CCTV POLICY

Document Title		
CCTV POLICY		
Document Author/Owner:	**Responsible Person:**	
Head of Facilities	CEO	
Approving Body:	**Date of Approval:**	
Board of Trustees		
Effective from:	**Review Date:**	
	June 2026	1
EITHER For Public Access? **Tick as appropriate**	**OR** For Internal Access only? **Tick as appropriate**	
YES ✓	**YES**	
Summary/Description:		
This document sets out the principles of data protection compliance at All Nations Christian College to ensure that it processes all data fairly and complies with the Data Protection Act 2018 and UK GDPR. This document should also be read in conjunction with the relevant privacy notice, these are available on the College website. Students should also ensure that they read the **HESA Student Collection Notice**.		
This document has been adapted from a policy document by The Open University, with grateful acknowledgment.		

ALL NATIONS CHRISTIAN COLLEGE

To cultivate biblically rooted, hope-filled and culturally relevant engagement with God's mission, by training and equipping disciples of Jesus Christ in partnership with the global church.

CCTV POLICY

1. CONTENTS OF POLICY

2. POLICY STATEMENT

The College is committed to ensuring the safety and security of its community through the responsible use of a CCTV system. The aims of this policy are to:

- Protect the health and safety of students (and their families), staff and visitors
- Protect College buildings and assets
- Reduce the likelihood of crime and anti-social behaviour, including theft and vandalism
- Assist in identifying, apprehending and prosecuting offenders
- Assist in the safeguarding of children living on site
- Assist in the investigation of breaches of the College Code of Conduct and policies by staff, students and visitors (including contractors), and, where relevant and appropriate, investigating complaints
- Comply with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Data Protection Act
- Conduct CCTV surveillance in a manner in keeping with the aims of this policy, ensuring that monitoring is conducted legally, professionally and ethically
- Ensure that through carefully selected camera positions, monitoring is not used for any incompatible purpose, such as to pry on individuals' privacy or to monitor employee performance

The College will ensure that all CCTV operations are conducted with the full knowledge of the College community, with appropriate and adequate signage to indicate the presence of CCTV, and all data will be handled in compliance with current data protection regulations.

The policy will be reviewed annually by the Senior Leadership Team to assess performance against the policy aims and to assess the continued need for CCTV monitoring.

3. DEFINITIONS

CCTV system – Closed Circuit Television. A surveillance system that uses cameras to capture video footage and transmit video images to a recording device.

ICO – Information Commissioners Office. The UK's independent regulator for data protection and freedom of information.

4. SCOPE

This policy document applies to all those who live, study or work on our College site, and also to those who visit our site. This includes, students (and their families), staff, volunteers, conference guests, staff of (and visitors to) other charitable organisations renting office space on site, long-term guests and visitors (including contractors).

5. LEGISLATIVE FRAMEWORK

This policy will be implemented to ensure that the use of the CCTV system is proportionate and lawful under the terms of the:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Information Commissioner's Office CCTV Codes of Practice

6. DATA PROTECTION

As the CCTV system processes identifiable images of individuals, and is therefore processing personal data, all data is processed in a manner to maintain its security. This includes protection against unauthorised or unlawful processing, accidental loss, destruction or damage. The lawful basis for processing the personal data as part of the CCTV system is legitimate interest.

This policy should be read in conjunction with the College's Data Protection Policy and Privacy Statement.

USE OF CCTV

The College's CCTV system and the images produced by it are the subject of this policy, for which the CEO is the responsible person in liaison with the ICT Manager and the ICT System Administrator, who are responsible for how the system is used under the Data Protection Act 2018 and UK GDPR.

The Senior Leadership Team have considered the need for using CCTV and have decided it is necessary for the prevention and detection of crime and for protecting the safety of individuals, and the security of the College premises. We will not use the system for any incompatible purposes and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate. The system operates 24 hours a day, 365 days per year.

7. CAMERAS

Cameras are located in order to provide surveillance of vulnerable points on the perimeter of the main College site.

Camera number	Camera specification	Location/Field of view	Reason for choice of location
CAM001	Hikvision DS-2CD2346G2-IU AcuSense, Pro EasyIP 4.0 Outdoor HD PoE Turret IP Camera w/ 2.8mm Lens, 30m Night Vision, Audio (4 MP)	Maple Hall FOV: kitchen fridge area	Surveillance of food stores and possible intruders to rear of kitchen
CAM002	Hikvision DS-2CD2346G2-IU AcuSense, Pro EasyIP 4.0 Outdoor HD PoE Turret IP Camera w/ 2.8mm Lens, 30m Night Vision, Audio (4 MP)	Rear of Coach House FOV: Rear lane pointing toward the rear of Oak House and the recycling centre	Surveillance of the rear lane and possible intruders from neighbouring woodland
CAM003	Hikvision DS-2CD2347G2H-LI(U) 4 MP Smart Hybrid Light with ColorVu Fixed Turret Network Camera w/ 2.8mm Lens, 30m Night Vision, Audio (4 MP)	Rear of Coach House FOV: Rear lane pointing towards the Oak Tree Cottages	Surveillance of the rear lane and possible intruders entering in vehicles or on foot
CAM004	Hikvision DS-2CD2347G2H-LI(U) 4 MP Smart Hybrid Light with ColorVu Fixed Turret Network Camera w/ 2.8mm Lens, 30m Night Vision, Audio (4 MP)	Courtyard – NE corner of the Ash Centre FOV: Courtyard/Reception	Surveillance of vehicles and individuals entering and leaving the courtyard; security of offices
CAM005	Hikvision DS-2CD2347G2H-LI(U) 4 MP Smart Hybrid Light with ColorVu Fixed Turret Network Camera w/ 2.8mm Lens, 30m Night Vision, Audio (4 MP)	SW Corner of the Ash Centre FOV: ground floor rear of Easneye House, patio and pathway to south of Easneye House	Surveillance of ground floor rear doors and windows to Easneye House and possible intruders from the front car park or woods
CAM006	Hikvision DS-2CD2347G2H-LI(U) 4 MP Smart Hybrid Light with ColorVu Fixed Turret Network Camera w/ 2.8mm Lens, 30m Night Vision, Audio (4 MP)	W aspect of Oak House A wing FOV: rear car park, Games room, kitchen rear entrance, recording studio	Surveillance of intruders to rear of the site from the surrounding woodland; surveillance of intruders to the rear entrance of Maple Hall kitchen and recording studio

All cameras are positioned to avoid any unintended capture of individuals and to respect privacy. Although some of the cameras are capable of audio recording, this function is not enabled.

8. CAPTURE, STORAGE AND PROCESSING OF IMAGES

Images are not displayed on a screen unless there has been a request to view an incident, or unless a live situation is developing. The images are stored on disk drives, in a RAID 5 array, on a secure network attached storage (NAS) device. The NAS is located in a locked cabinet in a locked room in a building with restricted access. When the images need to be viewed, they will be accessed via a secure login to the NAS which then provides access to the CCTV application.

Images are stored for a maximum period of 30 days. They are then automatically deleted from the server unless they have been downloaded as evidence as part of an ongoing investigation. Where this is the case, the images will be copied from the NAS and stored on a secure network drive, with restricted access, and will be retained in line with the College's Data retention schedule for the relevant category of evidence (e.g. complaint handling, safeguarding etc).

9. INFORMATION PROVISION

Site users are made aware of the presence of CCTV cameras by visible signs in place at the location of each camera, at Reception and at other prominent locations around the site. Signage provides the main College phone number for further information to be gained about the scheme.

10. ACCESS TO CCTV IMAGES

Access to images is restricted to the CEO, ICT Manager and ICT System Administrator. Access will be provided to the police, on request, as part of any evidence gathering exercise in the event of a crime.

Individuals (students, staff, visitors etc) can make a request for copies of their own images, or for images to be erased or restricted. The request must be made in writing and include:

- The date, time and location
- The reason for the request (which must comply with the aims of this policy)

All requests should be made as soon as possible to ensure that footage is not erased in line with the retention schedule. Requests should be sent to the Compliance Training Administrator CTA@allnations.ac.uk.

A log will be kept of each access to the images.

11. COMPLAINTS

All complaints relating to the CCTV system should be addressed to: The Compliance Training Administrator, CTA@allnations.ac.uk. All complaints will be handled in accordance with the College's Complaints Policy.

12. ROLES, RESPONSIBILITIES, POLICY APPROVAL & REVIEW

13.1. The **Board of Trustees** have legal oversight and responsibility for all College policies, providing leadership and active support for them and are responsible for ensuring:

- a legally compliant and fit for purpose CCTV Policy is in place and approved by them.
- satisfactory arrangements are made for its effective implementation, including the provision of resources.
- the Senior Leadership Team monitors, evaluates and periodically reviews this policy and recommends any changes to first the Governance Committee and then the Board of Trustees for approval.
- complaints and appeals brought under the terms of this policy are managed satisfactorily by the Senior Leadership Team.
- decision making complies with all relevant legislation and regulatory bodies.
- they receive details from the Senior Leadership Team of reported incidents of data breaches and outcomes of cases (particularly where a significant impact on someone has occurred or lessons need to be learned), or of a serious incident or one which could be of reputational risk to the College which should be reported to either the Information Commissioner's Office, the Office for Students and/or the Charity Commission.

The Board has overall responsibility to ensure that the deployment and use of the CCTV system is within the aims of this policy and for the protection of the interest of the College users and privacy of the individuals whose images are captured on the system.

13.2. The **CEO** is responsible for:

- The implementation and management of this policy; ensuring that procedures are implemented consistently and with clear lines of authority and actively and visibly leading the College's CCTV Policy and practice.
- Ensuring this policy is continually improved in consultation with students and staff.
- Monitoring, evaluating and periodically reviewing this policy and for obtaining approval from the Board of Trustees for any changes made.
- The management of complaints.
- Ensuring decision making complies with all relevant regulatory bodies.
- Reporting details to the Board of Trustees of reported incidents, outcomes of cases (particularly where significant impact on someone has occurred or lessons need to be learned), or of a serious incident or of one which could be of reputational risk to the College.

13.3. **The Data Protection Officer** is responsible for dealing with complaints and the management of data protection within the College.

13.4. **The ICT Manager** is responsible for the CCTV infrastructure ensuring that there is adequate maintenance and that required upgrades to hardware and software are performed.

13.5. **The ICT System Administrator** is responsible for maintaining the security of the captured (and recorded) images by ensuring adequate protections are placed on the hardware storing the images and by restricting access to the images to those with authority to do (as prescribed in this policy).

13. POLICY COMMUNICATION

This policy will be signposted in the Staff Additional Policies document and the Campus Access Handbook, and will be included in staff and student induction. Conference groups will be made aware of the presence of the CCTV through the Conferences and Lettings policy and in the site familiarisation briefing at the start of a conference. Other guests are alerted to the presence of CCTV by signage on site.

14. RELATED DOCUMENTS

- All Nations Christian College Bullying, Harassment and Sexual Misconduct Policy
- All Nations Christian College Campus Access Student Handbook
- All Nations Christian College Complaints Policy
- All Nations Christian College Data Protection Policy
- All Nations Christian College Safeguarding Policy
- All Nations Christian College Staff Additional Policies and Procedures
- All Nations Christian College Student Disciplinary Policy