



POLICIES AND PROCEDURES

CCTV POLICY

Updated June 2016

1. INTRODUCTION

This policy is intended to provide guidance as to good practice for users of the CCTV (closed circuit television) systems at North Huddersfield Trust School and is based upon the Code of Practice published by the Information Commissioner which set out the standards that must be met under the requirements of the Data Protection Act 1998, that:

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.*

2. NORTH HUDDERSFIELD TRUST SCHOOL CCTV SYSTEM

- Owner and controller of the system – Loz Wilson, Head Teacher
- The school considers that the CCTV Scheme contributes to security and the health and safety of pupils, staff and visitors
- CCTV systems have been notified to the Information Commissioner.
- The general management of CCTV in is vested with the Network Manager.

3. SITING THE CAMERAS

The Governing Body considered the proper location of CCTV cameras, where they exist, in and around school. The location of the cameras is based upon a variety of information including security and health and safety.

Standards

- All such CCTV equipment installed will only be sited in such a way that it can only monitor those spaces that are intended to be covered by the equipment.
- The cameras are situated in locations which ensure that they do not overlook properties or garden areas of neighbouring properties.
- The employees and pupils are made aware of the purpose(s) for which the scheme has been established and notices to this effect will be displayed around the school. Parents are informed through the school prospectus.

- The operators must only use the equipment in order to achieve the purposes for which it has been installed – this is to maintain the health and safety of pupils, staff and visitors to the school.
- Cameras that are adjustable by the operators must not be adjusted or manipulated by them to overlook spaces which are not intended to be covered by the scheme. Cameras cover only corridor areas and entrances to the school and do not allow for filming of pupils in lessons.
- If any person becomes aware about, or is concerned of the possibility of a camera location which might infringe privacy in an unacceptable way, they should report the matter to the Head Teacher as soon as possible.
- Signs, of no less than the minimum standard are placed so that the public are aware that they are entering a zone that is covered by CCTV. The signs contain the following information:
 - a. Identity of the person or organisation responsible for the scheme;*
 - b. The purposes of the scheme;*
 - c. Details of whom to contact regarding the scheme;*
 - d. Any other information that may become a statutory requirement.*

4. QUALITY OF IMAGES

Standards

- Regular checks are made to ensure that the system is operating properly.
- Images are retained on a hard disc drive for a period of 7 days. Copies can be made for investigation purposes only.
- Checks will be made to ensure the accuracy of any features such as the location of the camera and/or date and time reference. Where the time/date etc are found to be out of sync with the current time/date, the operators will take such remedial action as is continued in the operations manual to correct the error. A note of such changes will be recorded in the daily occurrence log.
- When installing cameras, consideration is given to the physical conditions in which the cameras are located.
- Cameras should be protected from vandalism in order to ensure that they remain in working order.
- A maintenance log will be kept in the monitoring centre of the system concerned.
- The school's Network Manager, with support from the Premises Manager, is responsible for:-
 - making arrangements for ensuring that a damaged camera is fixed;
 - ensuring that a camera is fixed within a specific time period;
 - monitoring the quality of the maintenance work.

5. PROCESSING THE IMAGES

- Images should not be retained for longer than is necessary and unless required for specific investigation or evidential purposes, deleted after 7 days have passed.
- Once the retention period has expired, the images should be removed or erased.
- Images that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.
- 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.
- Access to the recorded images should be restricted to a manager or designated member of staff who will decide whether to allow requests for access.
- Viewing of the recorded images should take place in a restricted area, for example, in a manager's 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.
- Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows (See Appendix A):
 - The date and time of removal;
 - The name of the person removing the images;
 - The name(s) of the person(s) viewing the images;
 - The reason for the viewing;
 - The outcome, if any, of the viewing;
 - The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.
- All operators and employees with access to images should be aware of the procedure that needs to be followed when accessing the recorded images.
- 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;
 - The user's disclosure policy

6. ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

All employees should be aware of the restrictions in relation to access to, and disclosure of, recorded images.

- Access to recorded images will be restricted to those persons within the school who need to have access in order to achieve the purpose of using the equipment.

- All access to the medium on which the images are recorded is documented.
- Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances. Subject to paragraph 1 above, disclosure will be limited to the following classes of persons/agencies:
 - Law enforcement agencies, where the images recorded would assist in a specific enquiry;
 - Prosecution Agencies;
 - Relevant legal representatives
- All requests for access or for disclosure should be recorded, if access or disclosure is denied, the reason should be documented.
- If access to or disclosure of the images is allowed, then the following will be documented (See Appendix B):
- 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. ACCESS BY DATA SUBJECTS

- 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).
- All subject access requests should be referred in the first instance to the Headteacher who will liaise with the Network Manager.
- 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.
- Data subjects should be provided with a standard subject access request form, a copy of this form is attached at appendix C. The 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.
- 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.
- 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.

- If third party images are not to be disclosed the Network Manager shall arrange for the third party images to be disguised or blurred.
- 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.

8. 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.

9. MONITORING COMPLIANCE WITH THIS CODE OF PRACTICE

- 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.
- Enquirers should be provided on request with one or more of the following:
 - A copy of this policy;
 - A subject access request form if required or requested;
 - The Complaints Procedure to be followed if they have concerns about the use of the system.
- The Network Manager undertakes regular reviews of the documented procedures to ensure that the provisions of the policy are being complied with.
- An internal annual assessment is undertaken which evaluates the effectiveness of the system.
- De-personalised details of complaints are maintained and will be included in an annual report on the CCTV system.
- A copy of the Complaints Procedure will be made available upon request.

APPENDIX A

RECORDING OF VIEWING BY AUTHORISED SCHOOL STAFF

Date and Time Image Viewed:	Date:	Time:
Name of Persons Viewing the Image:		
Name Designation:		
Reason for the viewing:		
Outcome, if any, of the viewing:		

RECORDING OF VIEWING BY THIRD PARTY (e.g. Police)

Date and Time Access Allowed:	Date:	Time:
Identification of any third party who was allowed access		
Name of school staff present:		
Reason for allowing access:		
Crime incident number if applicable:		
Location of the images:		
Signature of the person authorized to collect the medium – where appropriate:	<p align="center">-----</p>	
Date and time copy created for evidential purposes:	Date:	Time:

FORM TO REQUEST ACCESS TO CCTV IMAGES – FEE £10.00

Name:		
Address:		
Date of Birth:		
Telephone number:		
Date and Time Image Recorded:	Date:	Time:
Location:		

Note:

To carry out a search for the images, a fee of £10.00 will be charged.

Please complete the above form and attach a £10.00 cheque made payable to North Huddersfield Trust School.

The Headteacher will consider the request and respond within 28 days.