1.目的与范围
1.1. 芝士大学（“大学”）致力于维护其成员和访客，文化遗产建筑和古迹的安全与安全。为了满足这一要求，大学在战略位置部署了CCTV监控。

1.2. 本CCTV政策描述了CCTV监控系统的用途、使用和管理，以确保它满足所有相关监管和立法义务。

1.3. 大学将保持CCTV监控系统符合《数据保护法2018年》和《通用数据保护法规》（“GDPR”），并且已经写入了与信息专员的当前指导的一致性：“图片：数据保护实践指南，摄像机和个人信息”

2. 角色和职责概览
2.1. 数据控制人
2.1.1. CCTV系统由芝士大学，剑桥大学，CB3 0JG拥有，并由门房办公室，计算机办公室及其聘用的承包商管理。

2.1.2. 根据《数据保护法2018年》，大学是CCTV系统产生的图像和录音的“数据控制人”。大学已向信息专员办公室注册，注册号为Z6671415。

2.2. 门房
2.2.1. 门房负责CCTV系统的整体管理和操作，包括与安装，记录，审查，监控和确保与本政策一致的活动。

2.2.2. 门房负责确保在遵守ICO CCTV Code of Practice的情况下，适当的标志已经竖立。

2.2.3. 门房负责确保门房人员接受适当的培训，以操作CCTV系统，包括审查和监控与本政策相关的图像。

3. 目的和CCTV系统实施
3.1. 大学CCTV系统的目的是以下几方面：
   a. 确保工作人员，学生和访客的安全；
   b. 作为威慑和预防，减少，检测和调查犯罪和其他事件的手段；
   c. 协助调查可疑的大学规定违反事件；
   d. 监控和执行交通相关的事项在校园内

3.1.1. CCTV系统将用于观察大学的建筑和场地，以识别需要响应的事件。任何响应应与所见证的事件成比例。

3.1.2. 大学寻求以尊重个人隐私的方式运营CCTV系统。

---

20190530CCTVPolicyFinal.docx
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. 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.

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

3.2.6. 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 General Data Protection Regulation (“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 Computer Office staff 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 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.

   6.3. Images that are retained as part of an investigation will be accessible only by those conducting the investigation and the 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.

   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**

   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:
CCTV Policy

- the Senior Tutor and/or Dean of Discipline and a Disciplinary Committee as part of a student disciplinary investigation.
- the HR Manager and a Disciplinary Panel as part of a staff disciplinary investigation.

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
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 contact:

Data Protection Officer
Office of Intercollegiate Services
12b King’s Parade
Cambridge, CB2 1SJ

Tel: 01223 768745
Email: college.dpo@ois.cam.ac.uk