Part 1

Name of policy	**B4 Use of CCTV and Biometric Technology**
Status of policy	This is a non-statutory policy
Consultation	This policy has been developed following consultation with Senior Leadership Team and Buildings Committee Governors**.**
Relationship with other policies	This policy should be read in conjunction with: **B1 Health and Safety policy** **P4 Safeguarding and Child Protection policy** **CP1 Corvus Learning Trust (CLT) Data Protection policy**
Date policy was agreed	5th February 2024
Date for full implementation	Immediate
Date for review	Every two years: February 2026

This policy has been written with reference to:

- The Data Protection Act 2018 (DPA)
- Information Commissioner's Office CCTV Code of Practice
- Surveillance Camera Commissioner Code of Practice
- Protection of Freedoms Act 2012
- Department for Education Biometrics Guidance July 2022

Part 2

CCTV Policy

1. The Governing Body believes that the use of CCTV can play a legitimate role in creating and maintaining a safe and secure environment for students, staff and visitors. However, we acknowledge that the use of CCTV carries privacy and data protection implications and the impact on the rights of data subjects. This policy sets out our commitment to complying with our legal obligations and ensuring that the rights of data subjects are respected.

2. The controller and operator of the CCTV scheme are:

   Controller: Edgbarrow School of Corvus Learning Trust
   Contact email: secretary@edgbarrowschool.co.uk
   Telephone: 01344 772658
   Address: Grant Road, Crowthorne, Berkshire, RG45 7HZ

3. Day-to-day management responsibility for deciding what information is recorded, how it is used and who can access it is delegated to the head teacher and senior leadership team.

4. Day-to-day responsibility for operational maintenance of the cameras and security of the equipment has been delegated to the facilities manager and IT support.

5. The Data Protection Officer is:

Data Protection Officer: Data Protection Education Ltd.
Contact email: dpo@dataprotection.education
Telephone: 0800 0862018
Address: Unit 1 Saltmore Farm, New Inn Rd, Hinxworth, Hertfordshire, SG7 5EZ
Data Protection Education Ltd

6. This policy is guided by the Surveillance Camera Commissioner's Code of Practice (as required under the Protection of Freedoms Act 2012).

7. Misuse of CCTV data will be a disciplinary matter and may also constitute a criminal offence.

   Any breach of the policy or code of practice by School staff will be initially investigated by the Headteacher in order for them to take the appropriate disciplinary action.

8. Compliance with the Data Protection Act CCTV Code of Practice is the responsibility of all designated users of the CCTV system. All staff will be aware of, and comply with, the Edgbarrow School codes of practice for the use of CCTV.

Purpose

9. We use CCTV in and around our site only for legitimate purposes.

   Cameras may be used to monitor activities within the School grounds and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the School's students, staff and visitors.

In particular, we use CCTV:

A. for the safety and security of students, staff and visitors, including users of the sports centre and external hirers of facilities
B. to protect buildings and assets from damage, disruption, vandalism and other crime
C. to support law enforcement bodies in the prevention, detection and prosecution of crime
D. to assist in the defence of any civil litigation, including employment tribunal proceedings
E. to manage and support the ingress of vehicles/pedestrians onto site

Cameras are used for both recordings of data and live monitoring. Where live monitoring is available, we take steps to ensure that there is controlled access to live monitors to authorised members of staff only.

The CCTV system will NOT be used:

A. to record sound
B. for any automated decision taking; or
C. monitoring private and/or residential areas or premises
D. for covert surveillance, unless there are exceptional circumstances where the surveillance is required for investigating a crime or equivalent malpractice, when notifying individuals about the monitoring would prejudice its prevention or detection. See section 19.

Locations of cameras

10. Cameras will only be located in positions that are required for the identified purposes. CCTV cameras will be positioned or masked to prevent monitoring and recording of any external private property.

CCTV may monitor the following locations 24 hours a day, 7 days a week:

A. Points of entrance onto the site
B. Points of entrance into the buildings
C. Playgrounds and carparks
D. Communal areas and corridors
E. Communal sports facilities in the sports centre, such as the gym/weights room

Signage is displayed at all points of entry on site and at points of entry into areas where cameras are present.

Retention

11. Data will be kept no longer than necessary, after which it is automatically deleted permanently. No backups are available. Our standard retention period is 30 days.

12. Where the data is extracted and required for other legal purposes (e.g., investigation of a crime), data will be kept as long as required for that purpose. Each such instance will be recorded.

    In this case, appropriate organizational and technical measures must be taken to ensure the security and integrity of the data. These may include, but are not limited to:
    - Storing recordings in a secure location
    - Limiting access to the recordings
    - Giving recordings a unique identifier for future reference
    - Updating records when the recordings are accessed
    - Ensuring recordings are deleted when they are no longer required for the stated purpose
    - Following any additional security steps required by an external agency, such as complying with police advice on handling evidence

Access to CCTV data

13. The CCTV monitoring will be restricted to authorised members of staff only. Authority will be given by the Headteacher.

14. Access to CCTV images can only be used in support of a defined legitimate purpose and not for any other routine purpose.

15. When access is requested and is to be viewed by anyone other than the delegated person responsible, it must be authorised by the delegated authority and documented.

16. Any CCTV footage will be viewed in a secure location.

17. Exemptions, as described in the ICO guidelines may be applied to any data disclosure.

Criminal Proceedings

18. CCTV data will be disclosed to the Police or other agencies only where a clear legal obligation to do so has been identified and appropriate documentation (usually a Disclosure Request Form provided by the requesting agency) received under Schedule 2, Part 1 Paragraph 2, of the Data Protection Act 2018 (previously S29 of the Data Protection Act 1998).

    Once this information has been disclosed it is noted that the receiving party becomes the data controller

Covert surveillance

19. Covert surveillance will only be considered where the surveillance is required for investigating a crime or equivalent malpractice, when notifying individuals about the monitoring would prejudice its prevention or detection.

    Before any covert surveillance takes place:

    - The Headteacher and the governors will define the scope of the surveillance, following advice from the Trust data protection and legal teams and in line with the latest guidance from the ICO.

      The scope should include the purpose, data subjects, location and coverage, disclosure rules, and time limitations of the surveillance
    - The data protection lead will carry out a Data Protection Impact Assessment
    - The governors will carry out a balancing test to determine why the surveillance needs of the School outweigh the rights of the data subject(s) in question
    - The scope, DPIA and balancing test will be verified by the Trust data protection and legal teams to ensure the surveillance is lawful

Subject Access Requests

20. Data subjects may ask for copies of their data under their right of access under the Data Protection Act 2018 and will be handled as per the Subject Access Request Procedure.

    Where a request for CCTV data is made, we require information on the time, date and place of the images. Information may be provided as still images or video, with or without redaction as deemed necessary. On occasions, requests may be actioned by asking the data subject to view the data directly.

Monitoring and review

21. This policy will be reviewed every two years, or when changes are proposed to the CCTV system

22. Any changes to the CCTV system will be preceded by a data protection impact assessment (DPIA)

23. CCTV use will be audited annually by the data protection officer or the Trust lead for data protection,

24. Significant CCTV requests or use will be reported to the governors and SLT in line with existing processes

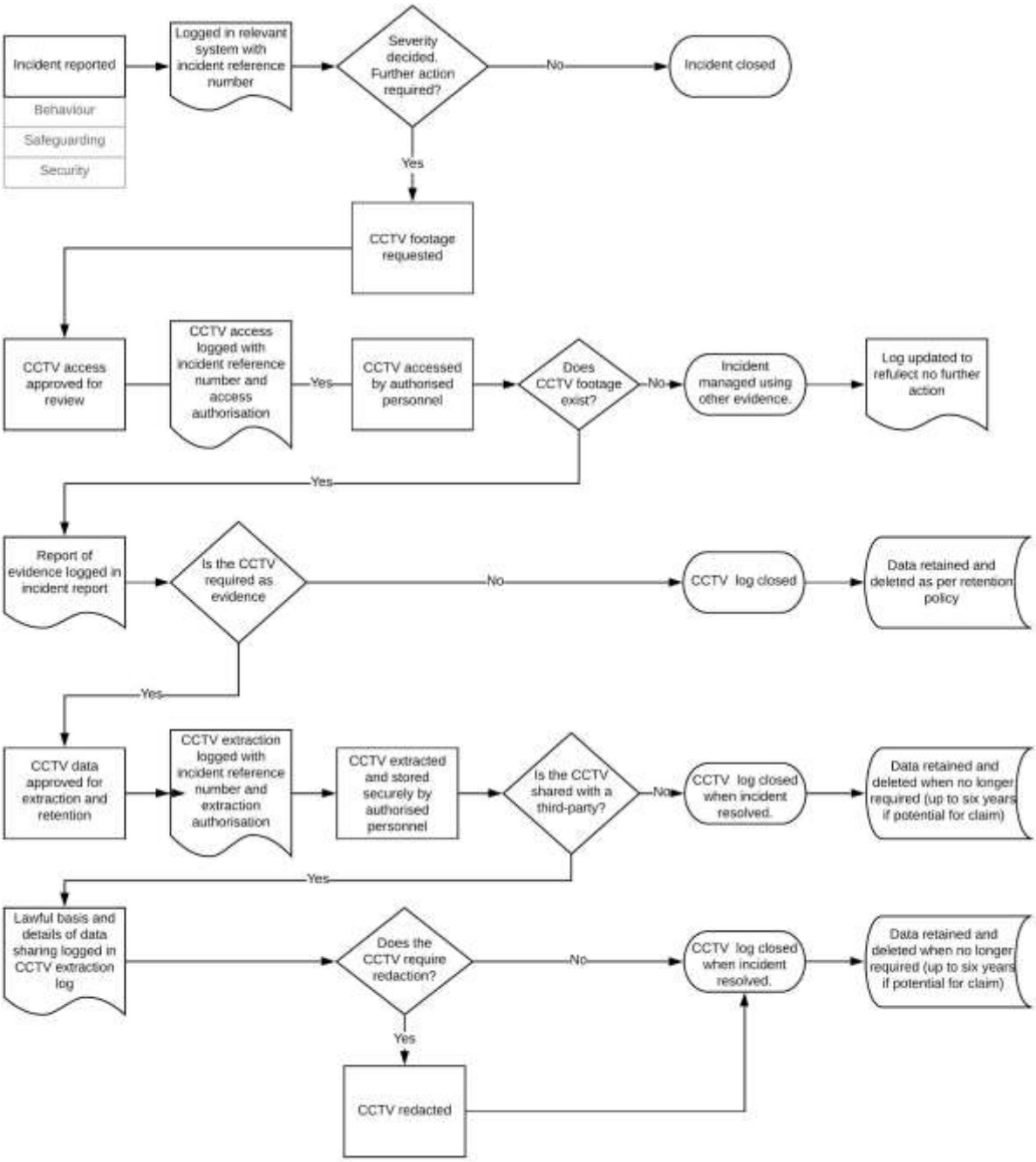
25. Periodic monitoring to ensure compliance is the responsibility of the Headteacher and any issues arising will immediately be reported to the Chair of Governors and the Governing Body's Buildings and Finance Committee

Appendix A: Example CCTV signage

Appendix B: example CCTV access, extraction and approval flow

This flowchart is intended as a guide information flow to ensure that CCTV access and extraction occurs only when both these conditions are met:

- a prior incident exists (where that incident type is documented as a purpose of the CCTV in the organisation's CCTV Policy) and is recorded as an incident
- when authorised by the appropriate personnel



Part 3
Biometric policy

Introduction

26. The Governing Body believes the main purpose of biometric technology is to improve the canteen services for students and staff through the use of cashless catering. The use of cashless catering leads to:

    - The convenience for students and staff of not having to look after and handle cash in school each day.
    - Improved security for handling cash transactions in the school.
    - Reduction in opportunities for children to lose money.
    - A reduction in queuing time at break and lunch.

27. The biometric cashless catering system is owned by the school.

28. An appropriate interface to the system is provided for the use of the school catering contractor.

Operation of the system

29. The day-to-day management of the system is delegated from the Headteacher to the systems manager and the school business manager.
30. Under the terms of a software support contract the software provider may have secure access to the system for the purposes of maintenance and support.

Operational control

31. The system will only be used to provide information on cohorts of students as agreed by the SLT and the Governors.
32. Any consent required by law will be obtained from those students and/or one or more of their parents or carers. At the start of each school year consent will be sought from parents of new incoming pupils.
33. A scheduled routine will be run every night to check the data stored on the Biometric system against the data on the School's information management system and the data stored for any student marked as a leaver during any School day will automatically be deleted.
34. Any student who leaves the School and is subsequently readmitted will need to be re-enrolled on the system.

Security

35. When a person registers their finger in BioStore, no image is saved. Instead, approximately 40 to 60 minutia points are recorded – minutia points are the location and direction of where a ridge ends or splits in two. The rest of the information from the finger scan is discarded. The information used is encrypted and called a template. The data is extremely secure in its encrypted form, but even if it were not encrypted it is impossible to recreate the original image of the finger from this data. The BioStore system only stores a short string of encrypted numbers – too few to provide enough detail for the original print to be reconstructed.

    The BioStore database is encrypted using AES256 – an industry standard and highly secure technology. All communications between applications and the database are also encrypted using AES256. The School has its own secret unique group of AES256 encryption keys, which means that the database and any backup of its contents can only be accessed on licensed hardware, and the encrypted data is only available to the registered licensee. Even if the School's security were to be compromised and a backup of the database stolen, the encrypted data would still be unreadable, even by another school.

36. Any changes to the biometric system will be preceded by a data protection impact assessment (DPIA)

Access by the data subject

37. The Data Protection Act provided data subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those held in the biometric system. Any such requests will be handled through the SAR process.

Monitoring and review

38. Any breach of the policy by School staff will be initially investigated by the Headteacher in order for them to take the appropriate disciplinary action.

39. Performance monitoring, including random operating checks, may be carried out by the Systems Manager, the school business manager, or the data protection team, including the Trust data protection lead

37. Any complaints about the School's Biometric system should be addressed to the Headteacher