



GOVERNORS' CCTV AND WEBCAM PROCEDURES

Issue No	Author/ Owner	Date Written	Approved by Governors on	Comments
1	WF	April 2014	14 May 2014	
1.1	WF	October 2015	21 October 2015	Updated to include webcams
1.2	MM	November 2021	8 December 2021	Updated following installation of new system

Backwell School considers that:

- The CCTV (Closed Circuit Television) scheme can contribute to the security and health and safety of all students, staff and visitors.
- The purpose of the CCTV scheme at Backwell School is to provide continuous monitoring systems that assist with the protection of the property, law enforcement, traffic management, community safety and the reduction of crime and disorder, thereby improving the quality of life for the public in general and specifically to visitors to the Backwell School site.

Backwell School confirms that:

- The CCTV system at Backwell School has been notified to the Information Commissioner.
- The general management of CCTV at Backwell School is currently vested with the Head of Site Operations.
- The day to day management of the CCTV system is the responsibility of the Head of Site Operations.
- The Owner, Operator and Data Controller of the Scheme is the Headteacher, Backwell School, Station Road, Backwell BS48 3BX.
- The CCTV cameras will be in operation 24 hours a day, 7 days a week.
- Webcams will be in operation as necessary.
- The school will notify visitors to the site of the use of CCTV by signage at site entrances.
- Webcams used in a monitoring role shall be considered as an integral part of the CCTV installation throughout the remainder of this document and captured media and images are afforded the same levels of control and protection.

The purpose of this procedure is to regulate the use of CCTV systems and webcams at Backwell School. This procedure is based upon the Code of Practice published by the Information Commissioner, which set out the standards that must be met if the requirements of the Data Protection 1998 Act are to be met. Section 37 of the Data Protection Act is shown below.

Section 37 of the Data Protection Act

The Data Protection Act requires that all CCTV installations designed to provide either crime prevention, crime detection or to enhance the safety of people on site, must comply with the requirements of the Act. These are that:

- 1 Data must be processed fairly and lawfully.
- 2 Data can only be obtained for lawful purposes.
- 3 Data shall be adequate, relevant and not excessive
- 4 Data shall be accurate and kept up to date.
- 5 Data shall be kept secure and not be kept for longer than is necessary.
- 6 Data shall be processed in accordance with the rights of individuals under the Act.
- 7 Appropriate measures shall be taken to prevent unauthorised or unlawful processing of data against accidental loss, destruction or damage.
- 8 Personal data will not be transferred to a country outside European Economic Area.

Backwell School will meet its responsibilities under the Data Protection Act as follows:

1 Data must be processed fairly and lawfully

Cameras are sited in such a way that they only monitor those spaces which are intended to be covered by the equipment. The school will make every effort to ensure that cameras do not focus on private homes, gardens and other areas of private property.

Signs are placed so that students, staff and the public are aware that they are entering a zone which is covered by surveillance equipment; the signs stating "These premises are under CCTV surveillance".

2 Data can only be obtained for lawful purposes

Disclosure of images to third parties is permissible only in limited and prescribed circumstances. Examples of third parties are:

- Law enforcement agencies if the recorded image would assist in a specific criminal inquiry.
- Prosecution agencies.
- Relevant legal representatives.
- The media, but only in exceptional circumstances if it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. Permission must be obtained from the Headteacher prior to release.

Data obtained can only be used for the prevention or detection of criminal activity, the apprehension and prosecution of offenders and the safeguarding of students, staff and visitors.

Access to recorded images is restricted to only those who need to have access to achieve the purpose of using the equipment. This access is documented with the following information:

- The identity of the data subject or third party to whom disclosure was made.
- The date of disclosure.
- The reason for allowing disclosure.
- The extent of the information disclosed.
- The name and signature of the managed or designated member of staff allowing the disclosure.

The approved list of Backwell School staff who have access to CCTV footage is included at Appendix 3. All other staff must complete a viewing data request form which will need to be authorised by the Head of Site Operations - CCTV Subject Access Request Form - Appendix 2.

In accordance with section 7 of the Data Protection Act 1998 (subject access), any individual who believes that their image has been captured by this scheme is entitled to make a written request to the Data Controller, in this case the Headteacher. Upon payment of the current fee and the supply of essential information, a systems search will be conducted and subject to certain conditions, the individual will be allowed access to the personal data held.

All subject access requests should be referred in the first instance to the School Business Leader

All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and know how such requests are to be dealt with. Data subjects should be provided with a standard subject access request form (Appendix 2).

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

Prior to any authorised disclosure, the School data Protection Officer (PC) will need to determine whether the images of another 'Third Party' individual features in the personal data being applied for and whether these third party images are held under a duty of confidence.

If the School data Protection Officer (PC) decides that a subject access request, from an individual, is not to be complied with, the following should be documented.

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

3 Data shall be adequate, relevant and not excessive

Cameras are sited so that they do not record more information than is necessary for the purpose for which they were installed.

4 Data shall be accurate and kept up to date.

Any personal information which is recorded and stored must be accurate.

A documented procedure is kept which ensures that the accuracy of the system features are checked and if necessary amended or altered.

5 Data shall be kept secure and not be kept longer than is necessary

Images are retained on a hard disc for a period of 10 days. Copies can be made for investigation purposes but requests for disc copies must be made via a Subject Access Form CD Copy Request and must be returned, for destruction within 14 days. (Appendix 1)

All CCTV saved footage will only be kept for a maximum of 7 days. Once the retention period has expired, the images will be erased by the Head of Site Operations. Only members of the School

Leadership Team can authorise the storing of images beyond the 7 day period. Images will be stored until all legal avenues have been exhausted.

The Head of Site Operations is responsible for carrying out the following procedures on a weekly basis.

- Checking and recording that the equipment performs properly.
- Ensuring any special features are accurate (e.g. time display).
- Reporting immediately if equipment is faulty or damaged.

6 Data shall be processed in accordance with the rights of individuals under the Act

Individuals have the right to be provided with a copy of the information held about them. They have the right to prevent processing which is likely to cause damage or distress. They have rights in relation to decision taking.

7 Appropriate measures shall be taken to prevent unauthorised or unlawful processing of data against accidental loss, destruction or damage

It is required that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of data and against accidental loss, damage or destruction. In order to achieve this there is a need to assess any harm that might result from the processing, damage, loss or destruction of this data.

The nature of the data to be processed should be considered and where it contains details of inappropriate/unnecessary material it must be processed with greater care.

7.1 Access to the images

- The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.
- Requests for Data Subject Access should be made to the Headteacher in writing using the form at Appendix 2. There should be sufficient information (date, time, location) in this request to allow for the images to be found.
- The location that will be used for viewing of any images will be the Head of Site Operation's office.
- The images that are filmed will be held in a secure location.
- Images can only be accessed by staff who have been authorised to do so by the Headteacher (as recorded in Appendix 3) and who have signed the CCTV Protocol.
- Images will only be released to third parties if authorised by the Head of Site Operations
- If images are viewed by third parties in school the date and time of this must be recorded and they must be accompanied by an authorised member of staff at all times.
- Should any images be shared with third parties, the school will record the following information:
 - The date on which the images were removed from the general system.
 - The reason why they were removed.
 - The location of the image.
- In addition, if the image is being shared with the police the following information will also be collected;

- Any crime incident number to which the images are relevant.
- The signature of the collecting officer; see below.
- An appropriate administration fee will be charged.
- The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

7.2 Use of images

- The images may be used as evidence within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.
- Images will not be released for commercial purposes and will never be released to the media for purposes of entertainment.
- Images may be released to the media for use in the investigation of a specific crime but this will only be with the written authority of the police.

8 Personal data will not be transferred to a country outside the European Economic Area.

This principle places limitations on the ability to transfer personal data to countries and territories outside of the EEA.

Data will not be made available to the public via internet or website.

Monitoring Compliance with this Code of Practice

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

- A copy of this code of practice.
- Subject access requests form (Appendix 2) if required or requested.

The Head of Site Operations should undertake regular reviews of the documented procedures to ensure that the provisions of the Code are being complied with.

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

Details of any complaints will be recorded and will be included in CCTV system annual report to the Board of Governors by the School Business Leader.



**CCTV Subject Access Request Form
CD Copy Request**

Requested by
Name:
Department:
Position:
Contact Telephone No:

Reason For Request	
Location:	
Date:	Time:

THIS REQUEST WAS **ACCEPTED/DECLINED FOR THE FOLLOWING REASONS **Delete as appropriate

Authorised by			
Signature:	Print:	Date :	
Release of the CD	Date:	Time:	CD Name:
Copied by:			

AFTER THE REMOVAL OF THIS CD I ACCEPT RESPONSIBILITY FOR THE DOCUMENTATION OF ANY FURTHER ACCESS TO THE DATA

Signature:	Print:	Date:
------------	--------	-------

RETURN OF THE CD TO THE SYSTEM

Disc must be returned within 14 days

Signature:	Print:	Date:
Authorised member of staff receiving CD		
Signature:	Print:	Date:

THIS SHEET MUST BE KEPT BY THE HEAD OF SITE OPERATIONS AND A COPY GIVEN TO THE PERSON MAKING THE REQUEST



CCTV Subject Access Request Form

Requested by	
Name:	
Department:	
Position:	
Contact Telephone No:	

Reason for the Request	
Location:	
Date:	Time:

THIS REQUEST WAS **ACCEPTED/DECLINED FOR THE FOLLOWING REASONS	
**Delete as appropriate	

Authorised by		
Signature:	Print:	Date:

THIS SHEET MUST BE KEPT BY THE HEAD OF SITE OPERATIONS AND A COPY GIVEN TO THE PERSON MAKING THE REQUEST

Appendix 3

Staff Access Rights

Level	Name	Title	Access
1	Mark Middleton	Head of Site Operations	Full Access and operational use
2	PCs and PSCOs	Constabulary	Downloading of CCTV footage
3	All SLT	Unspecified	Viewing access only
3	Site Manager	Site Manager	Viewing access only
4	IT Department	Unspecified	Viewing access of IT Sites Only
5	Reception Staff	Unspecified	Viewing access only of Front Gate
6	Pastoral Leads	Unspecified	Viewing access only when requested for identification purposes

ALL other staff will need to complete a Subject Access Request Form authorised by the Head of Site Operations.