Oak Bank School Policy

CCTV Policy

Prepared By: P Cohen

Review and Amendment						
By	PC	RF				
Date	01/10/14	11/01/17				
Signed						
Governor	JH	PB				
Date	15/10/14	28/03/17				
Signed						

CCTV System Policy

1. Introduction

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

1.2 The system comprises a number of fixed internal cameras and functional external cameras located around the school site. Classroom cameras will feature audio recording. All cameras are monitored and images reviewed via two desktop PC's within the school by authorised persons only.

Staff authorised to use CCTV are:

- Sue Whitcomb (Business Manager)
- Peter Cohen (Executive Head)
- Rachael Freer (Head of school)
- Phillip Collier (Deputy Head)
- Stephen McConnell (KS2 Behaviour manager)
- Rachael Cox (KS3 Behaviour manager)
- David Chapman (KS4 Behaviour manager)

Images and video footage can only be recorded and stored by Rachael Freer or Peter Cohen and such footage will be kept in a secure limited access on w drive on the school system. CCTV saved to this drive cannot be deleted due to set permissions by the administrator.

1.3 This Code follows Data Protection Act guidelines: Those are:

Data should be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible
- with those purposes
- Adequate relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in accordance with individuals' rights
- Secure
- Not transferred to countries without adequate protection

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 Scheme

- To protect the school buildings and their assets
- To increase personal safety and reduce the fear of crime and anti-social behaviour
- To support the school and police in a bid to deter and detect crime, vandalism, anti- social behaviour and acts of aggression
- To assist in identifying, apprehending and disciplining/prosecuting offenders
- To protect members of the public and private property
- To assist in managing the school

3. Statement of Intent

3.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of 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 will be used to monitor activities within the school 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, together with its visitors.

3.4. Cameras are not to focus on private homes, gardens and other areas of private property.

3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

3.6 The planning and design has endeavoured to ensure that the Scheme 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 Scheme will be administered and managed by the Senior Leadership Team, in accordance with the principles and objectives expressed in the code. Access to images will be strictly controlled.

4.4 The CCTV system will be operated 24 hours each day, every day of the year and regularly maintained.

5. Images and Associated Audio Data

5.1 Images and associated data should not be retained for longer than is necessary and unless required for specific investigation or evidential purposes, deleted after 31days have passed.

5.2 Once the retention period has expired, the images and associated data should be removed or erased.

5.3 Images and associated data that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.

5.4 Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed or be capable of being viewed by anyone other than authorised persons.

5.5 Access to the recorded images and associated data should be restricted to the or designated member of staff who will decide whether to allow requests for access.

5.6 Viewing of the recorded images and associated data should take place in a restricted area, for example, in the headmaster's office or designated member of staff's office, other employees should not be allowed to have access to that area when a viewing is taking place.

5.7. Removal of the medium on which images and associated data are recorded, for viewing purposes, should be documented as follows:

- The date and time of removal;
- The name of the person removing the data;
- The name(s) of the person(s) viewing the data;
- The reason for the viewing;
- The outcome, if any, of the viewing;
- The date and time the data were returned to the system or secure place, if they have been retained for evidential purposes.

5.8. All operators and employees with access to images and associated data should be aware of the procedure that needs to be followed when accessing the recorded images.

5.9. All operators should be trained in their responsibilities under the Code of Practice, i.e. they should be aware of:

- The user's security policy e.g. procedures to have access to recorded images and associated data;
- The user's disclosure policy

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. Access to and disclosure of images to third parties

All employees should be aware of the restrictions set out in this code or practice in relation to access to, and disclosure of, recorded images.

7.1 Access to recorded images will be restricted to those persons who need to have access in order to achieve the purpose(s) of using the equipment.

7.2 All access to the medium on which the images are recorded should be documented.

7.3 Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances. Subject to paragraph 1 above, in disclosure will be limited to the following classes of persons/agencies.

- Law enforcement agencies, where the images recorded would assist in a specific enquiry;
- Law enforcement agencies where the images would assist a specific criminal enquiry;
- Relevant legal representatives

7.4 All requests for access or for disclosure should be recorded, if access or disclosure is denied, the reason should be documented

7.5 If access to or disclosure of the images is allowed, then the following will be documented. (Appendix B)

- The date and time at which access was allowed or the date on which disclosure was made;
- The identification of any third party who was allowed access or to whom disclosure was made;
- The reason for allowing access or disclosure;
- Location of the images
- Any crime incident number to which images may be relevant
- Signature of person authorised to collect the medium – where appropriate.

7.6 Recorded images will not be made more widely available – for example they should not be routinely made available to the media or placed on the Internet.

7.7 If it is intended that images will be made more widely available, that decision should be made by the Headteacher or designated member of staff and the reason for that decision should be documented.

7.8 If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable.

8. Access by data subjects

8.1 In accordance with Section 7 of the Data Protection Act 1998 (Subject Access), an individual who believes that their image has been captured by this scheme is entitled to make a written request to the Data Controller. Upon payment of the current fee*, and the supply of essential information, a systems search will be conducted and subject to certain conditions, the individual will be allowed access to the personal data held (The current maximum fee is £10.00 and may be reviewed)

8.2 All subject access requests should be referred in the first instance to the Headteacher

8.3 All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and how such requests are to be dealt with.

8.4 Data subjects should be provided with a standard subject access request form, which:

- Indicates the information required in order to locate the images requested;
- Indicates the information required in order to identify the person making the request;
- Indicates the fee that will be charged for carrying out the search for the image requested.

NB. The above form will also enquire whether the individual would be satisfied with merely viewing the images recorded. The form will also indicate that the response will be provided promptly and in any event within 40 days of receiving.

8.5 Individuals, at the time of any subject access request, will be given a description of the type of images recorded and retained and the purpose for which the recording and retention takes place. They should be informed of their rights as provided by the 1998 Act,

8.6 Prior to any authorised disclosure, the Headteacher will need to determine whether the images of another “third party” individual features in the personal data being applied for and whether these third party images are held under a duty of confidence,

8.7 If third party images are not to be disclosed the System Manager shall arrange for the third party images to be disguised or blurred,

8.8 If the Headteacher decides that a subject access request from an individual is not to be complied with, the following should be documented:

- The identity of the individual making the request;
- The date of the request;
- The reason for refusing to supply the images requested;
- The name and signature of the person making the decision.

9. Other Rights

Under the Data Protection Act individuals also have the following rights which may be applicable to CCTV schemes:

- Right to prevent processing likely to cause damage or distress;
- Rights in relation to automated decision taking;
- Right to seek compensation for failure to comply with certain requirements.

Where a request is made in relation to other rights, these shall be referred to the Headteacher who will document the request and respond to it.

10. Monitoring Compliance with this Code of Practice

10.1 The contact point indicated on the sign should be available to members of the public during normal office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.

10.2 Enquirers should be provided on request with one or more of the following:

- A copy of this code of practice;
- A subject access request form if required or requested;
- The Complaints Procedure to be following if they have concerns about the use of the system.

10.3 The Business Manager should undertake regular reviews of the documented procedures to ensure that the provisions of the Code are being complied with.

10.4 An internal annual assessment should be undertaken which evaluates the effectiveness of the system.

10.5 De-personalised details of complaints will be maintained and will be included in an annual report on each CCTV system.

10.6 A copy of the Complaints Procedure will be made available upon request from the school's Business Manager.

This document was produced June 2009 and is due for its annual review in February 2014.

Reviewed by RF in January 2017

I have read the policy relating to the access of the school CCTV system. I understand that failure to adhere to this policy will be deemed as professional misconduct. Failure to follow the outlined procedures will be deemed gross misconducted and may lead to suspension or termination of employment.

SIGNED	NAME	DATE
	SUE WHITCOMB	
	PETER COHEN	
	RACHAEL FREER	
	PHIL COLLIER	
	STEPHEN McCONNELL	
	RACHAEL FREER	
	DAVID CHAPMAN	