CHRIST'S COLLEGE
UNIVERSITY OF CAMBRIDGE

Building Access Data Policy

Introduction

Christ's College operates a building access system to provide a safe and secure environment for students, staff and visitors and to protect College property.

This document details the accepted use and administration of the building access system, and the data logged on it to ensure the College complies with the GDPR and Data Protection Act and other relevant legislation.

This policy has been written to balance the individual right to privacy with that of the College Community to live in a safe and secure environment.

Purpose

The College has installed a building access system with the main aim of reducing the threat of crime, protecting the College property and ensuring the safety of all individuals. To accomplish this objective, the system is used for the following purposes:

1. Control access to locations in College including car parks, rooms, lockers and storage areas
2. Deter individuals who may have criminal intent
3. Assist with the prevention and detection of crime
4. Assist with the identification, apprehension and prosecution of offenders in relation to criminal and public order offences
5. Assist with the identification of individuals, activities and incidents which may result in disciplinary proceedings against students or staff involved
6. Monitor the security of the site entrances and all doors, locked cupboards and storage areas
7. Facilitate the movement and control of vehicles using the College car parks
8. Enable the identification of individual(s) who misuse College property
9. Identify individuals who remove books from the Library without first using self-service checkout

Log Retention

The log data for the system is used to ensure that the system is working correctly. It may also be used when appropriately anonymised to gauge the use of a particular room resource such as the use of the College Library. Logs will be kept for no longer than is necessary and in this case is taken to be 3 years to enable the analysis of the offline doors' battery usage. The archive period will be the shortest amount of time required for the system to fulfil its purpose.
The archive period will be reviewed annually to ensure it is appropriate, it will however also be reviewed as part of any post-incident review of door access.

Staff

The data captured by the system will be monitored by the College Porters who are responsible for security. The Director of College Services has overall responsibility for the system, but operational responsibility belongs to the Head Porter.
The duty porters will monitor the system at their workstation. They will also ensure that all outer doors are functioning correctly and have the appropriate method of opening and schedule.
Requests for data disclosure should be sent to the Head Porter who is able to review any data stored within the defined retention period.

IT and Maintenance staff as well as Building Access contractors will occasionally view data to ensure the system is working efficiently and to correct any faults that may occur.

All Porters will be briefed on the correct operation of the system.

Disclosure of data

The disclosure of data will be treated with care to ensure the rights of the individual(s) and fair processing. There may be rare circumstance when the release of data to a third party is required if their need outweighs those of the individual(s) whose access(es) were recorded.
Disclosure will be limited to:

1. Police and other law enforcement agencies, where the data could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.
2. Prosecution agencies
3. Relevant legal representative
4. People whose data have been recorded and retained. N.B. This will not occur if such a disclosure will prejudice a criminal enquiry or proceedings
5. Member of College or University staff involved with a disciplinary process
6. In rare cases to others to assist in the identification of a perpetrator, witness or victim of a criminal incident (e.g. to provide an insurance company with evidence of damage occurring to a car in the car park)

All disclosures should be logged to include date, reason (including crime number if applicable), recipient, job function of the recipient and their organisation, reason, person who released it and details of the data released and what media was used. Release of personal data under the UK GDPR should be logged by the College Information Manager in the Subject Access Request log.
The method used to provide the media should be secure (e.g. an unencrypted USB stick sent via standard post should not be used) and preferably by hand where the recipient can sign the logbook to confirm their receipt.

Individual's access rights

The UK General Data Protection Regulation (GDPR) gives individuals the right to access personal information about themselves this includes their door access information. All such requests should be made to the Head Porter. The Head Porter or their deputy will liaise

with the Information Manager or Bursar to ensure compliance, and that no third-party information is revealed. The individual will be asked to provide:

1. Date and Time
2. Location in College
3. Any additional information that may be relevant to assisting the search for the information

The Information Manager or Bursar as the College Data Protection Lead has the right to refuse the request especially if the release of the information would prejudice an on-going criminal or disciplinary case.
Individuals have the right to prevent processing of their data if such processing is likely to cause substantial and unwarranted damage to them. All such requests should still be made to the Head Porter who will consult with the Information Manager or Bursar. the individual will be notified in writing of the outcome no later than 30 days from the receipt of the request.

Freedom of Information or EIR requests

The release of any personally identifiable information (PII) is exempt under the FOI or EIR as it must follow UK GDPR data principles; this includes the information held in this system.

This policy may be released under the Freedom of Information Act.

Complaints

Any complaints about the system should in the first instance be addressed by the Head Porter. If the complainant is not satisfied with the response received, they should write to the Director of College Services.
Any requests relating to the UK GDPR or Freedom of Information Act should be addressed to the relevant Compliance Officer at the address below:

Christ's College
St Andrew's Street
Cambridge CB2 3BU
UK
For UK GDPR email dpa@christs.cam.ac.uk or foi@christs.cam.ac.uk for Freedom of Information requests