / or provide evidence from health and safety incidents, to aid crime prevention and detection and any equivalent malpractice.
- The CCTV system is owned and operated by the Trust, the deployment of which is determined by the Colleges Leadership Team.

6. Who might we share your information with?

- We aim to keep this information about you confidential.

- We may be asked to share data with other third parties where there is a lawful reason for their request. These may include: the police, social services, legal firms acting on you're or the Trust's behalf, insurance companies, or other government or regulatory agencies.

7. Privacy Notices

Our privacy notices which are available on our website state the following:

CCTV

CCTV recordings are used and retained for a limited period to ensure the safety of student applicants, students, parents/guardians, staff and visitors to the Trust. Access to view and monitor these recordings is limited to the appropriate staff who will report and act accordingly if suspicious or inappropriate actions or behaviours are identified. CCTV images may be passed on to the police for the purposes of crime detection or prevention and Franklin College Trust will also disclose CCTV footage when requested by insurance companies. CCTV may be used to assure the integrity of our examination arrangements, with footage shared with Awarding Organisations for audit and fraud prevention purposes. This is in line with the Data Protection Act and UK GDPR as the lawful basis for CCTV processing includes and is not limited to for legitimate interests and a public task.

8. What do we do with your information?

- We collect this information which is held on the CCTV system for the safety and security of those who are on the Trust premises.
- The CCTV may be viewed by authorised staff and in the event of an accident or other incident may be viewed by other members of staff at the Trust.

9. How do we protect your data?

- We take the security of your data seriously and have controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed inappropriately.
- Where we engage third parties to process personal data on our behalf, we do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

10. How long do we keep this information about you?

- We keep information recorded on CCTV for 60 days, where the IT system can accommodate the volume of data stored, after which it is deleted. Where recordings are requested or required to provide evidence of incidents, the relevant section of recording will be downloaded and stored by the Trust. These recordings will be kept in line with the Trust's Data Retention policy.
- Technical controls: Individual User Authentication & Password Policies, encrypted storage, Audit Trails & Logs and access control systems for auditing.
  CCTV recordings will be stored securely and only retained for as long as necessary. Footage will normally be retained for a limited period unless it is required for an investigation, this is in line with the Trust Retention Schedule and covered in the lawful basis. Access to CCTV footage will be restricted to authorised personnel only.

11. Your Rights

Under data protection law, you have the following rights regarding your data:

- **Access**: You have the right to request access to the personal data we hold about you in certain circumstances.
- **Rectification**: You have the right to request that we correct any inaccurate or incomplete data in certain circumstances.
- **Erasure**: You have the right to request the deletion of your personal data in certain circumstances.
- **Restriction**: You have the right to request that we restrict the processing of your personal data in certain circumstances.
- **Data Portability**: You have the right to request that we transfer your personal data to another organisation.
- **Objection**: You have the right to object to certain types of processing of your data in certain circumstances for example if it is likely to cause, or is causing, damage or distress.
- **Withdrawal of Consent**: If we process your data based on your consent, you have the right to withdraw that consent at any time in certain circumstances.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstance, have inaccurate personal data rectified, blocked, erased or destroyed

To exercise any of these rights, please contact the Trust's Data Protection Officer (DPO).

Right to request access to your information

- Under data protection legislation individuals have the right to request access to information about them that the Trust holds. The rights of other individuals will always be considered. The right will be considered and whether it is appropriate to provide you with the information. To make a request for this, please email information.governance@franklin.ac.uk who will process the request in partnership with Franklin College Trust's Data Protection Officer.
- If you have any queries or concerns which are not answered by this policy, other data protection related policies or privacy notices about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance to information.governance@franklin.ac.uk. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/make-a-complaint
- To request a Subject Access Request (SAR), you must follow the organisation's Data Protection Policy. Once the request is received, it will be processed within one month in accordance with data protection regulations. The request will also be recorded in the SAR log for tracking and compliance purposes.
- A record will be kept of any incidents, access requests, or viewing of CCTV footage.
- The incident log will be maintained securely and monitored by the Premises Manager or Data Protection Officer.

12. What we may need from you

- We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

13. Access and Viewing of CCTV Footage

- Access to CCTV footage will be strictly controlled and limited to authorised personnel only. Authorised personnel may include:
- The Premises Manager
- The Data Protection Officer
- Other authorised staff where necessary for investigation purposes
  CCTV footage may only be viewed when there is a legitimate reason, such as:
- Investigating an incident
- Supporting health and safety investigations
- Assisting law enforcement where required
  All requests to view or access footage must be recorded in the CCTV incident log.
  CCTV footage will not be shared with third parties unless required for legal reasons, such as requests from the police or in response to a valid Subject Access Request.

14. Training and Awareness

- CCTV training and guidance on maintaining the incident log will be provided by the Premises Manager or the Data Protection Officer. Only authorised staff members will have access to CCTV footage.
- CCTV Signage – Clear signs will be displayed in areas where CCTV is in operation to inform staff, visitors, and members of the public that recording is taking place. The signage will include:
- Notification that CCTV is in operation
- The purpose of monitoring (e.g., safety and security)
- The name of the organisation responsible for the CCTV system
- Contact details for further information

  Signage will be placed at entrances and in visible areas so that individuals are aware they are entering an area monitored by CCTV.

15. Policy Review

- This policy will be reviewed by the Premises Manager, Data Protection Officer and College Leadership Team to ensure it remains up to date and effective. Any necessary amendments will be made in consultation with relevant parties. This is to make sure that we continue to meet the highest standards and to protect your privacy. We always reserve the right, to update, modify or amend this policy. We suggest that you review this policy from time to time to ensure you are aware of any changes we may have made, however, we will not significantly change how we use information you have already given to us without your prior agreement. The latest version of this policy can be found on the Trust's website.

16. Contact Information

- For further information or assistance regarding CCTV, please contact the Premises Manager: Telephone: [01472 875 000]. Postal Address: [Premises Manager, Franklin College Trust, Chelmsford Avenue, Grimsby, DN34 5BY]