



The Chalfonts Community College

CCTV Policy

2022-2023

Approved by: RFL Committee **Date:** 22 March 2022

Last reviewed on: March 2022

Next review due by: September 2023

Contents

1. Statement of Intent	3
2. Legal Framework	3
3. Operation of the system.....	4
4. System functionality & Access.....	4
5. Recordings.....	5
6. Breaches of the code (including breaches of security).....	5
7. Complaints	5
8. Access by the Data Subject.....	5
History	5

1. Statement of Intent

At The Chalfonts Community College, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members, and to monitor any unauthorised access to our site.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- i. We comply with all data protection legislation, including the Data Protection Act 2018.
- ii. The images that are captured are useable for the purposes we require them for.
- iii. We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- i. Observing what an individual is doing
- ii. Taking action to prevent a crime
- iii. Using images of individuals that could affect their privacy.

2. Legal Framework

This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

- i. The Regulation of Investigatory Powers Act 2000
- ii. The Protection of Freedoms Act 2012
- iii. The General Data Protection Regulation (GDPR)
- iv. The Data Protection Act 2018
- v. The Freedom of Information Act 2000
- vi. The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- vii. The Freedom of Information and Data Protection (Appropriate Limit and
- viii. Fees) Regulations 2004
- ix. The School Standards and Framework Act 1998
- x. The Children Act 1989
- xi. The Children Act 2004
- xii. The Equality Act 2010.

3. Operation of the system

The CCTV system is a closed digital system and is administered and managed by the IT Support team.

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

Recordings are stored on hard drives for 14 days and are wiped at expiry or retained for investigatory purposes if required.

Warning signs have been placed throughout the premises where the CCTV system is active.

The CCTV system will not be trained on individuals unless an immediate response to an incident is required.

The CCTV system will not be trained on private vehicles or property outside the perimeter of the school.

Be used only for the purposes for which it is intended, including supporting public safety, protection of students, staff and law enforcement.

4. System functionality & Access

IT Support will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

Access to the CCTV system will be strictly limited to named CCTV Operators as below:

- i. Caroline Whitehead, Principal
- ii. Victoria Lang, Vice Principal
- iii. Grant Wolpert, Director of Finance & Operations
- iv. Tina Borer, Behaviour Manager
- v. Maria Byrne, CCTV Operator
- vi. Steve Andrews, Site Manager
- vii. Chris Park, Assistant Site Manager
- viii. IT Support team, including Trident
- ix. Richard Smith, Assistant Principal
- x. John Quesnell, Heidi Loveland, Amanda Irvine, Jamie Howard & Stewart Charge, Year Leaders

Visitors and other contractors wishing to enter areas of work where images are being displayed will be subject to particular arrangements as outlined below.

- i. Operators must satisfy themselves over the identity of any other visitors who view images and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be logged and signed off before recordings are viewed.
- ii. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

5. Recordings

Recordings exported from the CCTV system can only be stored in the 'Restricted Drive'. Indexed and date stamped. Images/recorded data can only be viewed with authorised consent of those staff noted and recorded within the CCTV register.

Recordings will only be released following submission of a completed request form on the authority of the Principal, then only to the Police or as required under a Subject Access Request.

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

Any breach of the Code of Practice by school staff will be initially investigated by the Principal, in order for them to take the appropriate disciplinary action.

Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

7. Complaints

Any complaints about the school's CCTV system should be addressed to the Principal.

8. Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made to the Data Protection Officer in line with the Data Protection Policy.

History

Date	Issue	Status	Comments
November 2020	1		Policy Created
March 2022	2	Amendments	Updated CCTV Operators

