Archbishop Beck Catholic College

CCTV Policy

ARCHBISHOP BECK CATHOLIC COLLEGE - CCTV POLICY

The Governing body is committed to securing the safety and well-being of employees, students and others affected by activities on College premises.

Aims

- To provide a safe environment for staff and students
- To provide improved site security
- To prevent and identify petty vandalism and theft
- To prevent anti-social behaviour in areas around the college
- To ensure the health and safety of the staff and students and visitors to the college

1. Introduction

1.1 The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Archbishop Beck Catholic College hereafter referred to as 'the college'. This policy is to be read in conjunction with the *Code of Practice* issued by the *Information Commissioners*.

1.2 The system comprises a number of fixed and dome cameras located around the college site. All cameras are recorded within the building and these are subject to monitoring and review. Recorded images can also be viewed on the any of the authorised desk top computers and are predominately viewed in the Deputy Heads and Estates Team offices. Point 3A (iv) also details who is authorised to view the system.

1.3 This policy follows Data Protection Act and GDPR guidelines.

1.4 The policy will be subject to a biennial review and to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned by the college.

Objectives of the CCTV Scheme

2.1 (a) To assist in managing the college

(b) To protect the college buildings and their assets

(c) To increase personal safety and reduce the fear of crime

(d) To assist in identifying, apprehending and prosecuting offenders

(e) To protect members of the public and private property

(f) To support the Police in a bid to deter and detect crime

(g) To monitor staff and contractors when carrying out work duties.

(h) To monitor and uphold discipline among students in line with the College Rules.

3. Statement of intent

3.1 The CCTV scheme is already registered with the Information Commissioner under the terms of the Data Protection Act 1998 and complies with the requirements both of the Data Protection Act, General Data Protection Regulations (GDPR) and the Commissioner's Code of Practice.

3.2 The system, information, documentation and recordings obtained, will be treated in accordance with the Data Protection Act and the appropriate Articles of GDPR.

3.3 Cameras will be used to monitor activities within the college and its car parks and other public areas. This is for the primary purpose of securing the safety and well- being of the college, together with its' visitors, which includes those utilising the college facilities as hirers. It is also intended to be used to identify criminal activity occurring, anticipated, or perceived, and so the positions and areas monitored (detailed in appendix 1.) reflect all of these purposes.

3.4 The cameras will not focus on private homes, gardens and other areas of private property and through the careful positioning of the cameras, minimal collateral intrusion is anticipated.

3.5 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without written authorisation being obtained from the Headteacher for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

3.6 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Copies will only be released to the media by the Headteacher for use in the investigation of a specific crime and with the written authority of the police. USBs or images sent via an email will **never** be released to the media or any other person for purposes of entertainment.

3.7 The planning and design has endeavoured to ensure that the scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.8 Warning signs, as required to be displayed by the Information Commissioners, have been placed at all access routes to areas covered by the college CCTV. The warning signs will be checked on a regular basis and any warning sign destroyed or damaged will be replaced.

3A : **GDPR**

3.A.1. To ensure compliance with GDPR a Data Protection Impact Assessment (DPIA) has been completed on the CCTV system and found to be appropriate. Advice has also been taken from the Information Commissioners and there are no significant changes to the advice already given by them with the advent of GDPR and they await any changes that may be made, once the UK Data Protection Bill has been passed through Parliament. The areas identified below have been reviewed:

i) **Signage**: Appropriate signage is already in place advising the Data Subjects of the fact there is a CCTV system used throughout the college and who has responsibility for this.

ii) **Data Access**: This remains the same and the policy details who can have access to the information contained within the CCTV system.

iii) **Data Retention**: The information is only processed for as long as its purpose requires it and this is currently under review, with extracted images deleted if no longer required. All extracted images will now be retained under Faculties – Network Support - CCTV with a Single Point of Contact (SPOC) assigned with the Network team who will have the sole responsibility of extracting the images required.

iv) **Access**: This will be restricted to the Headteacher, SLT members, Network Manager/IT Team, Estates Team and any other individual authorised by the Headteacher who will be known as 'Authorised Persons'. All these roles have legitimate reasons for being able to access the system. All other staff that require information from the CCTV system will contact an 'Authorised Persons' who will be authorised to access the system and provide the information required. Further requests to become Authorised Persons will be agreed by the Headteacher if the request meets the criteria required, namely that the use of the CCTV system will enhance their role.

v) **Authorised Persons:** The Authorised Persons will have their own individual log-in into the CCTV system and will be restricted to accessing the cameras only applicable to their role. e.g Exams officer may only access rooms/halls that have examinations in them to ensure compliance with current guidelines.

vi) **Extraction of images**: The Authorised persons will 'bookmark' the footage that they have identified from the system and they will then contact the SPOC within the Network Team responsible for extracting the data. This will be completed and the information will be made accessible only to the person requesting it, through security settings.

4. Operations of the system

4.1 The scheme will be administered and managed by the College Business Manager (on behalf of the Headteacher), in accordance with the principles and objectives expressed in this policy.

4.2 The day-to-day management will be the responsibility of both the Network Manager/IT Team and the Estates Manager. The Estates Team will have responsibility for it out of hours (including school holidays) and at weekends.

4.3 The CCTV system will be operated 24 hours each day, every day of the year.

4.4 The Network Manager/IT Team and Estates Manager will check and confirm the efficiency of the system daily (when school is in session), and in particular that the equipment is properly recording and that cameras are functional.

4.5 If the need for maintenance arises the Estates Manager will arrange this and must be satisfied of the identity and purpose of contractors before allowing entry.

4.6 Other administrative functions of the Network Manager/IT Team will include maintaining hard drive space, filing and maintaining occurrence and system maintenance logs, as necessary.

5. Monitoring procedures

5.1 Camera surveillance may be maintained at all times.

5.2 Monitors are installed in the IT Room, and in the Estates Office on which CCTV output may be continuously viewed. Access to the system can also be made on any suitable desk top computer once provided with sufficient access for Authorised Persons only.

5.3 The CCTV System is not actively or routinely monitored either during the college day or after college hours.

5.4 If covert surveillance is planned or has taken place, the Headteacher, or nominated representative, is the only person allowed to authorise such use and it must be used in accordance with the aims and objectives of the policy.

5.5 The footage is only kept for a maximum of 28 working days unless saved onto the external hard drive (at which point it will be saved for as long as the investigation is being carried out/until the matter is fully resolved)

6. Viewing footage and USB procedures

6.1 If a copy of an incident or event is recorded from the hard drive (or SD card in the case of the bus) onto a USB and in order to maintain and preserve the integrity of the USB, the following procedures for their use and retention must be strictly adhered to:

(i) Each USB must be identified by a unique mark.
(ii) A new USB must be used before recording on it
(iii) A register shall be kept of each USB recorded.
(iv) All USB's will be encrypted

6.2 If a USB is made, then this may be viewed by the Police for the prevention and detection of crime and with prior permission given by the Headteacher.

6.3 A record will be maintained of the release of USBs to the Police or other authorised applicants by the Network Manager/IT Team. Any releases **MUST** be communicated to the Headteacher.

6.4 Viewing of incident/event by the Police must be recorded in writing and in the appropriate log book. Requests by the Police can only be actioned under section 29 (3) of the Data Protection Act 1998 and Article for the purposes of:

1) The prevention and detection of crime
2) The apprehension and prosecution of offenders

6.5 USBs will only be released to the Police on the clear understanding that the USB remains the property of the college, and both the USBs and information

contained on it are to be treated in accordance with this code. The college also retains the right to refuse permission for the Police to pass to any other person the USB or any part of the information contained thereon.

6.6 The Police may require the college to retain the USB for possible use as evidence in the future. Such requests will be properly indexed and properly and securely stored in the college safe until they are needed by the Police.

6.7 Applications received from outside bodies (e.g. solicitors or hirers) to view CCTV footage or release USBs, will be referred to the Headteacher. In these circumstances, either viewing the footage or compiling a USB or saving an image will normally only be allowed or released where satisfactory documentary evidence is produced showing that they are required for either legal proceedings, they are part of a subject access request, or are in response to a Court Order.

A fee can be charged in such circumstances: £10 for subject access requests; sum not exceeding the cost of materials in other cases.

7. Breaches of the code (including breaches of security)

7.1 Any breach of this policy by college staff will be initially investigated by the Headteacher (or duly nominated person), in order for them to take the appropriate disciplinary action.

7.2 Any serious breach of this policy will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

8. Assessment of the scheme and code of practice

8.1 Performance monitoring, including random operating checks, may be carried out by the Network Manager/IT Team, the Estates Manager or other person directly authorised by the Headteacher.

9. Complaints

9.1 Any complaints about the college's CCTV system should be addressed to the Headteacher.

9.2 Complaints will be investigated in accordance with section 8 of the Information Commissioners Code of Practice, which is to be read in conjunction with this policy.

10. Access by the Data Subject

10.1 The Data Protection Act and Article 15 of GDPR provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

10.2 Requests for Data Subject Access should be made to the Headteacher.

11. Public information

11.1 Copies of this Policy will be available to the public via the college website.

12. Legal Requirements

12.1 The use of CCTV at Archbishop Beck College has already been registered with the Information Commissioner in compliance with the Data Protection Act and GDPR advice.

12.2 Signs have been placed at each block entrance to the college, stating that CCTV is in operation and advising as to who operates the system and a contact number.

12.3 In addition to this, smaller signs indicating the use of CCTV have been installed around the college.

Summary of Key Points

- This policy will be reviewed every two years.
- The CCTV system is owned and operated by the college.
- The system will *not* be *actively* monitored either during the college day or out of college hours, as there is no dedicated CCTV Operator employed.
- USBs will be used properly, indexed, stored and destroyed after appropriate use.
- USBs and hard drive footage may only be viewed by persons authorised by the college or other appropriate authority.
- USBs required as evidence will be properly recorded, witnessed and packaged before copies are released to the Police.
- USBs will not be made available to the media for commercial or entertainment purposes.
- USBs will be disposed of securely by incineration/shredding.
- Any covert surveillance or use of a Covert Human Intelligence Source (CHIS) being considered or planned as part of an operation must comply with any corporate policies and procedures. However further legal advice should be obtained prior to undertaking any covert operation utilising the CCTV system.
- Any breaches of this code will be investigated by the Headteacher, or other member of staff assigned by the Headteacher if not the Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Headteacher.

Appendix 1

CCTV Locations

EXTERNAL CAMERAS

	Camera Name
1	1st Muga Playground
2	3G Entrance
3	3G Pitch Seating
4	3G Pitch
5	Bike Area 1
6	Bike Area 2
7	Bike Area 3
8	Car Park PTZ
9	East Ext
10	Front Entrance South
11	Main Entrance PTZ
12	Muga by 3G
13	North Kitchen Ext
14	Northside Rear
15	PE Outside Entrance
16	Pedestrian Gate
17	Rear Mid Playground
18	Side PTZ
19	3G PTZ
20	Student Entrance
21	Westside Front Car Park

22	Westside Front Rear

INTERNAL CAMERAS

Ground Floor

	Camera Name
1	Reflection Room
2	Student Serv Seating Area
3	Main Student Entrance
4	Main Reception
5	PE Entrance 2
6	PE Entrance 3
7	Library
8	ICT Corridor
9	Canteen LHS
10	Canteen RHS
11	Canteen Middle
12	Coffee Shop Area
13	Drama Area
14	Front Meeting Room
15	Male WC
16	Outside SD Office
17	Dinner Line
18	DT Area 1

First Floor

	Camera Name
1	LSSP Corridor
2	1st Floor West
3	English Corridor North
4	English Eastside
5	English Eastside Corridor
6	English Seating Area
7	History Seating Area

8	Languages Area
9	1st Floor Languages Seating
10	LRC
11	Inclusion
12	RE > Humanities Corridor
13	RE Computer Area

Second Floor

	Camera Name
1	6th Form Link 1
2	6th Form Link 2
3	6th Form
4	Atrium Looking South
5	ICT Area South
6	ICT Towards Maths
7	Southside Top Corridor
8	Northside Maths Corridor Top
9	Maths Seating Area
10	Science 9 Corridor
11	Science 3 Area South
12	6th Form From Science 9

Stairwells

	Camera Name
1	1st East Link
2	1st Floor East Stairs
3	1st Floor Link Northside
4	1st Floor South
5	1st Floor West Link
6	1st Floor West Stair
7	2nd Floor Link Corridor
8	2nd Floor Top South
9	Bottom Stairs West
10	East Link Corridor Ground
11	Ground Floor Stairs
12	Ground Floor West
13	North Bottom Staff
14	North Stairs 1st Floor
15	North Top Stairs
16	Northside Bottom Stair
17	South Ground
18	South Stair 1st Floor
19	South Top Floor
20	Southside Bottom Stairs
21	Top Floor East Link
22	Top Stairs East
23	Top West Link Corridor
24	Top Westside Stairs
25	East side GF
26	West side GF
27	North side GF
28	South side GF