CCTV Policy and Procedure

January 2021

Approved By:	**Date:**
Next review Due by:	
Any signature required:	

All things are possible for those who believe. (Mark 9:23)
Learning together we grow in faith.

CONTENTS

1. INTRODUCTION

This procedure for handling the use of Closed Circuit Television (CCTV) (from this point forward referred to as "The System") in schools has been consulted upon between Rochdale Metropolitan Borough Council – 'the Local Authority' and the recognised Teachers' Associations and has been consulted on with the Trade Unions representing support staff within schools. The term 'Governing Body' used through this procedure shall be taken to include those persons or committees acting in the name of the Governing Body.

The Teacher Associations and Unison, the Support Staff Union have been consulted on this guidance however do not fully agree with it.

A CCTV system has been introduced to various locations in Little Heaton CE Primary School. This system, known as the 'Ademco CCTV System', comprises a number of cameras installed at strategic

locations. Some of the cameras are fully operational with pan, tilt and zoom facilities. Others are fixed cameras, images from which are presented in the same room. The cameras are there to enhance the working environment and keep staff, pupils and visitors safe and this policy is a safeguard against infringing liberties for the purposes of the Data Protection Act the 'Data Controller' is the School and the nominated person is the head teacher. The head may, however, delegate responsibility for the management of the System to a System Manager.

The System Manager is responsible for the correct application of this policy and the security of the footage. The System Manager is the point of contact for any queries regarding the CCTV system of the School and oversees the use of and access to any equipment or stored footage. The System Manager at this School is the Headteacher.

The Ademco CCTV system has been notified to the Information Commissioner under registration no Z8407324.

Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Document.

The School recognises that public authorities and those organisations carrying of the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998 and the European Convention on Human Rights, and consider that the use of CCTV in Little Heaton CE Primary School is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety and is an operational requirement.

Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for Local Authorities and Schools to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare.

It is recognised that operation of the Ademco CCTV System may be considered to infringe on the privacy of individuals. The school recognise that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic wellbeing of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.

The Policy and Procedures shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial.
The Ademco CCTV System shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. This applies to everyone: staff, pupils, parents and visitors.

2. OBJECTIVES OF THE SYSTEM

The objectives of the Ademco CCTV System as determined by the School which form the lawful basis for the processing of data is:-

- To help reduce the fear of crime
- To help deter crime
- To help detect crime and provide evidential material for court
- To assist in the fulfilment of the statutory Health and Safety requirements
- To assist in the maintenance of the physical security of the school building and campus
- To assist in monitoring any Emergency Planning operations

- To assist in detection of professional misconduct and provide evidential material for school proceedings NB: the legality of its use in school proceedings must be established at the time to ensure it meets the necessary thresholds (further explanation is provided under "proportionate and reasonable use").

The CCTV system is to be used only for the objectives stated above. Use of CCTV footage for any other purpose is only legal where an alternative, statutory basis exists, such as powers for crime detection and prevention in the Crime and Disorder Act 1998, or where explicit, written consent of the person/s involved has been given.

Proportionate and reasonable use
Use of the CCTV system must not be excessive or unreasonable. When considering whether or not to use CCTV footage, the System Manager must decide whether the use is legitimate in view of the School's clearly stated objectives, as asserted above. If a particular request is made for access to footage, even if it is considered as appropriate in line with the objectives, the System Manager must decide whether it is proportionate.

For example, it may be necessary to use the footage where there are no alternative ways to resolve the issue in hand. Where there are issues of a disciplinary nature, CCTV should not be used unless no other evidence exists and The System is used for verification purposes. In any case where there is some uncertainty, advice from The Information Protection and Assurance Unit at Rochdale Council should be sought. Contact details can be found at Appendix A.

Necessary thresholds, and whether schools can use the footage in respect of school proceedings, can only be established at the time and its use must be justified, necessary and proportionate in each case. An assumption cannot be made that because the footage is in existence it can be used whenever a situation relating to professional misconduct occurs. The procedures within this policy will need to be observed including, authorisation from the System Manager and advice from Schools Personnel Team who will liaise with the Information Team to ascertain whether footage can be in used in school based proceedings otherwise evidence obtained will be inadmissible.

Operating Manual
This document offers instructions on all aspects of the day to day operation of The System. To ensure the purpose and principles of the CCTV system are realised.

3. STATEMENT OF PURPOSE AND PRINCIPLES

Purpose
The purpose of this document is to state the intention of the owners and the managers, as far as is reasonably practicable, to support the objectives of the Ademco CCTV System, (hereafter referred to as 'The System') and to outline how it is intended to do so.

The 'Purpose' of The System, and the process adopted in determining the 'Reasons' for implementing 'The System' are as previously defined in order to achieve the objectives detailed previously.

General Principles of Operation
The System will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

The operation of The System will also recognise the need for formal authorisation of any covert 'Directed' surveillance or crime – trend (hotspot') surveillance as required by the Regulation of Investigatory Powers Act 2000 and the police force policy.

The System will be operated in accordance with the Data Protection Act 1998 at all times.

The System will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this document, or which are subsequently agreed in accordance with this document.

The System will be operated with due regard to the principle that everyone has the right to respect for his or her private life.

The public interest in the operation of The System will be recognised by ensuring the security and integrity of operational procedures.

Throughout this document it is intended, as far as reasonably possible, to balance the objectives of The System with the need to safeguard the individual's rights. Every effort has been made throughout the document to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that The System is not only accountable, but is seen to be accountable.

Participation in The System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this document and to be accountable under the document.

Copyright
Copyright and ownership of all material recorded by virtue of The System will remain with the data controller.

Cameras and Area Coverage
The areas covered by CCTV to which this document refers are the public areas to cover the school building and campus.

Monitoring and Recording Facilities
A monitoring room is located in the server room.

CCTV operators are able to record images from selected cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with this document. All viewing and recording equipment shall only be operated by trained and authorised users.

Human Resources
Unauthorised persons will not have access without an authorised member of staff being present.

The monitoring area shall be staffed by specially selected and trained staff.

All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and the responsibilities contained within this document. Further training will be provided as necessary.

Processing and Handling of Recorded Material
All recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be processed and handled strictly in accordance with this Document.

Operators Instructions
Technical instructions on the use of equipment housed within the monitoring area are contained in a separate manual provided by the equipment suppliers.

Notes:

1. The installation of a CCTV camera is considered to **be overt** unless it is installed in a manner whereby its presence is deliberately intended to be concealed from the view of any person likely to be within the field of view of that camera.

2. Cameras which may be placed in domes or covered to reduce the likelihood of assessing their field of view, or to protect them from weather or damage, would not be regarded as covert provided that appropriate signs indicating the use of such cameras are displayed in the vicinity.

3. The use of 'dummy' cameras as part of a CCTV System is strongly discouraged. The greatest deterrent value of a CCTV System is its power to produce evidential material and, in doing so, to reassure those it is intended to protect.

4. It is acknowledged that many CCTV Systems are operated on a 'part time' basis or without the benefit of a staffed monitoring room. In such cases reference to 'monitoring rooms' throughout this Document should be applied to existing monitoring and recording facilities as appropriate.

5. It is also recognised that, in the interest of security and operator safety, some CCTV System owners do not wish the precise location of the relevant monitoring room to be included within the text of a Document.

6. It is strongly recommended that the recording of images should not take place at more than one location.

4. PRIVACY AND DATA PROTECTION

Public Concern
Although the majority of the public at large may have become accustomed to 'being watched', those who do express concern do so mainly over matters pertaining to the processing of the information, (or
data) i.e. what happens to the material that is obtained.

Note: *'Processing'* means **obtaining, recording** or **holding** the information or data or **carrying out any operation** or **set of operations** on the information or data, including;
1. organisation, adaptation or alteration of the information or data;
2. retrieval, consultation or use of the information or data;
3. disclosure of the information or data by transmission, dissemination or
4. otherwise making available, or
5. alignment, combination, blocking, erasure or destruction of the information or data.

All personal data obtained by virtue of The System, shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of The System. In processing personal data there will be respect for everyone's right to respect for his or her private life.

Data Protection Legislation
The operation of The System has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.

The 'data controller' for The System' is the School and day to day responsibility for the data will be devolved to Claire Crawford – Head of School.

All data will be processed in accordance with the principles of the Data Protection Act, 1998 which, in summarised form, includes, but is not limited to:
1. All personal data will be obtained and processed fairly and lawfully.
2. Personal data will be held only for the purposes specified.
3. Personal data will be used only for the purposes, and disclosed only to the people, shown within these documents of practice.
4. Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
5. Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
6. Personal data will be held for no longer than is necessary.
7. Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.
8. Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

Request for information (subject access request)
Any request from an individual for the disclosure of personal data which he/she believes is recorded by virtue of The System will be directed in the first instance to the System Manager or Data Controller.

The principles of Sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request; those Sections are reproduced as Appendix B to this.

If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation, or consult with the Information Protection & Assurance Manager, within the Performance and Development Directorate.

Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' request form is included in Appendix G.

Exemptions to the Provision of Information
In considering a request made under the provisions of Section 7 of the Data Protection Act 1998, reference may also be made to Section 29 of the Act which includes, but is not limited to, the following statement:

Personal data processed for any of the following purposes -
1. the prevention or detection of crime
2. the apprehension or prosecution of offenders are exempt from the subject access provisions in any case 'to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection'.

Note Each and every application will be assessed on its own merits and general 'blanket exemptions' will not be applied.

5. ACCOUNTABILITY AND PUBLIC INFORMATION

The Public

For reasons of security and confidentiality, access to the CCTV monitoring area is restricted. However, in the interest of openness and accountability, anyone with legitimate reasons wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the System Manager.

Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' will be programmed into The System as required in order to ensure that the interior of any private residential property within range of The System is not surveyed by the cameras. If such 'zones' cannot be programmed the operators will be specifically trained in privacy issues.

A member of the public wishing to register a complaint with regard to any aspect of The System may do so by contacting the System Manager's office. All complaints shall be dealt with in accordance with the School's complaints procedure, a copy of which may be obtained from the school's website. Any performance issues identified will be considered under the organisations disciplinary procedures to which all members of Little Heaton CE Primary School, including CCTV personnel are subject.

All staff is contractually subject to regulations governing confidentiality and discipline. Unlawful disclosure of CCTV footage or failing to keep information secure may result in further action taking place against those who breach the regulations. Any individual who suffers damage or distress by reason of any contravention of this document may be entitled to compensation.

System Owner
The Little Heaton CE Primary School, named at appendix A, being the nominated representative of The System owners will have unrestricted access to the CCTV monitoring area and will be responsible for receiving regular and frequent reports from the System Manager.

System Manager
The nominated person named at appendix A will have day-to-day responsibility for The System as a whole.

Signs
Signs will be placed in the locality of the cameras and at main entrance points to the relevant areas. The signs will indicate:
1. The presence of CCTV monitoring;
2. The 'ownership' of The System;
3. Contact telephone number of the 'data controller' of The System.
In circumstances that audio recording is being used, this should be stated explicitly and prominently.

6. ASSESSMENT OF THE SYSTEM

Evaluation
The System will periodically be independently evaluated to establish whether the purposes of The System are being complied with and whether objectives are being achieved. Through provision of a Service Level Agreement this may be undertaken by Officers from the Local Authority.

1. An assessment of the incidents monitored by The System
2. An assessment of neighbouring areas without CCTV
3. Whether the purposes for which The System was established are still relevant
4. Cost effectiveness

Monitoring
The System Manager will accept day to day responsibility for the monitoring, operation and evaluation of The System and the implementation of this document.

The System Manager shall also be responsible for maintaining full management information as to the incidents dealt with by staff. A log of requests shall be maintained as per appendix *** and this must be retained for all requests to view CCTV and all instances where approval has been provided to view CCTV.

Audit
The organisation's auditor or other nominated appropriate person, or his/her nominated deputy, who is not the System Manager, will be responsible for regularly auditing the operation of The System (annually) and compliance with this document. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, video tape histories and the content of recorded material. Through provision of a Service Level Agreement this may be undertaken by Officers from the Local Authority.

7. HUMAN RESOURCES

Staffing of the Monitoring Room and those responsible for the operation of The System
Equipment associated with The System will only be operated by authorised personnel who will have been properly trained in its use and procedures.

Discipline
Every individual with any responsibility under the terms of this Document and who has any involvement with The System to which they refer, will be subject to the School's discipline document. Any breach of this Document or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

The System Manager will accept primary responsibility for ensuring there is no breach of security and that the document is complied with. He/she has day to day responsibility for the management of the room and for enforcing the discipline rules.

Non-compliance with this document by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

8. CONTROL AND OPERATION OF CAMERAS

Guiding Principles
Any person operating the cameras will act with utmost integrity at all times.

The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

Every use of the cameras will accord with the purposes and key objectives of The System and shall be in compliance with this document.

Cameras will not be used to look into private residential property. 'Privacy zones' shall be programmed into The System (whenever practically possible) in order to ensure that the interior of any private residential property within range of The System is not surveyed by the cameras.

Camera operators will be mindful of exercising prejudices which may lead to complaints of The System being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of The System or by the System Manager.

Primary Control

Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

Operation of The System by the Police
Under extreme circumstances the Police may make a request to assume direction of The System to which this document applies. Only requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of The System owners, or designated deputy of equal standing.

In the event of such a request being permitted, the Monitoring area will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so, will then operate under the direction of the police officer designated in the written authority.

In very extreme circumstances a request may be made for the Police to take total control of The System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of The System owners. Any such request should be made to the System Manager in the first instance, which will consult personally with the most senior officer of The System owners (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or person of equal standing.

Maintenance of the System
To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality the CCTV system shall be maintained to a high standard.

Any maintenance agreement will make provision for regular/periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.

The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of The System.

It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

9. ACCESS TO AND SECURITY OF, MONITORING AREA AND ASSOCIATED EQUIPMENT

Authorised use of the CCTV System
Only trained and authorised personnel will operate any of the equipment located within the CCTV monitoring area, (or equipment associated with the CCTV system).

Public access

Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the System Manager. Any such visits will be conducted and recorded.

Authorised Visits
Visits by inspectors or auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning. No more than (two) inspectors or auditors will visit at any one time. Inspectors or Auditors will not influence the operation of any part of The System during their visit. The visit will be suspended in the event of it being operationally inconvenient. Any such visit should be recorded in the same way as that described above.

Declaration of Confidentiality
Regardless of their status, all visitors to the CCTV monitoring room, including inspectors and auditors, will be required to sign a declaration.

Recommended wording is as follows:-

'In signing this visitors book all visitors to the CCTV monitoring area acknowledge that the precise location of the CCTV monitoring room and personal details of those operating The System, is, and should remain confidential. They further agree not to divulge any information obtained, overheard or overseen during their visit.'

It is also best practice to display a notice at the entrance to the room that they are entering a restricted area, and entry is dependent upon acceptance of the need for confidentiality. A typical notice is included in Appendix D.

Security
Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the room will be secured.

10. MANAGEMENT OF RECORDED MATERIAL

Guiding Principles
For the purposes of this document 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of The System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.

Every video or digital recording obtained by using The System has the potential of containing material that has to be admitted in evidence at some point during its life span. Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of The System, will be treated with due regard to their individual right to respect for their private and family life.

It is therefore of the utmost importance that irrespective of the means or format (e.g. paper copy, video tape, digital tape, CD, or any form of electronic processing and storage) of the images obtained from The System, they are treated strictly in accordance with this document from the moment they are received by the monitoring room until final destruction. Every movement and usage will be meticulously recorded.

Access to and the use of recorded material will be strictly for the purposes defined in this document only.

Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

National standard for the release of data to a third party
Every request for the release of personal data generated by this CCTV System will be channelled through the System Manager. The System Manager will ensure the principles contained within Appendix C to this Document are followed at all times.

In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:
1. Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this document;
2. Access to recorded material will only take place in accordance with the standards outlined in this Document;
3. The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Members of the police service or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded.

Note: Release to the media of recorded information, in whatever format, which may be part of a current investigation, would be covered by the Police and Criminal Evidence Act, 1984. Any such disclosure should only be made following authorisation from the System Manager.

If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix C.

It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV system will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

Video Tapes - Provision & Quality
To ensure the quality of the tapes, and that recorded information will meet the criteria outlined by current Home Office guidelines, the only video tapes to be used with The System are those which have been specifically provided in accordance with the Operations Manual.

Tapes – Retention
Recorded tapes will be retained for a period of one calendar month. Before reuse or destruction, each tape will be magnetically erased in full accordance with the manufacturer's requirements.

Videotapes will be always be used and stored in accordance with the Operations Manual. At the conclusion of their life within the CCTV System they will be destroyed and the destruction certified.

Tape Register
Each tape will have a unique tracking record maintained in accordance with the operations manual, which will be retained for at least three years, after the tape has been destroyed. The tracking record shall identify every use, and person who has viewed or had access to the tape since the initial breaking of the seal to the destruction of the tape.

Recording Policy
Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period in 4-hour real time mode, through multiplexers onto S-VHS videotapes. The number of images through each multiplexer will be such that the time between successive frames once played back in time lapse mode shall not exceed 2 seconds.

Images from selected cameras will be recorded in real time at the discretion of the CCTV operators or as directed by the System Manager.

Evidential Tapes
In the event of a tape being required for evidential purposes the procedures outlined in the document will be strictly complied with.

11. VIDEO PRINTS

Guiding Principles
A video print is a copy of an image or images which already exist on video tape/computer disc. Such prints are equally within the definitions of 'data' and recorded material.

Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken.

Video prints contain data and will therefore only be released under the terms of Appendix C to this Document, 'Release of data to third parties'. If prints are released to the media, (in compliance with Appendix C), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with this document.

A record will be maintained of all video print productions in accordance with this document. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken.

Appendix A. Key Personnel and Responsibilities

System Owner
Little Heaton CE Primary School
Tel: 0161 672 0555
Address: Boardman Lane, Rhodes, Middleton M24 4PU

Responsibilities:
Little Heaton CE Primary School is the 'owner' of The System.
The school's role will include a responsibility to:

1. Ensure the provision and maintenance of all equipment forming part of The System in accordance with contractual arrangements, which the owners may from time to time enter into.

2. Agree to any proposed alterations and additions to The System, this document.

System Manager
Mrs C Crawford – Head of School
Tel: 0161 672 0555
Address: Little Heaton CE Primary School, Boardman Lane, Rhodes, Middleton M24 4PU

Responsibilities:
The Headteacher is the 'manager' of The System.

They have delegated authority for data control on behalf of the 'data controller'.

Their role includes responsibility to:

1. Maintain day to day management of The System and staff;

2. Accept overall responsibility for The System and for ensuring that this document is complied with.

Appendix B. Extracts from Data Protection Act 1998

Section 7
(1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled:
(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.
(b) If that is the case, to be given by the data controller a description of –
(i) the personal data of which that individual is the data subject;
(ii) the purpose for which they are being or are to be processed;
(iii) the recipients or classes of recipients to whom they are or may be disclosed,
(c) to have communicated to him/her in an intelligible form:
(i) the information constituting any personal data of which that individual is the data subject;
(ii) any information available to the data controller as the source of those data;
(d) where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him/her such as, for example, his/her performance at work, his/her creditworthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, to be informed by the data controller of the logic involved in that decision-taking
(2) A data controller is not obliged to supply any information under subsection (1) unless he/she has received:
(a) A request in writing, and
(b) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he/she may require.
(3) A data controller is not obliged to comply with a request under this section unless he/she is supplied with such information as he/she may reasonably require in order to satisfy him/herself as to the identity of the person making the request and to locate the information which that person seeks.
(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he/she is not obliged to comply with the request unless:
(a) The other individual has consented to the disclosure of the information to the person making the request, or
(b) It is reasonable in all the circumstances to comply with the request without the consent of the other individual.
(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of

the other individual concerned, whether by omission of names or other identifying particulars or otherwise.
(6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
(a) Any duty of confidentiality owed to the other individual,
(b) Any steps taken by the data controller with a view to seeking the consent of the other individual,
(c) Whether the other individual is capable of giving consent, and
(d) Any express refusal of consent by the other individual.
Note: In considering such instances the data controller must effectively also consider the degree of privacy that the third parties might or might not reasonably expect in being at that location at that time.
(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her request is limited to personal data of any prescribed description.
(8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.
(9) If a court is satisfied on the application of any person who has made a request under the forgoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him/her to comply with the request.
In this section: 'prescribed' means prescribed by the Secretary of State by regulations; 'the prescribed maximum' means such amount as may be prescribed; 'the prescribed period' means forty days or such other period as may be prescribed; 'the relevant day', in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection(3).
(10) Different amounts or periods may be prescribed under this section in relation to different cases.

Note: These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety.

Copies of the act and the Information Commissioners document can be downloaded from their website www.dataprotection.gov.uk

Section 8
(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.
(2) The obligation imposed by section 7(1) (c) (i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:
(a) The supply of such a copy is not possible or would involve disproportionate effort, or
(b) The data subject agrees otherwise;
(c) And where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.
(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.
(4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.
(5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.
(6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of

any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request. (7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Note: These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety.

Copies of the act and the Information Commissioners document can be downloaded from their website www.dataprotection.gov.uk

Appendix C. National Standard for the release of data to third parties

1. Introduction
Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect and support of the general public, The Systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

The School is committed to the belief that everyone has the right to respect for his or her private life. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who express concern tend to do so over the handling of the information (data) which The System gathers.

2. General Policy
All requests for the release of data shall be processed in accordance with the Procedure Manual. All such requests shall be channelled through the data controller.
Note: The *data controller* is the person who (either alone or jointly with others) determines the purpose for which and the manner in which any personal data are, or are to be processed. (In most cases the data controller is likely to be the scheme owners or for a 'School' the partners share responsibility). Day to day responsibility may be devolved, usually to The System Manager.

3. Primary Request To View Data
a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
ii) Providing evidence in civil proceedings or tribunals
iii) The prevention of crime
iv) The investigation and detection of crime (may include identification of offenders)
v) Identification of witnesses
b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
i) Police (1)
ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
iii) Solicitors (2)
iv) In civil proceedings (3)
v) Accused persons or defendants in criminal proceedings (3)
vi) Other agencies, (which should be specified in the Document) according to purpose and legal status (4).

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:
i) Not unduly obstruct a third party investigation to verify the existence of relevant data.
ii) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena.
A time limit shall be imposed on such retention, which will be notified at the time of the request.

Note: A time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (e.g. a time limit was about to expire).

d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative, shall:
i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
ii) Treat all such enquiries with strict confidentiality.

Notes

(1) The release of data to the police is not to be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (It may be appropriate to put in place special arrangements in response to local requirements).

(2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred.

In all circumstances data will only be released for lawful and proper purposes.

(3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(4) The data controller shall decide which (if any) “other agencies” might be permitted access to data. Having identified those ‘other agencies’, such access to data will only be permitted in compliance with this Standard.

(5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour).

4. Secondary Request to View Data
a) A ‘secondary’ request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:
i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);
ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);
iii) Due regard has been taken of any known case law (current or past) which may be relevant,

(E.g. R v Brentwood BC ex p. Peck) and
iv) The request would pass a test of 'disclosure in the public interest' **(1)**.
b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:
i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Document **(2)**.
ii) If the material is to be released under the auspices of 'public wellbeing, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV Code of Practice.
c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

Any requests to view data should be recorded on the CCTV log sheet as at Appendix H.

Note:
(1) 'Disclosure in the public interest' could include the disclosure of personal data that:
i) provides specific information which would be of value or of interest to the public well being
ii) identifies a public health or safety issue
iii) leads to the prevention of crime
(2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request, (see III above).

5. Individual Subject Access under Data Protection legislation
1) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
i) The request is made in writing;
ii) A specified fee is paid for each individual search;
iii) The data controller is supplied with sufficient information to satisfy him or herself as to the identity of the person making the request;
iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks,
(It is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);
v) The person making the request is only shown information relevant to that particular search and which contains personal data of her or himself only, unless all other individuals who may be identified from the same information have consented to the disclosure;
b) In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.
c) The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should be made to comply with subject access procedures and each request should be treated on its own merit.
d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:
i) Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
ii) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
iii) Not the subject of a complaint or dispute which has not been actioned;

iv) The original data and that the audit trail has been maintained;
v) Not removed or copied without proper authority;
vi) For individual disclosure only (i.e. to be disclosed to a named subject)

Template for access request at Appendix E

6. Process of Disclosure:
a) Verify the accuracy of the request.
b) Replay the data to the requester only, (or responsible person acting on behalf of the person making the request).
c) The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request shall be shown.
d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requester.

Note: The Information Commissioners Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.

7. Media disclosure
Set procedures for release of data to a third party should be followed, if the means of editing out other personal data does not exist on-site, measures should include the following;
a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:
i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.
ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Document).
iv)The release form shall be considered a contract and signed by both parties.
v) The Council's Media & Communications service should be notified prior to release.

8. Principles
In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:
a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in this document for the CCTV scheme;
b) Access to recorded material shall only take place in accordance with this document;
c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix D. Restricted Access Notice

WARNING

RESTRICTED ACCESS AREA

Everyone, regardless of status, entering this area is required to complete an entry in the Visitors book.

Visitors are advised to note the following confidentiality clause and entry is conditional on acceptance of that clause:
Confidentiality Clause:

'In being permitted entry to this area you acknowledge that the precise location of the CCTV monitoring room is, and should remain, confidential. You agree not to divulge any information obtained, overheard or overseen during your visit. An entry accompanied by your signature in the Visitors book is your acceptance of these terms'.

Appendix E. Subject Access Request Form

LITTLE HEATON CE PRIMARY SCHOOL CCTV SURVEILLANCE SYSTEM
Data Protection Act, 1998

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

Your Rights
Subject to certain exemptions, you have a right to be told whether any personal data is held about you.

You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. RMBC will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

1. The other individual has consented to the disclosure of information, or
2. It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

School Rights
The School may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:
1. Prevention and detection of crime
2. Apprehension and prosecution of offenders
And giving you the information may be likely to prejudice any of these purposes.

Fee
A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, Postal Orders, etc. should be made payable to **'Little Heaton CE Primary School'**.

THE APPLICATION FORM: (N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)

Section 1 Asks you to give information about yourself that will help the School to confirm your identity. The School has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full face photograph of you.

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4: You must sign the declaration
When you have completed and checked this form, take or send it together with the required TWO Identification documents, photograph and fee to:
THE CCTV MANAGER, Little Heaton CE Primary School, Boardman Lane, Rhodes, Middleton M24 4PU
(If you have any queries regarding this form, or your application, please ring the CCTV Manager on Tel No. 0161 6720555.

The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you.

PLEASE USE BLOCK LETTERS
Title (Circle as appropriate) Mr Mrs Miss Ms
Other title (e.g. Dr., Rev., etc.)
Surname/family name
First names
Maiden name/former names
Sex (Circle as appropriate) Male Female
Date of Birth
Place of Birth Town/County
Your Current Home Address
(to which we will reply)
A telephone number will be helpful in case you need to be contacted. Tele No.

SECTION 2: Proof of Identity
To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address.
Failure to provide this proof of identity may delay your application.

SECTION 3: Supply of Information
You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to;
(a) View the information and receive a permanent copy
(b) Only view the information

SECTION 4: Declaration
DECLARATION (to be signed by the applicant)
The information that I have supplied in this application is correct and I am the person to whom it relates.
Signed by Date
Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

If the information you have requested refers to a specific offence or incident, please complete this Section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.

If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.
Were you: (circle as appropriate)
A person reporting an offence or incident
A witness to an offence or incident
A victim of an offence
A person accused or convicted of an offence
Other – please explain

Date(s) and time(s) of incident
Place incident happened
Brief details of incident

Before returning this form • Have you completed ALL Sections in this form?
Please check: • Have you enclosed TWO identification documents?
• Have you signed and dated the form?
• Have you enclosed the £10.00 (ten pound) fee?

Further Information:
These notes are only a guide. The law is set out in the Data Protection Act, 1998, obtainable from The Stationery Office. Further information and advice may be obtained from:
The Information Commissioner,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.
Tel. (01625) 545745
Please note that this application for access to information must be made direct to XXXXM.B.C. (address on Page 1) and **NOT** to the Data Protection Commissioner.

OFFICIAL USE ONLY
Please complete ALL of this Section (refer to 'CHECK' box above).
Application checked and legible?
Date Application Received
Identification documents checked?
Fee Paid Details of 2 Documents (see page 3) Method of Payment
Receipt No.
Documents Returned?
Member of Staff completing this Section:

Name:

Location:

Signature:

Date:

Appendix G. Regulation of Investigatory Powers Act Guiding Principles: Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act 2000 came into force on 2nd October last. It relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:-

*Subject to subsection (6), surveillance is directed for the purposes of this Part if it is **covert** but **not intrusive** and is undertaken-*
(a) For the purposes of a specific investigation or a specific operation;
(b) In such a manner as is likely to result in the obtaining of private information about a person (Whether or not one specifically identified for the purposes of the investigation or operation); and
(c) Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance

CCTV being used intrusively will be authorised other than by this section of the RIP Act. Appropriate guidelines already exist for intrusive surveillance.

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will fall into sub section c above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The document says some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authority will almost certainly be required. Slow time requests are authorised by a Superintendent or above. If an authority is required immediately, an Inspector may do so. The forms in both cases must indicate the reason and should fall within one of the following categories:-

An authorisation is necessary on grounds falling within this subsection if it is necessary-
(a) In the interests of national security;
(b) For the purpose of preventing or detecting crime or of preventing disorder;
(c) In the interests of the economic well-being of the United Kingdom;
(d) In the interests of public safety;
(e) For the purpose of protecting public health;
(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
(g) For any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then in writing by way of the forms. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

Examples:
Insp. Authorisation
An example of a request requiring Inspector authorisation might be where a car is found in a car park late at night and known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Supt Authorisation
Where crime squad officers wish to have a shop premises monitored from the outside, which is suspected of dealing in stolen goods over a period of days.
No Authorisation
Where officers come across a local drug dealer sitting in the town centre/street and wish to have the cameras monitor them, so as not to divulge the observation taking place.

Appendix H. CCTV – log of requests to view CCTV footage