BLUE COAT C E (AIDED) INFANT AND JUNIOR SCHOOLS' FEDERATION

CCTV and Audio Recording Policy

Contents

Introduction

The Purpose of this policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television). The Federation is fully committed to ensuring the safety and wellbeing of its staff, pupils, visitors, and contractors. To support this commitment, we have invested in the security and safety of our buildings and facilities, including the use of CCTV systems.

We recognise that while CCTV can be an effective tool for enhancing security, it may also be perceived as intrusive to privacy. Therefore, we are dedicated to using such systems responsibly and in accordance with relevant legislation and guidance.

This policy will be reviewed regularly to ensure it remains fit for purpose. In addition, any time new equipment is introduced, a full review and risk assessment will be conducted. As a minimum, we aim to review this policy every two years.

1. Aims

This policy outlines the Federation's approach to the operation, management, and use of surveillance and closed-circuit television (CCTV) systems across school premises. The Federation is committed to ensuring that CCTV is used responsibly, proportionately, and in accordance with legal and ethical standards.

Statement of intent

The primary purpose of the CCTV system is to support the Federation in achieving the following objectives:

- Safeguard individuals: Protect pupils, staff, visitors, and contractors from harm to their person or property.
- Enhance safety: Promote a sense of personal security and reduce the fear of crime, abuse, or intimidation.
- Protect assets: Safeguard Federation buildings and property from intrusion, vandalism, damage, or disruption.
- reduce the incidence of crime and anti-social behaviour (including theft and vandalism)
- preventing bullying
- Support law enforcement: Assist police efforts to deter, detect, and gather evidence of criminal activity.
- Identify offenders: Aid in the identification, apprehension, and prosecution of individuals involved in unlawful acts.
- Investigate incidents: Help determine the cause of accidents or adverse events and prevent recurrence.
- Manage facilities: Support the day-to-day security and operational management of Federation buildings.
- Provide evidence: Supply visual documentation for internal disciplinary procedures involving staff or pupils.

2. Use and Compliance

The CCTV system is registered with the Information Commissioner's Office (ICO), and renewal dates are recorded and monitored. The Federation is committed to full compliance with:

- The **Data Protection Act 2018**
- The **UK General Data Protection Regulation (UK GDPR)**
- The **ICO's CCTV Code of Practice**

The CCTV system is owned and operated by the School, the deployment of which is determined by the School's leadership team.

2.1 Limitations of Use

The CCTV system will *not* be used to:

- Infringe upon an individual's right to privacy
- Monitor individuals in areas with a heightened expectation of privacy (e.g., toilets, changing rooms)
- Track individuals unless responding to an active emergency or incident
- Serve any purpose beyond those explicitly stated in this policy

Our camera placement is designed to maximise coverage. However, the Federation acknowledges that not all incidents can be guaranteed to be captured. While the listed uses are comprehensive, other relevant purposes may emerge and will be assessed in line with legal and ethical standards.

2.2 Data Handling and Disclosure

CCTV footage will never be used for commercial purposes. The system is operated solely for safeguarding, security, and incident investigation within the Federation.

In rare circumstances, law enforcement may request footage for media release. The Federation will only comply with such requests upon receipt of formal written authorisation, and solely to assist in the investigation of a specific crime.

All recorded footage must be of sufficient quality to support identification and legal proceedings, if required. The integrity and clarity of recordings are essential for their admissibility and usefulness in any formal investigation.

3. Relevant Legislation and Guidance

This policy is informed by a comprehensive framework of legislation and statutory guidance to ensure the responsible and lawful use of CCTV systems within the Federation. It aligns with the principles of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other relevant safeguarding and privacy standards.

3.1 Legislation

The operation of CCTV systems is governed by the following legal instruments:

Legislation	Purpose / Relevance
UK General Data Protection Regulation (UK GDPR)	Governs the processing of personal data, including CCTV footage.
Data Protection Act 2018	Supplements UK GDPR and outlines specific provisions for data handling.
Human Rights Act 1998	Protects the right to privacy under Article 8.
European Convention on Human Rights	Provides broader human rights protections,

	including privacy and dignity.
Regulation of Investigatory Powers Act 2000	Regulates surveillance and investigatory powers.
Protection of Freedoms Act 2012	Introduced specific provisions for the regulation of CCTV and biometric data.
Education (Pupil Information) (England) Regulations 2005 (amended 2016)	Governs the handling and sharing of pupil information.
Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004	Sets limits and fees for data access requests.
School Standards and Framework Act 1998	Establishes standards for school governance and pupil welfare.
Children Act 1989 & Children Act 2004	Provides the legal framework for safeguarding and promoting the welfare of children.
Equality Act 2010	Ensures non-discriminatory practices in the use of CCTV and other school operations.

3.2 Guidance

Surveillance Camera Code of Practice (2021) Issued under the Protection of Freedoms Act 2012, this code outlines principles for the appropriate use of surveillance camera systems, including transparency, accountability, and proportionality.

4. Definitions

To ensure clarity and shared understanding throughout this policy, the following terms are defined:

Surveillance: The act of observing individuals or locations for the purpose of monitoring activity, ensuring safety, or gathering information.

CCTV (Closed-Circuit Television): A system of video cameras used for surveillance purposes. Unlike broadcast television, CCTV footage is transmitted to a limited set of monitors or recording devices.

Covert Surveillance: The use of surveillance equipment in a manner that individuals are unaware they are being monitored. This type of surveillance is only permitted under exceptional circumstances and must comply with legal and ethical standards.

Covert surveillance refers to the use of monitoring equipment in a manner that individuals are unaware they are being observed. The Federation recognises that such surveillance is highly intrusive and will only be considered in exceptional circumstances.

Covert monitoring may be authorised when there is reasonable suspicion of a criminal offence, upon police advice for the prevention or detection of crime, or where there is a significant risk to public safety. Any decision to implement covert surveillance must be proportionate, justified, and compliant with legal and ethical standards, including data protection and human rights legislation.

5. Staff Monitoring

CCTV footage will **not** be used to monitor staff performance, evaluate teaching quality, or assess lesson delivery. The system is in place solely for safeguarding, security, and incident investigation purposes.

Any use of CCTV footage involving staff will be in line with data protection legislation and only where necessary for safety, legal compliance, or disciplinary procedures following a reported incident. The Federation is committed to respecting the privacy and professional integrity of all staff members.

6. Legal Compliance and Authorisation

Prior to any covert surveillance activity, a **Data Protection Impact Assessment (DPIA)** will be conducted to ensure compliance with the **Data Protection Act 2018** and **UK GDPR**.

Where required, formal authorisation **will** be obtained from the Home Office, and all relevant documentation will be completed and securely retained.

The Federation is committed to ensuring that covert surveillance is used only when absolutely necessary, and always in accordance with legal, ethical, and safeguarding standards.

6.1 Location of Cameras (See Appendix 4)

CCTV cameras are installed in areas that require monitoring to support the objectives outlined in **Section 1.1** of this policy. Their placement is designed to enhance safety, protect property, and support the day-to-day management of the Federation's facilities.

Cameras are currently located in the following areas (subject to periodic review):

- Main entrance and exit points
- Corridors and stairwells
- Playgrounds and outdoor recreational areas
- Perimeter gates and fencing
- Car parks and drop-off zones
- Reception and administrative areas
- Storage and utility zones
- General communal areas (excluding toilets and changing rooms)

6.2 Signage and Visibility

In accordance with the Information Commissioner's Office (ICO) Code of Practice, appropriate signage is displayed wherever CCTV cameras are in operation. These signs:

- Clearly identify the Federation as the operator of the CCTV system
- State the Federation's role as the data controller
- Provide contact details for further information or data access requests

7. Roles and responsibilities

7.1 The governing board

The Governing Board holds ultimate responsibility for:

- Ensuring the CCTV system is operated in accordance with this policy
- Overseeing compliance with all relevant legislation outlined in Section 2.1
- Supporting strategic decisions regarding CCTV usage and expansion

7.2 The Executive Headteacher

The Executive Headteacher is responsible for the day-to-day leadership and strategic oversight of the CCTV system. Duties include:

- Managing the operation and use of the CCTV system
- Liaising with the Data Protection Officer (DPO) to ensure usage aligns with policy aims and legal requirements
- Ensuring staff follow the guidance set out in this policy
- Reviewing the CCTV policy to maintain legal compliance
- Ensuring authorised personnel receive appropriate training from the DPO
- Approving any upgrades or expansions to the system following a Data Protection Impact Assessment (DPIA)
- Deciding, in consultation with the DPO, whether to comply with third-party disclosure requests

7.3 The data protection officer (DPO)

The DPO ensures the Federation's CCTV practices comply with data protection law. Responsibilities include:

- Training authorised users in system operation and data protection
- Training staff to recognise and respond to Subject Access Requests (SARs)
- Handling SARs in accordance with UK GDPR and the Data Protection Act 2018
- Monitoring ongoing compliance with data protection legislation
- Advising on and conducting DPIAs
- Acting as the point of contact for the Information Commissioner's Office (ICO)
- Ensuring footage is obtained lawfully, stored securely, and destroyed after the retention period
- Maintaining accurate records of data processing activities and making them available upon request
- Informing individuals of their rights and how their data is used
- Ensuring CCTV systems produce high-quality footage suitable for identification
- Preventing infringement on individuals' reasonable expectations of privacy
- Conducting termly audits of footage storage and deletion practices
- Reviewing and responding to third-party access requests

7.4 The system manager

The System Manager oversees the technical operation and maintenance of the CCTV system. Responsibilities include:

- Managing daily functionality and upkeep of the system
- Ensuring the security of the system and stored footage
- Conducting termly checks for faults and vulnerabilities

- Verifying the accuracy of date and time stamps on recordings

7.5 Administration staff

Administration staff support the secure and transparent use of CCTV by:
Recording all visitor access in a system log book, including:

- Date and time of access
- Details of footage viewed
- Purpose of access

8. System Operation

The Federation's CCTV system is designed to operate continuously and reliably to support the safeguarding and security objectives outlined in this policy.

The CCTV system is operational 24 hours a day, 365 days a year, including weekends and holidays.

The system is registered with the Information Commissioner's Office (ICO) **in** accordance with data protection legislation.

8.2 Audio and Visual Recording

The system is configured to record both visual footage and audio in designated areas (reception offices).

Audio recording is used to enhance safety and incident investigation, and will only be active in areas where individuals have been clearly informed of its presence.

Signage at entry points and monitored zones will clearly state that audio and video (See appendices 1 and 2) recording is in operation, in line with transparency requirements under the UK GDPR and Data Protection Act 2018.

8.3 Timestamp Accuracy

All recordings will include **date and time stamps** to support accurate documentation and potential legal use.

The **System Manager** will verify the accuracy of these timestamps:

- **Termly**, as part of routine system checks
- **When clocks change**, to ensure alignment with daylight saving adjustments

9. Storage of CCTV Footage

The Federation is committed to ensuring that CCTV footage is stored securely, retained appropriately, and disposed of in accordance with data protection legislation.

9.1 Retention Period

CCTV footage will be retained for a standard period of 30 days. After this period, the system will automatically overwrite the footage to prevent unnecessary data accumulation and ensure compliance with data minimisation principles.

9.2 Extended Retention

In specific circumstances, footage may be retained beyond the standard 30-day period. This may occur when a law enforcement agency is investigating a crime and requires access to footage as part of an active investigation. Any extended retention will be fully documented and justified in accordance with data protection principles and the Federation's safeguarding responsibilities.

9.3 Data Security and Integrity

Recordings intended for evidential use will be downloaded and encrypted to ensure the security of the data, the integrity of the footage, and its admissibility in legal or disciplinary proceedings. These measures are essential to maintain the chain of custody and protect the rights of all individuals involved.

9.4 Monitoring and Compliance

The Data Protection Officer (DPO) will conduct termly checks to ensure that footage is being stored securely and accurately, that it is being deleted in line with the retention schedule, and that the system remains compliant with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

10. Access to CCTV Footage

Access to CCTV footage is strictly controlled to ensure privacy, security, and compliance with legal obligations.

10.1 Authorised Access

Access will only be granted to authorised personnel for the purposes outlined in Section 1.1, or where there is a lawful reason to view the footage.

All access must be proportionate, justified, and in line with the Federation's safeguarding and data protection responsibilities.

10.2 Access Logging

Individuals accessing CCTV footage must record the following details in the **access log**:

- Full name
- Date and time of access
- Reason for access

10.3 Monitor Placement

Visual display monitors will be positioned to ensure that only authorised personnel can view the footage.

Monitors will not be placed in public or shared areas where unauthorised viewing could occur.

11. Downloading Captured Data Onto Other Media

To preserve the integrity of CCTV data and ensure its admissibility in legal proceedings, all downloads from the system must follow strict protocols.

11.1. Evidential Protocols

To preserve the integrity of CCTV data and ensure its admissibility in legal or disciplinary proceedings, all downloads from the system must follow strict protocols.

11.2 Preparation and Identification

Each piece of download media, such as a USB drive or DVD, must be clearly marked with a unique identifier. Before use, the media must be cleaned of any previous recordings to prevent data contamination.
The System Manager is responsible for recording the date and time the media is inserted into the system, along with the reference number assigned to the download media.

11.3 Evidential Handling

Download media required for evidential purposes must be sealed, witnessed, and signed by the System Manager. It must also be dated and stored securely in the designated evidence store.
If the media is not copied for police use prior to sealing, a copy may be made at a later time. However, once copied, the media must be resealed, witnessed, signed, dated, and returned to the evidence store to maintain its evidential integrity.

In cases where download media is archived, its reference number must be recorded and indexed appropriately to ensure traceability and compliance with data handling standards.

11.3 Access and Approval

Before any data or images are released, a Data Access Form must be completed and submitted to the Executive Headteacher for approval.

Images may be viewed by:

- **The System Manager:** Mr. D. Anson
- **The Executive Headteacher:** Mr. A. Orlik
- **The Deputy Executive Headteachers:** Mrs. L. Adlington-McArthur and Mr. D. Matthews
- **The DPO:** Mrs. L. Adlington-McArthur
- **School Business Manager:** Mrs. L. Mosedale
- **The police**: for the prevention and detection of crime

The Federation is committed to maintaining high standards of accountability and ensuring that all staff act in accordance with the law and the values of the school community.

*Note: Where an authorised individual may later be called as a witness to an offence, and the footage may be used as evidence, it is preferable that they **withhold viewing** until requested by the police.*

11.4 Disclosure and Ownership

A detailed record will be maintained of any viewing or release of download media to the police or other authorised applicants. If images are required as evidence, a copy may be released to the police under the procedures outlined in this policy. However, the download media and its contents remain the property of the Federation at all times. All media must be handled in accordance with data protection legislation to ensure privacy, security, and legal compliance.
The Federation retains the right to refuse permission for the police to share footage with third parties. If a Court requires the release of footage, it will be produced from the secure evidence store, sealed and intact, to preserve its evidential integrity.

11.5 Retention for Legal Purposes

The police may request the Federation to retain download media for potential future use as evidence. In such cases, the media will be properly indexed and securely stored until it is formally requested. This ensures that all evidential material is preserved in accordance with legal standards and data protection requirements.

11.6 Requests from External Bodies

Applications from external parties—such as solicitors or parents—seeking to view or obtain CCTV footage will be referred to the Data Protection Officer (DPO). Each request will be reviewed and decided upon by a senior leader in consultation with the DPO.
All decisions regarding external access to footage will be made in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Federation's safeguarding responsibilities. The Federation is committed to ensuring that all disclosures are lawful, justified, and respectful of the privacy rights of individuals.

12. Subject access requests (SAR) (See Appendix 3)

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, individuals have the right to request access to CCTV footage in which they appear. Upon receiving SAR the school will immediately issue a receipt and will then respond within one calendar month of receipt.

To assist in locating relevant footage, individuals making a SAR should inform the DPO in writing and provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage. Footage that identifies other individuals will be obscured (e.g. blurring or redaction). Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage.

The school reserves the right to refuse a SAR if, for example, the release of the footage to the subject would prejudice an ongoing investigation and/or repetitive, unfounded, or excessive (a reasonable fee may be charged in such cases). Individuals can find more information about their rights and the SAR process on the Information Commissioner's Office (ICO) website.

12.1 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the headteacher and/ or the DPO to an email address that will be supplied at the time of request.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

13. Data Protection Impact Assessment (DPIA)

The Federation is committed to the principle of privacy by design, ensuring that privacy considerations are embedded into every stage of the CCTV system's lifecycle—from initial deployment to replacement, development, and upgrading. Privacy is considered at every stage of system planning and operation to ensure that surveillance remains justifiable, necessary, and proportionate.

A Data Protection Impact Assessment (DPIA) will be carried out:

- Whenever the CCTV system is replaced, developed, or upgraded
- Annually, as part of routine privacy and compliance reviews
- Whenever new cameras are installed or existing cameras are repositioned

14. Security

The Federation is committed to maintaining the security and integrity of its CCTV system and the data it captures.

The System Manager is responsible for overseeing the security of the CCTV system and its footage. The system will be checked for faults once per term, and any issues will be reported immediately and repaired promptly following established procedures.

Footage will be stored securely, encrypted wherever possible and password protected.

All camera operation equipment will be locked away securely when not in use.

Cybersecurity measures will be implemented to protect against unauthorised access and cyber-attacks.

Software updates, especially those related to security, will be applied as soon as they are released by the manufacturer.

15. Grievances and Complaints

Complaints regarding the CCTV system or its operation should be directed to either:

- The Headteacher, or
- The Data Protection Officer (DPO)

All complaints will be handled in accordance with the Federation's Complaints Policy.

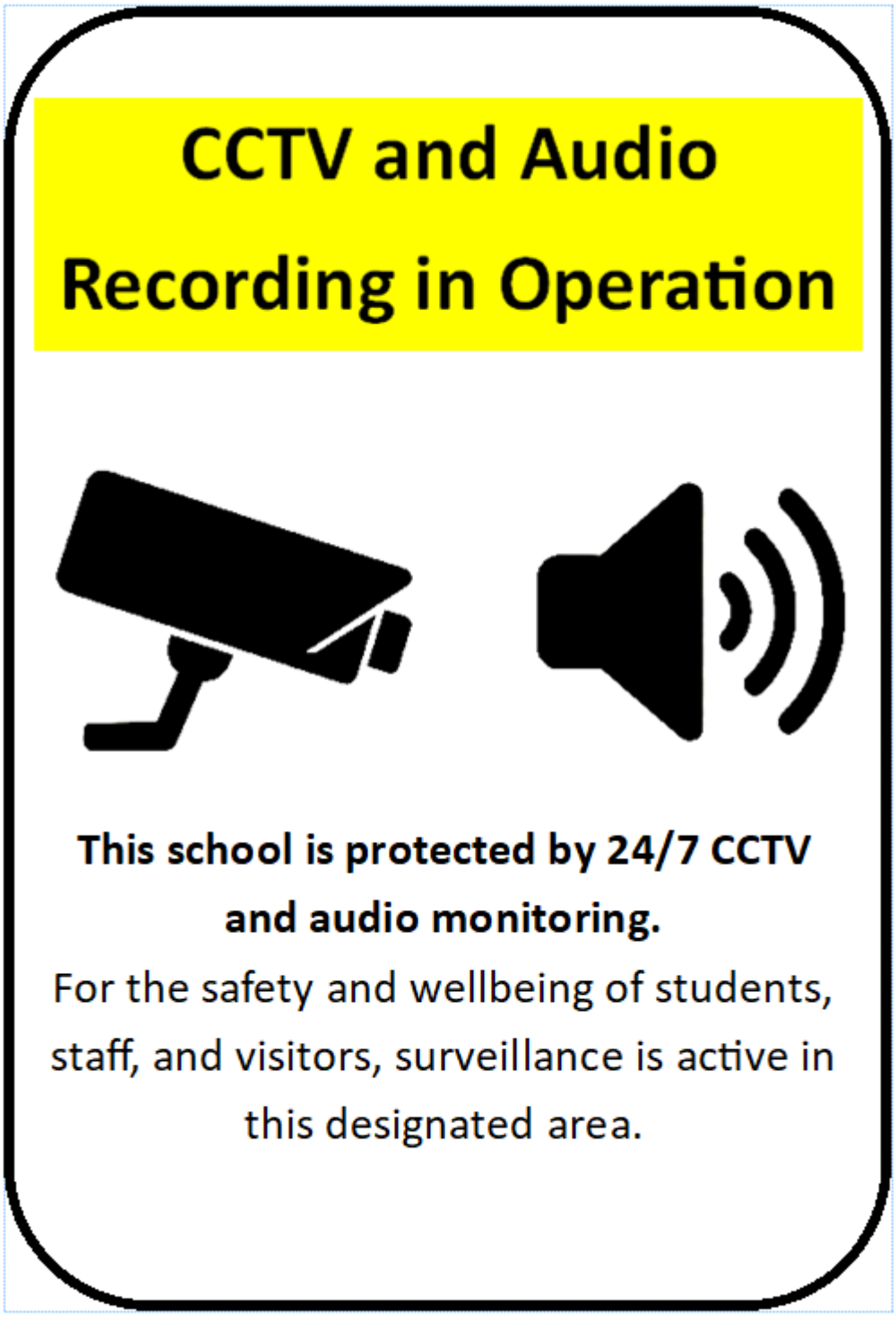
16. Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

17. Links to other policies

- Data protection policy (GDPR)
- Biometric data policy
- Privacy notices for parents/carers, pupils, staff, governors and suppliers
- Safeguarding policy

Appendix 1: Signage to notify public of CCTV and audio recording



Appendix 2: Signage to notify public of CCTV recording in operation

CCTV
in Operation

This school is protected by 24/7 CCTV monitoring.

For the safety and wellbeing of students, staff, and visitors, surveillance is active in designated areas.

(Appendix 3) Subject Access Request

FAO: Blue Coat Infant and Junior Schools Federation (G-DRP) Data Protection Officer

Please provide me with the information about me that I am entitled to under the General data Protection Regulation.

This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Your name:	
Date of birth:	
Child's name (if applicable):	
Relation with the Federation. (Please select) Other (please specify):	Pupil/Parent/Employee/Governor/Volunteer
Home address:	
Post Code:	
Contact number:	
Email address:	
Details of the information requested: Insert details (In box on the right) of the information you require. Please be as precise as possible, for example: • Your personnel file (staff) • Your child's medical records • Your child's behaviour record • Other (explain clearly what information you require)	Please provide me with:
Time period Give a date range of the information you are requesting, eg 'From 1 April 2022 to 31 March 2023'. Give times if they're relevant, eg 2-3pm for CCTV footage, or say what time the call started if you're requesting a phone call transcript	
Reason:	
Other details that will help the organisation find the information	

If you need any information from me, please let me know as soon as possible. The data controller **cannot charge a fee** for providing this information unless:

- The request is **manifestly unfounded or excessive**, or
- You request **additional copies** of the same information.

The controller must respond **within one month** of receiving your request.

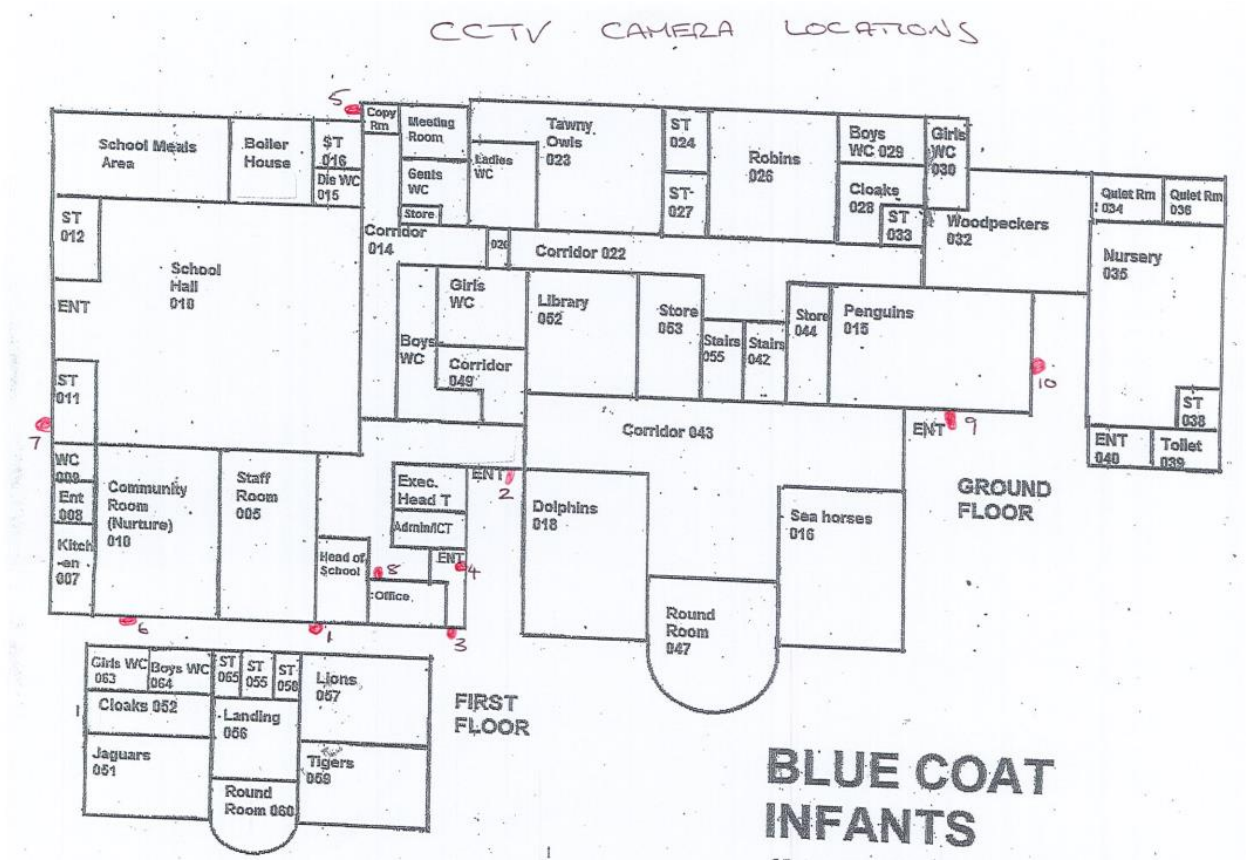
This period can be extended by **two further months** if the request is complex or numerous—but they must inform you and explain why.

If you need any advice on dealing with this request, you can contact the information commissioner's Office

on 0303 123 1113 or @ www.ico.org.uk

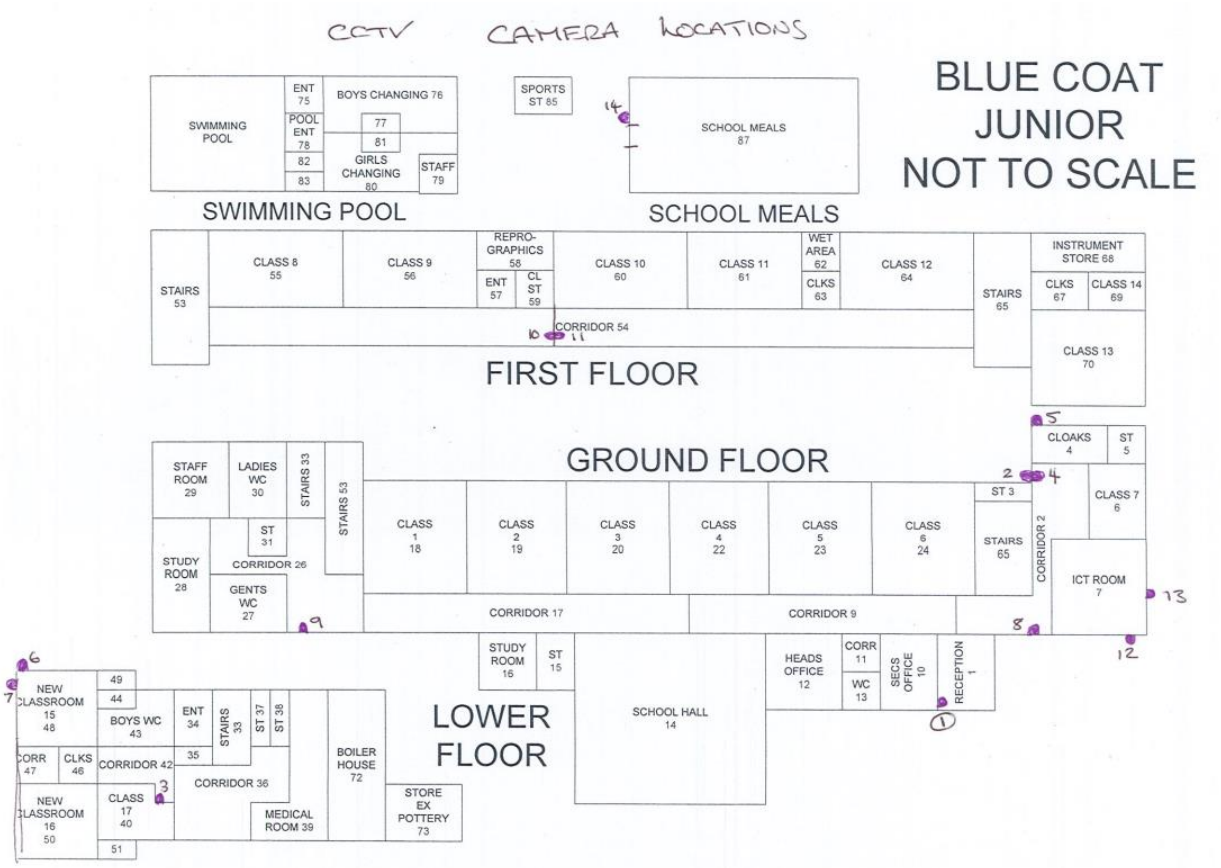
Appendix 4: Location of CCTV

The Closed-Circuit Television cameras are located in the flowing areas of Blue Coat C E Junior School:



1. Carkpark 1
2. Side Entrance
3. Front Entrance (with Audio)
4. Reception
5. Boiler House
6. Carpark 2
7. Rear playground
8. Corridor (Main hall)
9. Year 2 Entrance
10. Nursery Entrance

The Closed-Circuit Television cameras are located in the flowing areas of Blue Coat C E Junior School:



1. Reception/ Office (with audio recording)
2. Entrance to boys' toilets
3. Entrance to girls' toilets
4. Playground (climbing frame)
5. Playground (facing SRP and Peace Garden)
6. Pool Street Gate/ Lower Playground
7. Near Stairwells (Blossom Room
8. Far Stairwells/ Staffroom
9. Year 6 corridor
10. Year 5 corridor
11. Front carpark 1
12. Front carpark 2
13. Canteen entrance