CCTV Policy

1. Purpose and scope

1.1. Girton College ("College") is committed to maintaining the safety and security of its members and visitors, heritage buildings and antiquities. To facilitate this requirement, the College has CCTV surveillance at strategic points across the site.

1.2. This CCTV Policy describes the purpose, use and management of the CCTV surveillance system in College to ensure it meets all relevant regulatory and legislative obligations.

1.3. The College will maintain the CCTV surveillance system in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulation ("UK GDPR"), and has been written with due regard to the current guidance from the Information Commissioner's Office ("ICO") and The Surveillance Camera Code of Practice (PoFA 2012).

2. Roles and Responsibilities Overview

2.1. Data Controller

2.1.1. The CCTV system is owned by Girton College, Cambridge, CB3 0JG and managed by the Porters' Lodge, the IT Department and its appointed contractor.

2.1.2. In accordance with the Data Protection Act 2018, the College is the 'data controller' for the images and recordings produced by the CCTV system. The College is registered with the Information Commissioner's Office with the registration number Z6671415.

2.2. Head Porter

2.2.1. The Head Porter is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.2.2. The Head Porter is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

2.2.3. The Head Porter is responsible for ensuring the Porters have adequate training to operate the CCTV system, including monitoring images in relation to this policy.

3. Purposes and implementation of the CCTV System

3.1. The purposes of the College's CCTV system are as follows:

a. to ensure the safety of staff, students and visitors.
b. as a deterrent and for the prevention, reduction, detection and investigation of crime and other incidents.
c. to assist in the investigation of suspected breaches of College regulations by staff, students or visitors.
d. to monitor and enforce traffic related matters on site.

3.1.1. The CCTV system will be used to observe the College's buildings and grounds in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

3.1.2. The College seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

3.2. The implementation of the College's CCTV system

3.2.1. The CCTV system operates across the College's residential, public and parking areas.

3.2.2. Cameras are sited to ensure that they cover College premises as comprehensively as is required. Cameras are installed to cover College access points, car parks, buildings, residential accommodation (as described in 3.2.3), external buildings, and public areas which are considered to be vulnerable.

3.2.3. Cameras are not sited to focus on private residential areas and cameras situated in College residential accommodation focus on entrances and communal areas only.

3.2.4. Automatic Number Plate Recognition ("ANPR") cameras are sited at the car park boundary, to identify and provide access to authorised College members and visitors.

3.2.5. Any future dwelling developments near College premises which places private premises within the view of the cameras, will be protected for the privacy of the residents. This will be ensured by the pixilation of any such views by the appointed contractor.

3.2.6. CCTV Signs are placed at all College entrances to inform members of College, visitors and members of the public that CCTV is in operation.

3.2.7. The CCTV system will be reviewed on an annual basis to ensure the cameras are fit-for-purpose and sited in the relevant positions.

4. Data Protection Legislation

4.1. The College's operation of a CCTV system across its sites complies with the principles set out in the UK General Data Protection Regulation ("UK GDPR") and Data Protection Act 2018.

- Processed (i.e. collected, handled, stored, disclosed and destroyed) fairly, lawfully and transparently
- Processed only for specified, explicit and legitimate purposes
- Adequate, relevant and limited
- Accurate (and rectified if inaccurate)
- Not kept for longer than necessary
- Processed securely

4.2. The College will undertake a 'data protection impact assessment' before each new or updated camera is installed, to ensure the privacy implications are fully recognised.

5. Monitoring and Recording

5.1. The College's CCTV system is monitored in the Porters' Lodge at the main College site and Swirles Court. The area is secure and staffed 24 hours a day.

5.2. The CCTV images are recorded centrally on servers located securely at the College and are accessible and monitored by the College Porters. The IT Department personnel and appointed contractors have access to these images only where technical support is required.

5.3. CCTV images will only be downloaded by an appropriately trained person.

5.4. The cameras are positioned and installed to provide images of suitable quality around the College site for the purposes specified. The system is checked on a daily basis to ensure the accuracy of the data.

6. Image Retention Schedules

6.1. Images are retained for a maximum of 30 days and overwritten unless they are required as evidence in an investigation of an offence or by law.

6.2. Images requested as the result of an incident, must be secured immediately and within 72 hours at the very latest, to ensure any potential evidence is available to the relevant investigation team.

6.3. In recognition of the forthcoming 'Terrorism (Protection of Premises) Act 2025'[1], all CCTV footage will be held for a maximum of 30 days for investigatory purposes for events held at the College that match the following criteria:

- Medium or large events over 200 guests
- Events which are subject to an individual risk assessment

6.4. Where there have been no incidents or requests arising from the event within this period, the images will be deleted in accordance with the College's Records Retention Schedule.

6.5. Images that are retained as part of an investigation will be held securely and will be reviewed and destroyed in accordance with the timescales agreed in the College's Records Retention Schedule.

6.6. Images that are retained as part of an investigation will be accessible only by those conducting the investigation and the Head Porter or Deputy Head Porter.

7. Access and applications for CCTV Images

Access and Applications by Individuals

7.1. Individuals who wish to have access to CCTV images relating to themselves should complete the College's 'Data Subject Access Form' or contact the College Data Protection Lead.

7.2. Individuals will be required to provide suitable and valid identification before the College will process the 'data subject access request'.

7.3. To enable the College to accurately identify the individual, a detailed description must be provided of the images required, including location, date(s) and time(s). Individuals should also specify the format in which they require the images to be provided.

7.4. Individuals should expect to have a response to their 'data subject access request' within one calendar month of submitting their request. The College will contact the individual where there may be a delay in completing the request, in order to agree an extended deadline.

[1] Commonly known as Martyn's Law: https://www.gov.uk/government/publications/terrorism-protection-of-premises-act-2025-factsheets

7.5. The College may be unable to comply with an individual's 'data subject access request' if the images requested contain another identifiable person or persons. The 'data subject access request' will be reviewed by the College Data Protection Lead to determine if it necessary to obtain consent from the identifiable person or persons or if on balance the image(s) can be feasibly released without the person's consent.

Access and Applications by Third Parties[2]

7.6. Applications for CCTV images regarding a person or persons by a Third Party must be made using the College's 'Data Subject Access Form' or by contacting the College Data Protection Lead.

7.7. Applications made on behalf of the 'data subject' will require written authorisation and valid proof of identity from the data subject before a request will be processed.

7.8. Disclosures of CCTV images, where it is appropriate, may be disclosed to:

- The "Gold Group" for all health, safety and security issues that pose a risk to the College and its members.
- The Senior Tutor and/or Dean of Discipline and a Disciplinary Committee as part of a student disciplinary investigation.
- The Head of HR and a Disciplinary Panel as part of a staff disciplinary investigation.
- Appointed agents or representatives acting on behalf of the College in relation to an incident or investigation involving the safety and security of its members, or the damage or destruction to the College's estate and properties.

7.9. Disclosures to a Third Party are limited and usually in relation to incidents that impact the security and safety of College members, crime prevention, detection or required by law. Further disclosures without consent, will be in accordance with the relevant legislative exemption.

7.10. All requests for disclosure to a Third Party will be in agreement with the College Data Protection Lead.

7.11. All disclosures of CCTV data will be recorded by the College Data Protection Lead and held in accordance with the College's Records Retention Schedule.

8. Policy Review

This policy is reviewed by Information Management Committee and approved by the College Council. It is reviewed at least once every three years. The Information Management Committee remains responsible for ensuring appropriate resources are in place to achieve compliance with data protection law in line with an appropriate overall risk profile.

9. Contacts

9.1. College Contact

[2] For the purpose of this policy, a **third party** refers to **anyone** who is **external** to the management of the CCTV system or an authorised person as outlined in Section 7.8. For example, all staff, Fellows and students are third parties.

To make an enquiry or raise a concern about the College's Data Protection policies or data processing activities or to make a 'data subject access request', please contact:

College Data Protection Lead
Girton College
Cambridge, CB3 0JG

Tel: 01223 338987
Email: data.protection@girton.cam.ac.uk

9.2. Complaints and concerns

To raise a concern or make a complaint regarding the College's handling of your 'data subject access request' or data processing activities, please follow the 'Complaints Procedure' available on the College website: https://www.girton.cam.ac.uk/information-compliance/complaints

Last updated: 29 May 2025
College Data Protection Lead

Version Control

Date	Version	Review Reason	Author
30/05/2019	1.0	Policy Review by Porters' Lodge and IT Department	College Data Protection Lead
04/06/2019	1.0	Review by Information Management Committee	College Data Protection Lead
01/07/2019	1.0	Publication	College Data Protection Lead
27/10/2021	1.1	Review by Porters' Lodge and IT Department	College Data Protection Lead
23/11/2021	1.1	Review by Information Management Committee	College Data Protection Lead
25/02/2022	1.1	Publication	College Data Protection Lead
15/11/2024	1.2	3-year review by Porters' Lodge and IT Department	College Data Protection Lead
26/11/2024	1.2	Review by Information Management Committee	College Data Protection Lead
12/12/2024	1.2	Publication	College Data Protection Lead
10/06/2025	1.3	Review by Information Management Committee	College Data Protection Lead
21/07/2025	1.3	Publication	College Data Protection Lead

Appendix A – Definitions

"Agents" include but are not limited to legal, insurance or security representatives and/or advisors

"CCTV system" as part of a "surveillance camera systems" which is defined by the 'Protection of Freedoms Act (PoFA) 2012'as:

(a) closed circuit television or automatic number plate recognition systems,
(b) any other systems for recording or viewing visual images for surveillance purposes,
(c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or
(d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

"Data Controller" as defined under Article 4(7) UK GDPR:

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

"Gold Group" consists of the College's Senior Officers:

Mistress, Vice Mistress, Bursar, Senior Tutor, Junior Bursar and Development Director

"Martyn's Law" or Terrorism (Protection of Premises) Act 2025:
An act which sets out the responsibilities, procedures and measures an organisation must put in place to ensure appropriate security is established to better protect the public from terrorism. The Act is expected to be implemented over a 24-month period and fully enforced in 2027.

"Personal Data" as defined under Article 4(1) UK GDPR:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Third Party" as defined under Article 4(10) UK GDPR:

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

For the purpose of this policy, a **third party** refers to **anyone** who is **external** to the management of the CCTV system or an authorised person as outlined in Section 7.8. For example, all staff, Fellows and students are third parties.