Part 1

Name of policy	**B4 Use of CCTV and Biometric Technology**
Status of policy	This is a non stuatutory 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** **The Data Protection Act 1998** (DPA) including the CCTV Code of Practice
Date policy was agreed	7 May 2015
Date for full implementation	Immediate
Date for review	Every two years

Part 2

Policy

1. The Governing Body believes the main purpose of CCTV cameras installed on the School site is to protect Edgbarrow School property and students by assisting in the prevention and / or detection of crime and / or disorder.

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

3. The Governing Body believes the main purpose of Biometric technology is to ensure that all students who have been granted the privilege to leave, and return to, the school site during the course of the school day are registered as being on or off site such that their whereabouts can be accounted for in the event of a safeguarding or emergency situation.

4. The use of Biometric Technology and CCTV at Edgbarrow School will follow the eight Data Protection Principles which are:

- personal data shall be processed fairly and lawfully
- personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- personal data shall be accurate and where necessary kept up to date
- personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes
- personal data shall be processed in accordance with the rights of data subjects under this act
- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data
- personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subject in relation to the processing of personal data

5. 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 and of Biometrics (please see Appendices 1 and 2).

Monitoring and Evaluation

6. 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 Grounds Committee.

Appendix 1

Edgbarrow School Code of practice for the use of CCTV

1. Introduction

1.1 The purpose of this Code of Practice is to regulate the management, operation and use of the closed circuit television (CCTV) system at Edgbarrow School, hereafter referred to as 'the School'.

1.2 The system comprises a number of fixed cameras located around the School site. Cameras may be monitored by selected senior staff together with those directly involved in the security of the school site.

1.3 This code follows the Data Protection Act guidelines.

1.4 The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned by the School.

2. Objectives of the CCTV system

- To protect the School buildings and their assets
- To increase personnel safety and reduce the fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying and apprehending offenders
- To protect members of the public and private property
- To assist in managing the School

3. Statement of intent

3.1 The CCTV system will be registered with the Information Commissioner under the terms of the Data Protection Act 2008 and will seek to comply with the requirements of both the Data Protection Act and the Commissioner's Code of Practice.

3.2 The School will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

3.3 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.

3.4 Cameras are not to focus on private homes, gardens and other areas of private property. 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 an authorisation being obtained as set out in the Regulation of Investigatory Power Act 2000.

3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recorded materials will only be released to the Police for use in the investigation or prevention of a specific crime. Recorded materials will never be released to any organisation or individual unless the Police have made a written request for such release.

3.6 The planning and design has endeavoured to ensure that the system 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.

3.7 Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the School CCTV.

4. Operation of the system

4.1 The system will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the Facilities Manager during the day, out of hours and at weekends.

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

5. Operational control

5.1 Every week, the Facilities Manager will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.

5.2 Access to images will be strictly limited to selected senior staff together with those directly involved in the security of the School site.

5.3 Staff, visitors and others entering areas with CCTV viewing monitors will be subject to particular arrangements as outlined below.

5.4 Authorised staff must satisfy themselves over the identity of any other visitors and the purpose of the visit. Where any doubt exists, the CCTV images must be turned off.

5.5 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual observations will not be permitted.

5.6 If an emergency arises out of hours, permission must be obtained from the Headteacher or Facilities Manager to view or process recorded material.

5.7 Other operational functions will include maintaining recorded materials and hard disc space, filing and maintaining occurrence and system maintenance logs.

5.8 Incidents involving the Emergency Services must be notified to the Headteacher or Facilities Manager.

6. Liaison

6.1 Liaison meetings will be held as required with all staff involved in the support of the system.

7. Monitoring procedures

7.1 Camera surveillance may be maintained at all times.

7.2 Pictures may be continuously recorded or when activated by movement.

7.3 If covert surveillance is planned, this must be authorised by the Headteacher or, in an emergency, by any of the Deputy Headteachers. A written record of this authorisation will be kept.

8. Recorded material

8.1 In order to maintain and preserve the integrity of the recorded material used to record events from the hard drive and the facility to use them in any future

proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each item of recorded material must be identified by a unique mark.
- Before use, each item on which images will be recorded must be cleaned of any previous recording.
- The person making the recording shall register the date and time of recorded material insert, including recorded material reference.
- Any recorded material required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure recorded material store. If recorded material is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence material store.
- If the recorded material is archived the reference must be noted.

8.2 Recorded materials may be viewed by the Police for the prevention and detection of crime, authorised officers of the Police for supervisory purposes, authorised demonstration and training.

8.3 A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register will be available for this purpose.

8.4 Viewing of recorded materials by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under Section 29 of the Data Protection Act 2008.

8.5 Should any recorded material be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 of this Code. Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of the School, and both the recorded material and information contained on it are to be treated in accordance with this Code. The School also retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions, when a Court requires the release of original recorded material, this will be produced from the secure recorded material store, complete in its sealed bag.

8.6 The Police may require the School to retain the stored materials for possible use as evidence in the future. Such recorded materials will be properly indexed and properly and securely stored until they are needed by the Police.

8.7 Applications received from outside bodies (eg solicitors) to view or release recorded materials will be referred to the Headteacher. In these circumstances, recorded materials will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of the materials in other cases.

8.8 Unless required by the Police to assist with the detection or prevention of crime, recorded materials will be deleted from the computer hard drive after 30 days.

9. Breaches of the Code (including breaches of security)

9.1 Any breach of the Code of Practice by School staff will be initially investigated by the Headteacher in order for him/her to take the appropriate disciplinary action.

9.2 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.

10. Assessment of the system and Code of Practice

10.1 Performance monitoring, including random operating checks, may be carried out by the Facilities Manager.

11. Complaints

11.1 Any complaints about the School's CCTV system should be addressed to the Headteacher and will be investigated in accordance with Section 9 of this Code.

12. Access by the data subject

12.1 The Data Protection Act provided data subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV.

12.2 Requests for data subject access should be made to the Headteacher.

13. Public information

Copies of this Code of Practice will be available on application.

Appendix 2

Edgbarrow School Code of practice for the use of Biometrics

1. Introduction

1.1 The purpose of this Code of Practice is to regulate the management, operation and use of the Biometric system at Edgbarrow School, hereafter referred to as 'the School'.

1.2 The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.3 The Biometric system is owned by the School.

2. Objectives of the Biometric system

2.1 The objectives of the Biometric system are:

- To ensure that the School has a record of students leaving or returning to the School site during the School day
- To ensure that all students can be accounted for in the case of fire or similar emergency
- To assist in the safeguarding of students
- To assist in managing the School

2.2 The Biometric system has been selected in preference to other methods of registering students who may leave and return to the School site during the School day because it is unique to the individual student and does not require them to remember to carry any item such as a card which could be lost or forgotten.

3. Statement of intent

3.1 The Biometric system will seek to comply with the requirements of the Data Protection Act.

3.2 The School will treat the system and all information obtained and used as data which are protected by the Act.

3.3 Information obtained from the system will only be used for the purposes outlined in Section 2 of this code.

4. Operation of the system

4.1 The system will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the Systems Manager.

4.3 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.

5. Operational control

5.1 The system will only be used to provide information on cohorts of students as agreed by the SLT and the Governors.

5.2 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.

5.3 The system will take 3 temporary snapshots of the fingerprint image to create an algorithm. These images will not be saved, and cannot be recalled once the enrolment process is complete.
5.4 The algorithm produced under Section 5.3 above will be stored in a database in a separate folder on a secure server. This folder will only be accessible to named administrative and support staff who require access to the software which is used to print student lists to be used in the event of a fire or other similar emergency.
5.5 The algorithm data cannot be accessed and read, neither can it be reconstructed to a fingerprint.
5.6 Registration data is written directly to the lesson registers in the School's information management system. In case of emergency, student lists can be printed from a number of specified PCs around the School site.
5.7 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 algorithm data stored for any student marked as a leaver during any School day will automatically be deleted.
5.8 Any student who leaves the School and is subsequently readmitted will need to be re-enrolled on the system.

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

6.1 Any breach of the Code of Practice by School staff will be initially investigated by the Headteacher in order for him/her to take the appropriate disciplinary action.
6.2 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. Assessment of the system and Code of Practice

7.1 Performance monitoring, including random operating checks, may be carried out by the Systems Manager.

8. Complaints

8.1 Any complaints about the School's Biometric system should be addressed to the Headteacher and will be investigated in accordance with Section 9 of this Code.

9. Access by the data subject

9.1 The Data Protection Act provided data subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV.
9.2 Requests for data subject access should be made to the Headteacher.

10. Public information

Copies of this Code of Practice will be available on application.