BARNFIELD PRIMARY SCHOOL

CCTV POLICY

1. INTRODUCTION

1.1 The purpose of this Policy is to regulate the review, management, operation, and use, of closed circuit television (CCTV) at Barnfield Primary School. CCTV is in use to:

- ✓ increase personal safety of students, staff and visitors, and reduce the fear of crime
- ✓ monitor and minimise unauthorised and inappropriate access
- ✓ protect the school buildings and their assets

1.2 The system comprises of a number of fixed cameras.

1.3 The system does not have sound recording enabled.

1.4 The CCTV system is operated by the school and the deployment of which is determined by the school's leadership team.

1.5 The CCTV is accessible only by certain key staff with responsibility for security or behaviour, Leadership Team, Chair of Governors, Caretaker and Office Manager.

1.6 Any changes CCTV monitoring will be subject to consultation with staff and the school community.

1.7 The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images and any sound recordings, is covered by the Data Protection Act 1998. This policy outlines the school's use of CCTV and how it complies with the Act.

1.8 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

1.9 The data controller (Headteacher), has responsibility for the control of images and deciding how the CCTV system is used.

2. STATEMENT OF INTENT

2.1 The CCTV system will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

2.2 The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

2.3 Cameras will be used to monitor activities within the school and its grounds to identify criminal activity actually occurring, anticipated, or perceived. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and school together with its visitors.

2.3.1 The system has been designed to the best of its abilities to deny observation on adjacent private homes, gardens and other areas of private property.

2.4 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

2.4.1 Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.

2.4.2 Images will never be released to the media for purposes of entertainment.

2.5 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.

2.6 Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site.

3. SYSTEM MANAGEMENT

3.1 The system will be administered and managed by Barnfield Primary School who will act as the Data Controller, in accordance with the principles and objectives expressed in the policy.

3.2 The day-to-day management will be the responsibility of both the Headteacher and Office Manager who will act as the System Manager.

3.3 The system and the data collected will only be available to the Data Controller, the Head and the System Manager.

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

3.5 The System Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

3.6 Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

3.7 The System Manager must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists access will be refused.

3.8 Details of **ALL** visits and visitors will be recorded in the system log book including time/data of access and details of images viewed.

3.9 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

4. COVERT MONITORING

4.1 The school may in exceptional circumstances set up covert monitoring. For example:

i. Where there is good cause to suspect that an illegal or unauthorised action(s), are taking place, or where there are grounds to suspect serious misconduct;

ii. Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances authorisation must be obtained from the data controller.

4.3 Covert monitoring must cease following completion of an investigation.

.

5. STORAGE AND RETENTION OF CCTV IMAGES

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely.

6. ACCESS TO CCTV IMAGES

6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

7. SUBJECT ACCESS REQUEST (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

7.2 All requests should be made in writing to the data controller. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The school will respond to requests within 40 calendar days of receiving the written request.

7.4 As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and the images pixelated so that only the person requesting access can be identified. The school has software that enables images to be pixelated, but if it is not possible to conceal the identity of others, disclosure is unlikely. Refusal to disclose images, even if pixelated, may be appropriate where its release is:

- ✓ Likely to cause substantial and unwarranted damage to an individual.
- ✓ To prevent automated decisions from being taken in relation to an individual.
- ✓ Likely to prejudice the legal rights of individuals or jeopardise an ongoing investigation.

8. ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

8.2 Requests for access should be made in writing to the data controller.

8.3 The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. COMPLAINTS

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher at the school.

9.2 If the issue remains unresolved the procedure for complaints should be followed (see School Complaints Policy)

9.3 If the issue remains unresolved, and the complainant considers that the school is not operating within the Code of Practice as issued by the Information Commissioners Office, they are advised to contact the Information Commissioners Office via www.ico.org.uk

May 2018