BOLTON SCHOOL

CLOSED CIRCUIT TELEVISION

POLICY AND PROCEDURE

Published by:	Clerk & Treasurer
Date Published:	14 August 2020
Version number:	5
Approved by:	Senior Officers

Index of Contents

Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) camera system at Bolton School Foundation.

The School has various CCTV systems in operation comprising a number of fixed, dome and vehicle cameras located around the school campus, sites controlled by Bolton School and on school vehicles. Each of the CCTV systems is owned by Bolton School Foundation.

Details of each of the systems in operation and the corresponding 'responsible person' can be found in Appendix 1.

In addition the School's third party transport provider, Tyrers, has CCTV on each of the vehicles used to transport pupils. Tyrers' CCTV Code of Practice is shown as Appendix 5.

This Policy follows Data Protection Act guidelines and will be subject to regular review.

Objectives of the CCTV schemes

- To increase personal safety of staff, pupils, visitors and clients and reduce the fear of crime
- To protect the school buildings, their assets and vehicles
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To assist in managing the school and its grounds and what takes place therein

Statement of intent

The CCTV schemes are registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's CCTV Code of Practice.

The school will treat the systems and all information, documents and recordings obtained and used as data which is protected by the Act.

Cameras will be used to monitor activities within the school grounds and other sites controlled by Bolton School Foundation. They will be used to identify criminal activity anticipated, perceived to be or actually occurring, and for the purpose of securing the safety and well-being of the schools' pupils, staff and its visitors.

Responsible persons have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

CCTV will not be used specifically for monitoring the work of employees or the activities of pupils, parents and visitors. CCTV evidence may be used in the event that the facts of an incident need to be clarified or in disciplinary proceedings, against an employee where such evidence tends to show, in the reasonable belief of the employer, that the employee has been guilty of misconduct. The employee or other individual e.g. parents, (perhaps with their child) involved in the matter/incident will be given the chance to see and respond to the images in these circumstances.

Covert CCTV will only ever be set up for the investigation or detection of crime or serious misconduct. The use of covert CCTV will be justified only in circumstances where the investigator has reasonable suspicion that the crime or serious misconduct is taking place and where CCTV use is likely to be a

proportionate means of securing evidence. The use of covert CCTV can only be authorised by a Senior Officer.

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

The planning and design of the CCTV systems has endeavoured to ensure that the systems will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the CCTV.

Operation of the system

The schemes will be administered and overseen by the Clerk and Treasurer or nominees, in accordance with the principles and objectives expressed in the CCTV Code of Practice and this policy.

The day-to-day management will be the responsibility of the relevant responsible person for each system.

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

The relevant responsible person for each system will be required to regularly check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are working.

An impact assessment of each of the systems will be conducted on a regular basis by the relevant responsible person.

Image monitoring procedures

Image monitoring may be maintained at all times.

Viewing of live images on monitors will be restricted to those listed in Appendix 1 unless the monitor displays a scene which is also in plain sight from the monitor location.

Cameras will be pointed and focused on several points/areas agreed by the relevant responsible person. Only the relevant responsible person will modify or authorise the modification of camera positions. An Impact Assessment, (see appendix 2), should be completed in the event of a camera position being modified.

Image storage procedures

The responsible person for each CCTV system will ensure that the images are only held for a maximum of 31 days and are then overwritten. On occasions the images may be retained for longer when required for evidential purposes, in which case they will be retained until no longer needed.

Access to the stored images will be strictly controlled by a password system managed by the relevant manager.

Routine viewing of recorded images will be limited to:

- The relevant responsible person or in their absence a nominated deputy (see appendix 1)
- The Clerk and Treasurer or her nominee.

When circumstances require, the relevant responsible person and the Clerk and Treasurer will have authority to allow other members of staff to view recorded images. The names of staff other than those listed above who view the recorded images will be recorded in an Access Register, see appendix 3, held by the relevant responsible person.

Images may be viewed by the Police for the prevention and detection of crime, or by the insurers if a claim has been made against the school. A record will be made in the Register (maintained by the relevant responsible person) of the viewing. Requests by the Police will only be actioned if required by law. Should images be required as evidence, a copy may be released to the Police under their evidence guidelines. A record of this release will be made in the Register.

Images will only be released to the Police on the clear understanding that they remain the property of the school, and both the disk or file and information contained on it are to be treated in accordance with this policy. The school will also retain the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained thereon.

Applications received from outside bodies (e.g. solicitors, insurers) to view or release disks will be referred to the Clerk and Treasurer. In these circumstances disks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, an insurance claim, a subject access request, or in response to a Court Order.

Breaches of the Policy (including breaches of security)

Any breach of the CCTV Policy by staff will be investigated under the school's Disciplinary Policy and Procedure.

Complaints

Any complaints about the school's CCTV camera system or application of this policy should be addressed in writing to the Clerk and Treasurer.

Public Information

This policy will be made available to the public on the School website.

Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to see data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made to the Clerk and Treasurer in writing either using the Data Subject Access Request Form, see appendix 4, or providing the information requested in the form. Applicants will receive a response within 40 calendar days of the date the request was received by the School.

Appendix 1

Bolton School CCTV Responsible Persons

Oversees the systems **Point of contact for Subject Access Requests**	Clerk and Treasurer				
CCTV Camera System Locations	School Campus	Arts Centre	Lester Road and School Vehicles	Nursery	ICT Department
Responsible for System Reviews, Storage & Access to Images	Head of Estates and Logistics Coordinator	Events Manager and Leisure Services Manager	Logistics Coordinator and 3rd party contractor	Nursery Manager	Head of ICT Services
System Users (Can view images)	Security Officers Sergeants Receptionists	Clerk & Treasurer, Events Manager, Assistant Events Manager, Events Operations Manager, Leisure Services Manager, Assistant Leisure Services Manager	Clerk & Treasurer	Deputy Nursery Manager Team Leaders Administrators Receptionist	Head of ICT Services, ICT Infrastructure Manager, Other ICT Staff

Appendix 2 **Bolton School Impact Assessment for the use of CCTV**

This Impact Assessment should be completed on an annual basis by the Manager responsible for the CCTV system. The completed Impact Assessment should be retained in the relevant department for School records.

A. This is an impact assessment statement for the use of surveillance CCTV at:

Bolton School Estate, Chorley New Road, including Park Road Junior School and Beech House Infant School on Dobson Road, Bolton
Bolton School Nursery, Dobson Road, Bolton
Lester Road, Little Hulton, Manchester
ICT Department, Bolton School, Chorley New Road, Bolton

This assessment has been carried out by:

NAME: _____ POSITION: _____

The assessment is effective from ….. / ….. / 20 … until review on ….. / ….. / 20 ….

Registration with the Office of the Information Commissioner last updated on ….. / ….. / 20 ….

Checks for serviceability of CCTV systems and clarity of images last completed on ….. / ….. / 20 ….

B. Areas on the school campus covered by installed surveillance CCTV, whether active or not.

CAMERA AREA	**No.**

(A separate sheet should be completed for each area, giving precise details of the use of surveillance CCTV and the data collected from that area. It may be adequate to group together some areas where the information to be recorded is entirely or partially common, without loss of specific reference.)

C. Impact assessment for use of CCTV in …… (area)

Purpose(s) for use of surveillance CCTV:

Advantages of use of CCTV over other possible methods e.g. additional lighting, increased patrols:

Assessment of amount of equipment used and time equipment is active:

Specific ways in which data collected will be used, including restrictions:

For stored data, the method used, the maximum length of time of storage, and how the data might be used:

All personnel having immediate access to data collected and stored, as part of specific duties:
(Included are any servicing company's personnel with general access)

Details of how data may be processed, by whom and for what purpose(s):

Details of further personnel who may gain temporary access to data as part of their duties:

Methods of notification of the presence of surveillance CCTV and other information channels e.g. signage, induction:

Details of all method(s) by which images, or collected data from CCTV may be streamed to any outside agency or other parties, if relevant. Restrictions on access are also included:

Where an outside agency is entirely responsible for the operation and control of the CCTV equipment, its monitoring and the collection and use of data collected, all relevant and necessary details:

Assessment of any possible impact of CCTV surveillance on the right to privacy, performance or general well-being of any individuals:

Other relevant information:

Does the system and arrangements still comply with the School's CCTV Policy? If no, what action is to be taken, by when and by whom:

Appendix 3 - Bolton School CCTV Access Register

Date access granted	Name of individual to whom access was granted	Dates & times of images accessed	CCTV System and cameras from which images were shown	Purpose for which access to images was granted. NB Provide Crime Reference Number where relevant.	Has a copy of the images been provided? If so, in what format?	Has the individual to whom access was granted been provided with a copy of the CCTV Policy and received an explanation of the terms under which the images are provided?	Name of individual who granted access NB This should only be a Manager responsible for the system	Date and signature of person completing this register

Appendix 4

BOLTON SCHOOL

DATA SUBJECT ACCESS FORM

To:	Clerk and Treasurer Bolton School Chorley New Road Bolton BL1 4PA
From:	*(Name, Address, Telephone Number, E-mail)*

In accordance with the Data Protection Act 1998 and Bolton School CCTV Policy I request to see the images of me recorded by the CCTV camera system.

My request refers to the following:

Date:	
Time Start:	
Time End:	
Camera (please indicate the area of the School):	
Event/Activity:	
If you are not known to the Clerk & Treasurer, please provide a description of yourself and what you were wearing at the time:	

Signed: _____

Name (Printed): _____

Appendix 5

Tyrers School Transport - CCTV Code of Practice

1.0 INTRODUCTION

1.1 CCTV systems installed in Tyrers Coaches vehicles and premises are intended to:
1.2 • Provide a safer environment for staff, customers and members of the public on buses, in stations and in depots.
1.3 • Deter prospective offenders
1.4 • Assist in determining the cause and severity of accidents to assist in insurance claims.
1.5 • Lessen the costs associated with vandalism to properties and vehicles.
1.6 • Assist in preventing fraud by drivers and customers.
1.7 • Provide recordings under strictly regulated conditions to permit detection and identification of offenders.
1.2 This Code of Practice is designed to:

• Ensure that the CCTV System achieves its purpose with fairness and sensitivity.

1.3 The owner of these systems is:

• RS Tyrer Ltd, 168 Chorley Rd, Adlington, PR69LQ.

1.4 The areas covered and the equipment specification are:

• As detailed in the Operating and Maintenance Manuals supplied with the systems employed in the various locations.

• Any depot/vehicle at any location where Tyrers Coaches or its subsidiaries may operate from.

1.5 Copyright:

• Tyrers Coaches Ltd retains the copyright to images recorded and on any stills photographs produced from monitors operated by digital recording equipment recorded by this scheme. No image obtained from monitoring or recording activity can be reproduced by any organisation or by any individual without the express permission of the Data Protection Officer.

1.6 The System Manager is:

• Robert Tyrer Moorland Gate Industrial Estate, Cowling Rd, Chorley, PR69EA.

1.7 The System Operators are:

• As designated by the Data Protection Officer but no more than two per depot location and any bus/vehicle owned by the group.

1.8 All job name descriptions and equipment descriptions are noted in Appendix 1

2.0 DATA PROTECTION IMPLICATIONS

2.1 The System is:

• Registered with the Information Commissioners Office

3.0 CHANGES TO THE CODE

3.1 Changes to the Code can only be made by:

• Executive Officer/Director/Data Protection Officer.

4.0 MANAGEMENT OF THE SYSTEM

4.1 Overall responsibility for the CCTV scheme

• Lies with the Data Protection Officer.

4.2 The Data Protection Officer will arrange the following:

• Designate day to day responsibility to staff.

• Devise detailed operational guidelines and review operational arrangements and revise the Code of Practice where appropriate.

• Discuss any complaints from the public about operation of the system and take appropriate action.

• Designate persons to review the recorded digital images and tapes.

• Designate persons to remove recording discs for evidential purposes.

• Ensure that privacy is respected, and

• Ensure that requirements of the Data Protection Act are met.

5.0 PUBLIC INFORMATION

5.1 Camera Positioning:

• All areas that may be covered by cameras have appropriate notification signs advising of the existence of CCTV and the identity of the owner of the system.

5.2 A copy of this Code of Practice is available from:

• Data Protection Officer, Tyrers Coaches, 168 Chorley Rd, Adlington. PR69EA

6.0 INDIVIDUAL RIGHTS

6.1 Individual privacy:

• Must be appropriately safeguarded and given due regard.

• Private and family life and the home must be respected.

• Cameras must not be used to look into private property. Private residences may come into view only as part of a wide angle or long shot, or as a camera is panning past them, or a camera on a vehicle is driving past them.

• Tracking and monitoring of individuals must be justifiable.

• Must be considered in the operation of any system, in accordance with the relevant section of the Human Rights Act 1998 Individual Rights.

7.0 ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

7.1 The system shall be evaluated by the Data Protection Officer:

• To ensure that the purposes for which the system was established are being maintained.

• To ensure that the monitoring complies with the Code of Practice. This shall include carrying out an audit of the system including examination of records, disc histories and the content of recorded discs.

8.0 STAFF

8.1 Operators of CCTV:

• Shall be designated by the Data Protection Officer.

8.2 Staff training shall be provided:

• By the Data Protection Officer and/or another qualified individual authorised by the DPO and system suppliers when necessary.

8.3 Staff shall be required to:

• Maintain high standards of probity and confidentiality.

• Acknowledge receipt and understanding of this code of practice.

• Ensure proper use of the equipment or recordings. Any abuse or improper use may be the subject of disciplinary hearings.

9.0 COMPLAINTS

9.1 About the operator of the system from the public or others:

• Will be dealt with by the Data Protection Officer who will investigate the complaint and take the appropriate action in the event of any breach of this Code of Practice. This may lead to disciplinary proceedings.

9.2 A member of the public may also complain:

• To the Information Commissioners Office.

10.0 CONTROLS AND OPERATION OF CAMERAS

10.1 Operating Controls:

• Only staff with responsibility for using the equipment shall have access to operating controls.

10.2 Viewing:

• Cameras must not be used to look into private property or into sensitive areas concerning personal privacy.

10.3 Checking:

• Spot checks will be carried out to ensure compliance with the previous items and operators are aware that recordings are subject to routine audit and they may be required to justify their interest to a member of public or a particular property.

11.0 ACCESS TO AND SECURITY OF MONITORS/EQUIPMENT

11.1 Access to view monitors and/or to operate equipment:

• Shall be limited to the designated operators of the systems, the Data Protection Officer or designated staff and the Police.

11.2 Public access to or demonstration of monitors shall not be allowed, except:

• Where a demonstration is provided to an individual to reassure that a particular camera does not view into their private residence other than on an incidental basis

• Where recorded data is shown to the subject/s and they can provide a just cause, in writing, and the Data Protection Officer approves such request.

12.0 RECORDED MATERIAL

12.1 Register Storage:

• The data register must be stored in a secure cabinet or locked safe room and kept locked at all times when unattended.

12.2 Data Usage:

• Digital systems will have their hard drive left in the recording device and set to record a minimum of 10 days on a rolling basis. These will only be removed for necessary viewing of incidents and maintenance.

12.3 Data required for evidential purposes:

• Must be separately indexed and securely stored to avoid accidental use.

12.4 Disposal of data:

• The Data Protection Officer shall ensure the secure disposal or destruction of data when appropriate.

12.5 Labelling:

• Data and hard drives to be individually and uniquely identified and labelled by the Operator.

12.6 Suspicious Incidents:

• Where Police have reasonable grounds for believing that a suspicious incident has been recorded, a Police Officer will arrange to view the data or a copy on CD of a digital recording by contacting the DPO. The Police may remove the data from Tyrers Coaches as evidence as part of their investigation provided it is agreed by the DPO. This would normally be given except where it may incriminate RS Tyrer Ltd. In which case it should be ordered through the normal judicial process. The Data Protection Officer and the Police Officer will log all removals of such data in the data register.

12.7 Data Removal:

• Once the data has been removed by the Police Officer, the Police will assume full responsibility for its security and integrity as evidence to be produced in court.

12.8 Copy Discs:

• No copies of data will be made without the express permission of the Data Protection Officer.

• Copies shall not be made other than for the prevention or detection of crime, for the presentation of evidence in court or for access by the defence in accordance with the Data Protection Act. Or investigation by an insurance company.

12.9 Data Management:

• All data should be kept in a locked cabinet when unattended and data should not be stored without the cabinet. Access to the digital recording equipment on bus should be locked at all times, with only nominated people holding keys.

13.0 DEALING WITH INCIDENTS

13.1 Incidents which require Police investigation:

• Shall be referred to the local Police Station where designated local contacts will form a working relationship with the system administrator.