Forty Hill CE Primary School

Code of Practice

For the operation of

Closed Circuit Television

Version Control

Item	Reason for Change	Version	Author	Date
1	Created based on v12 of the LBE CCTV code	1.0	Steve Durbin	17/06/2019
2	Legislation update – post-Brexit	2.0	Rezaur Choudhury	09/06/2021

Section 1 Introduction and Objectives

1.1 Introduction

1.1.1 A Closed-Circuit Television (CCTV) system has been introduced to Forty Hill CE Primary School and comprises a number of cameras installed at strategic locations. All of the cameras are fully operational, with most being fixed. Others are pan, tilt and zoom facility type cameras, images from which are presented in the same room.

1.1.2 For the purposes of this document, the 'owner' of the system is Forty Hill CE Primary School

1.1.3 For the purposes of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (hereinafter "the data protection legislation") the 'data controller' is Forty Hill CE Primary School The school is registered with the Information Commissioner, registration number Z924592X.

1.1.4 The 'system manager' is Claire Behling (SBM)

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

1.1.6 It is recognised that operation of the school's CCTV System may be considered to infringe on the privacy of individuals. The school recognises that it is their responsibility to ensure that CCTV on the premises should always comply with all relevant legislation, to ensure its legality and legitimacy. CCTV 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 well-being 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.

1.1.7 The legislation concerning CCTV in s.30 of the Protection of Freedoms Act 2012 has produced a CCTV Code of Practice from the new Surveillance Camera Commissioner that has been approved by Parliament and the school must pay due regard to the new code.

1.1.8 The school in managing its CCTV operations under this Code of practice will endorse and comply with all 12 guiding principles of the Surveillance Camera Code of Practice (see Appendix C).

1.1.9 The Codes of Practice and observance of the Operational Procedures contained in the manual 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.

1.1.10 The school 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.

1.2 Objectives of the System

1.2.1 The objectives of the school CCTV System which form the lawful basis for the processing of data are: -

- To help reduce the fear of crime
- To help deter crime
- To help detect crime and disorder or other public safety issues and provide evidential material suitable for court proceedings
- To assist in the overall management of the school and other public areas within its client base
- To assist the Local Authority in its enforcement and regulatory functions within the London Borough of Enfield area
- To assist in supporting civil proceedings which will help detect crime

- Any other specific objective identified by the owners or partners

1.3 Procedural Manual

1.3.1 This Code of Practice (hereafter referred to as 'the Code') is supplemented by a separate 'Procedural Manual' which offers instructions on all aspects of the day to day operation of the system that is an OFFICIAL-SENSITIVE document. To ensure the purpose and principles (see Section 2) of the CCTV system are realised, the procedural manual is based and expands upon the contents of this Code of Practice.

Section 2 Statement of Purpose and Principles

2.1 Purpose

2.1.1 The purpose of this document is to state the intention of the school in respect of use of CCTV, and as far as is reasonably practicable and to outline how it is intended to do so.

2.1.2 The 'Purpose' of the CCTV system, and the process adopted in determining the 'Reasons' for implementing 'The System' are as previously defined in order to achieve the objectives detailed within Section 1.

2.2 General Principles of Operation

2.2.1 The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

2.2.2 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 local police force policy.

2.2.3 There is a procedure for directed surveillance requests from third party organisations wishing to use this facility. Directed Surveillance Forms are available from the Monitoring Centre and the procedure and forms are included in the Procedural Manual.

2.2.4 The system will be operated in accordance with the data protection legislation at all times and comply with the Protection of Freedoms Act 2012 CCTV Code of Practice 12 guiding principles as contained in Appendix C and in accordance with the school's data protection policy.

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

2.2.6 The system will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.

2.2.7 The public interest in the operation of the system will be recognised by ensuring the security and integrity of its operational procedures is maintained.

2.2.8 Throughout this Code of Practice, it is intended, as far as reasonably possible, to balance the objectives of the CCTV System with the need to safeguard the individual's rights. Every effort has been made throughout this Code 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.

2.2.9 Participation in the system by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Code and to be accountable under this Code of Practice.

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

2.3 Cameras and Area Coverage

2.3.1 The areas covered by CCTV to which this Code of Practice refers are the public areas within the responsibility of the operating partners and cover Enfield Borough and other client areas as may be monitored by The System.

2.3.2 Some of the cameras offer full colour, pan tilt and zoom (PTZ) capability, High Definition (HD) recording, or may automatically switch to monochrome in low light conditions.

2.3.3 None of the cameras forming part of the System will be installed in a covert manner. Some cameras may be enclosed within 'All weather domes' for aesthetic or operational reasons but the presence of all cameras will be identified by appropriate signs.

2.3.4 Cameras located around and within the school are primarily for the protection of the school but may be used for crime prevention and detection as appropriate. Internal cameras are primarily for security and are part of the schools. The system may also be used for school management, performance and probity issues and are appropriately signed.

2.3.5 A list showing the number and location of all site cameras previously attached to these Codes is now displayed on the school's website.

2.3.6 Authorised users of the system may be permitted to have access to recorded data by remote secure terminals. Data handling and audit will apply in accordance with DPA and this code.

2.4 Human Resources

2.4.1 Unauthorised persons will not have access to site without an authorised member of staff being present

2.4.2 All authorised users of the school system should receive training relevant to their role in the requirements of the Human Rights Act 1998, the data protection legislation, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Progressive and continuation and formal refresher

2.5 Processing and Handling of Recorded Material

2.5.1 Unauthorised persons will not have access to site without an authorised member of staff

2.5.2 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 Code of Practice and the School's Procedural Manual.

2.6 Operators Instructions

2.6.1 Technical instructions on the use of equipment are contained in a separate manual provided by the equipment suppliers.

2.7 Changes to the Code of Practice

2.7.1 Any major changes to either the Code of Practice or upon the operation of the system will take place only after consultation with and upon the agreement of the CCTV Management within the Authority in the operation of the system.

2.7.2 A minor change, (i.e. such as may be required for clarification or that will not have such a significant impact) may be agreed by the Centre Manager and notified to those responsible for the Management of the system.

Notes.

I. 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.

II. 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.

III. The use of 'dummy' cameras as part of this CCTV System is NOT PERMITTED.

Section 3 Privacy and Data Protection Public Concern

3.1 Privacy

3.1.1 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;*

i) Organisation, adaptation or alteration of the information or data;

ii) Retrieval, consultation or use of the information or data;

iii) Disclosure of the information or data by transmission, dissemination or otherwise making available, or

iv) Alignment, combination, blocking, erasure or destruction of the information or data.

3.1.2 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 total respect for everyone's right to respect for his or her private and family life and their home.

3.1.3 Personal Data will be limited in the majority of data collected and recorded by this system and is defined as that reaching "recognition level" of an individual based upon the research and guidance taken from the Home Office Scientific Development Branch where the individuals details of head and torso are recorded at 50% of screen height or greater. Below this resolution level, it is not deemed Personal Data.

3.1.4 The storage and security of the data will be strictly in accordance with the requirements of the data protection legislation, other statutory legislation and additional locally agreed procedures.

3.2 Data Protection Registration

3.2.1 The school is registered with the Information Commissioner as a data controller, details are given in Section 1.

3.2.2 All data will be processed in accordance with the principles of the data protection law which state, in summary form that all personal information will be:

1) Processed lawfully, fairly and in a transparent manner
2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3) Adequate, relevant and limited to what is necessary
4) Accurate and, where necessary, kept up to date
5) Kept in a form which permits identification of data subjects for no longer than is necessary
6) Processed in a manner that ensures appropriate security

3.3 Signage

3.2.1 Data protection legislation compliant signage will be used throughout the covered area, example given below

3.3 Request for information (subject access)

3.3.1 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 data controller.

3.3.2 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 current Data Protection legislation.

3.3.3 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. An appropriate 'Subject Access' request form is available on the school website, although its use is not compulsory.

3.4 Exemptions to the Provision of Information

3.4.1 In considering a request made under the subject access provisions, reference may also be made to Schedule 2 Part 1 Para 2 of the Act which includes, but is not limited to, the following statement:

3.4.2 Personal Data processed for any of the following purposes -

a) the prevention or detection of crime

b) the apprehension or prosecution of offenders

are exempt from the subject access provisions in any case 'to the extent that the application of the listed provisions would be likely to prejudice any of the matters mentioned in paragraph (a) or (b).'

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

3.5 Criminal Procedures and Investigations Act, 1996

3.5.1 The Criminal Procedures and Investigations Act, 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the presentation of its own case, (known as unused material). An explanatory summary of the provisions of the Act is contained within the procedural manual, but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by the Data Protection Act 2018.

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, and in accordance of the School's requirements, access to the output of the cameras is restricted and in accordance with this Code of Practice.

4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' may 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. In any case, if such 'zones' are not programmed; all operators will be specifically trained in privacy issues.

4.1.3 To ensure probity and audit of the CCTV system all cameras will record at varying frame rates according to need and retained for a minimum period of 31 days for street CCTV or 14 days' minimum for High Definition (HD) cameras and remote building CCTV systems but may vary up to 31 days dependant on risk.

4.1.4 Independent inspection, Inspectorate Audits and regular audit and maintenance checks by staff will ensure that all cameras are recording 24/7 and to the required quality and all faults rectify.

4.1.5 Any member of the public wishing to register a complaint with regard to any aspect of CCTV cameras may do so by contacting the data controller. All complaints shall be dealt with in accordance with the school's complaints procedure. Data Protection complaints will be dealt with under the school's data protection policy. Policies are available on the school's website or from the school office. Any performance issues identified will be considered under the organisation's disciplinary procedures to which the workforce of the school, including personnel with access to CCTV are subject.

4.1.6 All staff are contractually subject to regulations governing confidentiality and discipline. Any individual member of the public who suffers damage or distress by reason of any contravention of this Code of Practice may be entitled to compensation.

4.2 System Owner

4.2.1 The system owner as documented at Appendix A, will have unrestricted personal access to the CCTV cameras and will be the responsible Officer for receiving regular and frequent management, operational, emergency and performance reports with the general responsibility for the operation of the system.

4.2.2 Formal consultation will take place between the governors, head teacher and the manager of the system with regard to all aspects of this Code of Practice.

4.3 System Centre Manager

4.3.1 The nominated manager named at Appendix A will have day-to-day responsibility for the system as a whole.

4.3.2 The system may be subject to audit by London Borough of Enfield's audit body, (or nominated deputy whose organisational level of responsibility is at least equal to that of the system manager, but who is not the system manager).

4.3.3 The system may also have independent external DPA audits of the operation and compliance with all aspects of DPA and any issues or breaches found will be reported to the system manager and processes addressed as required.

4.3.4 The system manager will ensure that every complaint is reported through to the school's complaint process.

4.4 Public Information

4.4.1 Code of Practice

A copy of this Code of Practice shall be published on the school's web site, and a copy will be made available

to anyone on request.

4.4.2 System performance information

System performance will be closely monitored and recorded and compiled into annualised year on year data that shall be made publicly available on the school's website and to anyone requesting it in accordance with the POF Act 2012 transparency requirements.

4.4.3 Signs

Signs as per the example at 3.33.3 above will be placed in the locality of the cameras and at main entrance points to the relevant areas.

The signs will indicate:

i) The presence and stated purpose of CCTV monitoring;

ii) The 'ownership' of the system;

iii) Contact telephone number of the 'data controller' of the system.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 The system will undergo Annual Inspectorate audits to relevant British standards to maintain its accreditations for all services it delivers including BS 7958 CCTV Management and Operation. Results of the audits will be used to review and develop improvements to processes and maintain accredited service delivery standards.

5.1.2 In addition, monthly and annual reviews of the performance of the system will be collated and reviewed in accordance with the POF Act 2012 and any recommended changes or alterations to the specified purpose and objectives of the school.

5.1.3 It is intended that performance evaluations of the system should take place at least annually.

5.2 Monitoring

5.2.1 5.2.1 The system manager will accept day to day responsibility for the monitoring, operation and evaluation of the system and the implementation of this Code of Practice.

5.2.2 5.2.2 The system manager shall also be responsible for maintaining full management information as to the incidents dealt with at the school, for use in the management of the system and in annual performance evaluations.

5.3 Audit

5.3.1 The London Borough of Enfield's auditor or other appropriate person, nominated deputy, who is not the system manager, will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, videotape histories and the content of recorded material.

5.3.2 The London Borough of Enfield's auditor or other appropriate person, nominated deputy, who is not the system manager, will conduct ad-hoc external DPA audits or operational compliance audits by use of Independent Inspectors who are voluntary local residents appointed to review the systems operation and compliance to this code and the POF Act 2012 guiding principals

Section 6 Human Resources

6.1 SCHOOL WORKFORCE responsible for the operation of the system

6.1.1 The CCTV cameras will be staffed and operated in accordance with the procedural manual. Equipment associated with will only be operated by authorised personnel who will have been properly trained in its use and all procedures including this Code of Practice.

6.1.2 Every person involved in the management and operation of the system will be personally trained in both the Code of Practice and the Procedural Manual, and be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he / she will be expected to comply with as far as is reasonably practicable at all times.

6.1.3 Arrangement may be made for a police liaison officer to be present to view CCTV information at certain times, or indeed at all times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedural Manual and passed CCTV training competency levels as required by the system manager.

6.1.4 All personnel involved with the system shall receive regular continuation training and formal refresher training annually in respect of all legislation appropriate to their role.

6.2 Discipline

6.2.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be subject to the school's discipline code, or if contracted staff their own Company discipline procedure's. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

6.2.2 The system manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day to day responsibility for the management of the school's CCTV cameras and for enforcing the discipline rules. Non-compliance with this Code of Practice by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

6.3 Declaration of Confidentiality

6.3.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be required to sign a declaration of confidentiality.

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

7.1.1 Any person operating the cameras will act with utmost probity and within the law at all times.

7.1.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been formally trained in their use, or under their direct supervision if under training, and the legislative implications of their use to the standard directed and required by the system manager.

7.1.3 7.1.2 Every use of the cameras will accord with the purposes and key objectives of the system and shall be in compliance with this Code of Practice.

7.1.4 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. Privacy zones will be regularly checked by responsible staff and logged and or faulted as required.

7.1.5 Primary camera “parking” positions and all camera tours shall also be in line with DPA and Human Rights legislation, whether by manual or automatic means to ensure the respect for individual’s privacy.

7.1.6 7.1.5 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.

7.2 Primary Control

7.2.1 Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls for the system.

7.3 Secondary Control

7.3.1 There is no secondary control of this system’s operating control system.

7.4 Operation of The System by the Police

7.4.1 Under extreme circumstances the Police may make a request to assume direction of The System to which this Code of Practice 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 if approved and authorised by the representative of the System owners, the system manager, or his/her designated deputy of at least equal standing in their absence.

7.4.2 In the event of such a request being permitted, the system will continue to be staffed, and CCTV equipment operated by, only those personnel who are trained and authorised to do so, and who fall within the terms of Section 6 and Section 7 of this Code. They will then operate under the direction of the police officer designated in the written authority.

7.4.3 There is no capability for the police to physically move or control cameras though the ability to view live images for directed management as in and operational control is in place.

7.4.4 Any agreed future capability of the Enfield Public Safety Centre to provide secure remote access to images for live streaming and or bulk data transfer to the police or other agencies will be subject to future agreement and security of data and audit processes approved by the Centre Manager.

7.5 Maintenance of the system

7.5.1 The school compliances with the Information Commissioners Code of Practice and ensures that images recorded continue to be of appropriate evidential quality and CCTV cameras are maintained to the correct standard.

7.5.2 Any maintenance contract 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 and recording quality.

7.5.3 The maintenance will also include regular periodic overhaul of all the equipment and replacement of any equipment, which is reaching the end of its serviceable life, or does not perform to its operational requirement as required under the Data Protection Act.

7.5.4 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.

7.5.5 The maintenance agreement will define performance criteria 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.

7.5.6 If cameras or other equipment is not functioning and beyond its operational or effective service they are to be replaced promptly and/or the old equipment removed from the system to maintain probity and compliance of the systems effectiveness.

7.5.7 It is the responsibility of the SCHOOL BUSINESS MANAGER to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the system maintenance contractor.

Section 8 Access to, and Security of, Monitoring Centre & Associated Equipment

8.1 Authorised Access

8.1.1 Only trained and authorised personnel will operate any of the equipment located within the school or other equipment associated with the System.

8.2 Public access

8.2.1 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 approved and conducted and recorded in accordance with the Procedural Manual and to the BS 5979 Alarm Receiving Centre requirements to maintain its accreditation.

8.3 Authorised Visits

8.3.1 Visits by Independent 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, but they must be escorted at all times. 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 suspended should be recorded in the same way as that described above including the reason for suspension given.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, all visitors to the school, including inspectors and auditors, will be required to sign the visitor's book and in doing so accept the declaration of confidentiality.

8.5 Security

8.5.1 In the event of the school having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with.

Section 9 Management of Recorded Material

9.1 Guiding Principles

9.1.1 **For the purposes of this Code '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 by way of video copying, including video prints.

9.1.1 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. It is a requirement that all Cameras operated by this system are recorded 24/7 if their operational requirement and purpose is crime detection and prevention or public safety.

9.1.2 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. There is an expectation that the public expect The System to be recording 24/7 and to a quality standard able to be provided and admitted in evidence if required.

9.1.3 It is therefore of the utmost importance that irrespective of the means or format (e.g. paper copy (still print), digital tape, CD, DVD, portable hard drive, or any form of electronic network transfer processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code of Practice and the Procedural Manual from the moment they are received until final destruction (or digital overwrite). Every movement and usage of recorded material will be meticulously logged as must the regular daily inspection of recordings of all cameras and all faults notified according to procedures.

9.1.4 Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice or other Codes in use for other services provide by the school only.

9.1.5 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment save that of educational value (if personal data redacted)

9.2 National standard for the release of data to a third party

9.2.1 Every request for the release of personal data generated by this CCTV System will be channelled through the SCHOOL BUSINESS MANAGER. The SCHOOL BUSINESS MANAGER will ensure the principles contained within Appendix B to this Code of Practice are followed at all times.

9.2.2 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:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice;
- Access to recorded material will only take place in accordance with the standards outlined in Appendix B and this Code of Practice;
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

9.2.3 Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with Appendix B, 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 in accordance with the Procedural Manual.

9.2.4 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 B and the Procedural Manual.

9.2.5 It may be beneficial to make use of 'real' media 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 will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3 Recording media - Provision & Quality

9.3.1 To ensure the quality of the digital media, and that recorded information will meet the criteria outlined by current Home Office guidelines, a networked digital recording system and specification has been used which conforms to the best practice guidance identified by the CAST (Centre for the Applied Science and Technology) of the Home Office and of BS 62676 the new standard for *Video Surveillance Systems for use in Security Applications*.

9.4 Media – Retention

9.4.1 Recorded digital media will be retained for a minimum period of THIRTY ONE DAYS in line with Home Office recommendations in the case of community safety cameras, with the exception of 14 days for High Definition (HD) cameras. Sites with video CCTV alarm building security systems may record between 14 days and 31 days dependant on risk.

9.4.2 The digital networked recording system automatically overwrites any unused or unsaved material, which conforms to the DPA principal dealing with the requirement for unnecessary storage and retention of data.

9.4.3 Media will be always be used and stored in accordance with the Procedural Manual and produced according to PACE (Police and Criminal Evidence Act) standards. All cameras with an operational requirement of crime prevention and detection or public safety must record 24/7 at varying frame rates according to need but if street CCTV retained for 31 days, and to a quality standard to meet DPA requirements.

9.5 Media Register

9.5.1 The digital recording system has, in addition to any paper records and retains a unique audit record of all recordings produced from the system. The system records identify every use, and person who has viewed, produced evidence, or had access to the media in order to comply with the security of data principal requirement of the DPA Act. However, the handover of evidence document is the main process for evidence review, download and evidence handling and copies of these are scanned and retained.

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera will be digitally recorded throughout every 24-hour period at various frame rates according to need, onto digital hard disk drive HDD network servers.

9.6.2 Images from selected cameras that are being actively controlled by operators are in addition automatically digitally recorded in real time onto the real-time network server during their selection and control by operators as a means of audit of operators work and usage of cameras.

9.7 Evidential media

9.7.1 In the event of media being required for evidential purposes the procedures outlined in the Procedural Manual will be strictly complied with.

Section 10 Still Image Prints

10.1 Guiding Principles

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

10.1.2 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 in accordance with the Procedural Manual.

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

10.1.4 A record will be maintained of all video print productions in accordance with the Procedural Manual. 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.

10.1.5 The records of the video prints taken will be subject to audit in common with all other records in the system.

Appendix A Key Personnel and Responsibilities

System Owners

Your nominated representative:

Claire Behling (SBM)
Forty Hill CE Primary School
Enfield EN2 9EY
020 8363 0769
sbm@fortyhill.enfield.sch.uk

Responsibilities:
Forty Hill CE Primary School is the 'owner' of the system. The school's representative will be the single point of reference on behalf of the owners (the school). His/her role will include a responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of the school's CCTV cameras in accordance with contractual arrangements.

ii) Ensure the interests of the owners (the school) and other organisations or clients in the scheme are upheld in accordance with the terms of this Code of Practice.

iii) Agree to any proposed alterations and additions to the system, or this Code of Practice through the system owner.

System Management (OUTSOURCED CONTRACT)

Contact Details: Cohort – 07974 913796 (Simon)

For the individual(s) responsible for the day-to-day operation of the system under the management of the owner's representative.

Responsibilities:

The system owner as noted above is the owner of the school's CCTV System

Their role includes responsibility to:

i) Maintain day to day management of the system and staff;

ii) Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;

iii) Maintain direct liaison with operating partners and clients.

Appendix B National Standard for the release of data to third parties

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

After considerable research and consultation, the nationally recommended standard of The CCTV User Group has been adopted by the System owners.

1 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.

Day to day responsibility may be devolved, usually to the school business manager.

2 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) Plaintiffs in civil proceedings **(3)**

v) Accused persons or defendants in criminal proceedings **(3)**

iv) Other agencies, (which should be specified in the Code of Practice) 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 be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc.

(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)

3 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. UK GDPR, Data Protection Act 2018, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);

ii) Any legislative requirements have been complied with;

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 Code of Practice (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, preferably within the legal department. The officer should have personal knowledge of the potential benefit (and risks) to be derived from releasing the (or refusing to release) material and an understanding of the CCTV System 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.

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).

4 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) 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):

   iv) 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).

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)

5 Process of Disclosure:

a) Verify the accuracy of the request.

b) Replay the data to the requestee 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 that 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*.

6 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 Code of Practice).

iv) The release form shall be considered a contract and signed by both parties (1).

Note *in the well-publicised case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted unlawfully. A verbal assurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid future accidental broadcasts.*

Attention is drawn the requirements of the Information Commissioners in this respect detailed in her Code of Practice summarised above.

7 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 the Code of Practice for the CCTV scheme;

b) Access to recorded material shall only take place in accordance with this Standard and the Code of Practice;

c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited unless the purpose is to promote public safety and the schools permitted purposes, and only by prior agreement of the school.

Appendix C	Protection of Freedoms Act 2012, Sect 30, 12 Guiding Principals

Guiding Principles (Extract from Camera Surveillance Code of Practice June 2013)

2.1 System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.