



CCTV Policy

Version 3

Status	Non-Statutory
Responsible committee/Individual	Trust Board/Local Governing Body
Author	CEO
Target Audience	All stakeholders
Date Policy Agreed	December 2020 (Version 1) December 2021 (Version 2) December 2022 (Version 3)
Review Date	December 2023

Contents:

Introduction	3
Scope	3
CCTV	3
Review of CCTV	5
Complaints	5
Records of Processing	6
Related Documents	6
Appendices:	
Appendix 1: Surveillance System Checklist	7
Appendix 2: Privacy Notice – CCTV	9

Introduction

This policy is concerned with the use and governance of CCTV technology, and the processing of Personal Data which has been collected by using CCTV technology. The policy is written in accordance with various Data Protection legislation, which includes but is not limited to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), and the Information Commissioner's Office's (ICO) surveillance code of practice.

Queries about this policy should be directed to Brighter Futures Learning Partnership Trust's Data Protection Officer.

Scope

This policy applies to all Trust employees (both those employed directly by the Trust and those employed on behalf of the Trust by a local authority (or other such body), any authorised agents working on behalf of the Trust, including temporary or agency staff, governors, volunteers, and third party contractors.

This Policy will refer to all individuals within scope of the policy as 'employees'. Employees who are found to knowingly or recklessly infringe this policy may face disciplinary action.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The Trust only uses surveillance in the context of CCTV.

The Trust does not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV

The Trust operates 'Closed Circuit Television' (CCTV) systems:

- for the prevention, reduction, detection and investigation of crime and other incidents;
- to ensure the safety of staff, students and visitors;
- to assist in the investigation of suspected breaches of Trust regulations by staff or students; and
- the monitoring and enforcement of traffic related matters (where applicable).

Planning CCTV Systems

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The Trust has various statutory responsibilities to protect the privacy rights of data subjects. Therefore during this planning phase the Trust will consider:

- i. The purpose of the system and any risks to the privacy of data subjects,
- ii. That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).
- iii. The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example the system must record with sufficient resolution to perform its task.
- iv. The system must also have a set retention period (the typical retention period is one month) and, where appropriate, the Trust must also have the ability to delete this information prior than the set retention period in order to comply with the rights of data subjects.
- v. That the Trust will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

The Trust will ensure that a contract will be agreed between the school (as Data Controller) and the CCTV system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the Trust.

CCTV Privacy Notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore the use of CCTV systems must be visibly signed.

The signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed Privacy Notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data.

Access to CCTV Recordings

CCTV footage will only be accessed to comply with the specified purpose. For example if the purpose of maintaining a CCTV system is to prevent and detect crime then the footage must only be examined where there is evidence to suggest criminal activity having taken place.

The CCTV system will have a nominated Information Asset Owner who will be responsible for the governance and security of the system. The Information Asset Owner will authorise officers to access CCTV footage either routinely or on an ad-hoc basis.

CCTV Footage Disclosures

A request by individuals for CCTV recordings that include footage of them should be regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the School's Information Policy.

If the school receives a request from another agency (for example a law enforcement agency) for CCTV recordings, then it will confirm the following details with that agency:

- i. the purpose of the request,
- ii. that agency's lawful basis for processing the footage,
- iii. confirmation that not receiving the information will prejudice their investigation,
- iv. whether the School can inform the data subject of the disclosure, and if not, the reasons for not doing so.

The School will liaise with its appointed Data Protection Officer should it have any concerns about such requests.

REVIEW OF CCTV

CCTV systems must be reviewed biennially to ensure that systems still comply with Data Protection legislation and national standards. The Information Asset Owner should use the checklist included in Appendix 1 of this policy to complete this review. It is the responsibility of the Information Asser Owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

Complaints

Complaints by individuals about the use of CCTV systems, or the way CCTV data is processed, should be treated as a data protection concern and the school's data protection officer should be made aware.

The School's Data Protection Officer is:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veritau.co.uk



Records of Processing

The school has a duty under Article 30 of the GDPR to ensure that all instances of data processing activity is recorded for regulatory inspection where required. The school maintains an information asset register in order to fulfil this requirement.

The school will ensure that the use of surveillance systems is recorded on their information asset register. This should detail each separate surveillance system in use.

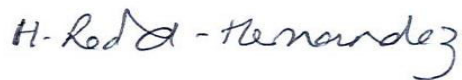
Related Documents

Employees who are responsible for planning, maintaining, or reviewing the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- [ICO Surveillance Code of Practice \(External Link\)](#)
- The School's Data Protection Impact Assessment (DPIA) Template (available through Veritau)

Policy Agreed: December 2022

Signed CEO of BFLPT – Helen-Redford-Hernandez:



Date: December 2022

Signed – Chair of BFLPT – Marcus Isman-Egal:



Date: December 2022

Policy to be reviewed: December 2023

Created: December 2020 (Version 1)
 December 2021 (Version 2)
 December 2022 (Version 3)

Appendix 1 – Surveillance System Checklist

Establishment Name:

Name and Description of Surveillance System:		
The purpose and requirements of the system are addressed by the system (i.e the cameras record the required information)	YES	NO
	Notes:	
The system is still fit for purpose and produces clear images of adequate resolution.	YES	NO
	Notes:	
Cameras are sited in effective positions to fulfil their task.	YES	NO
	Notes:	
Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties.	YES	NO
	Notes:	
There are visible signs showing that CCTV is in operation. These signs include: <ul style="list-style-type: none"> ▪ Who operates the CCTV, ▪ Their contact details, ▪ What the purpose of the CCTV is. 	YES	NO
	Notes:	
CCTV recordings are securely stored and access limited.	YES	NO
	Notes:	

The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information.	YES	NO
	Notes:	
The system has a set retention period. This retention period should only be long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period information should be deleted	YES	NO
	Notes:	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure.	YES	NO
	Notes:	
All operators have been authorised by the Information Asset Owner and have sat their mandatory data protection training.	YES	NO
	Notes:	
This system has been declared on the corporate register of surveillance systems.	YES	NO
	Notes:	

<p>Checklist Completed By:</p> <p>Name: Job Title: Date:</p>	<p>Checklist Reviewed and Signed By (Information Asset Owner):</p> <p>Name: Job Title: Date:</p>
---	---



Appendix 2 - Privacy Notice - CCTV

This privacy notice has been written to inform members of the public, parents, pupils and staff of Brighter Futures Learning Partnership Trust about how and why we process their personal data in relation to CCTV.

Who are we?

Brighter Futures Learning Partnership Trust is a 'Data Controller' as defined by Article 4 (7) of GDPR. This means that we determine the purposes for which, and the manner in which, your personal data is processed. We have a responsibility to you and your personal data and will only collect and use this in ways which are compliant with data protection legislation.

The school has appointed Veritau Ltd to be its Data Protection Officer (DPO). The role of the DPO is to ensure that the school is compliant with GDPR and to oversee data protection procedures. Veritau's contact details are:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
Telephone: 01609 53 2526



What information do we collect and why do we collect it?

By using CCTV systems the school collects, stores, and uses static or moving images of individuals located in the surveillance area.

The school may be able to identify those individuals by using other existing information.

The school operates CCTV for the following purposes:

- for safeguarding children,
- for the prevention and detection of crime.

Our lawful basis for processing your personal data is Article 6(1)(e) and 6(1)(f) respectively:

- 6(1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller – Safeguarding children.
- 6(1)(f) - Processing is necessary for the purposes of legitimate interests - prevention and detection of crime.

Who has access to your personal data?

Your information will only be made available to school employees where there is a need to investigate the recording. Only employees authorised by school management may have access to this footage.

Who do we share your personal data with?

We will only share CCTV footage with other agencies where there is a lawful reason to do so - for example to share with the police for the purposes of crime prevention or to assist in locating an absconding pupil.

How long do we keep your personal data for?

The school will retain this data for no longer than 60 days.

Do you transfer my data outside of the UK?

Generally the information that the school holds is all held within the UK. However, some information may be held on computer servers which are held outside of the UK. We will take all reasonable steps to ensure your data is not processed in a country that is not seen as 'safe' by the UK government.

What rights do you have over your data?

Under GDPR, individuals have the following rights in relation to the processing of their personal data:

- to be informed about how we process your personal data. This notice fulfils this obligation,
- to request access to your personal data that we hold, and be provided with a copy of it,
- to request that your personal data is erased where there is no compelling reason for its continued processing.

If you have any concerns about the way we have handled your personal data or would like any further information, then please contact our DPO on the address provided above.

If we cannot resolve your concerns you may also complain to the Information Commissioner's Office (the Data Protection Regulator) about the way in which the school has handled your personal data. You can do so by contacting:

First Contact Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow Cheshire
SK9 5AF
casework@ico.org.uk // 0303 123 1113

