St Brides Major CW Primary School

Love Learning for Life
Caru Dysgu am Oes

CCTV Policy

Introduction

The St Brides Major CW Primary School uses closed circuit television (CCTV) and the images produced to:

- prevent or detect crime
- monitor the school buildings and grounds
- provide a safe and secure environment for pupils, staff and visitors
- prevent loss or damage to school property.

The school is committed to ensuring that CCTV is used appropriately in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy outlines the school's use of CCTV and how it complies with current regulation.

Purpose

The purpose of this policy is to regulate the management, operation and use of CCTV systems within the school and ensure it complies with the Information Commissioners Office (ICO) CCTV Code of practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use.

The Code of Practice is published at:

https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

This policy has due regard to legislation and statutory guidance, including:

- The Protection of Freedoms Act 2012
- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- ICO CCTV Code of Practice

Roles and responsibilities

Governing Body

The Governing Body has overall responsibility for ensuring that the school complies with the guidance in this policy.

Lead Person

The lead person in St Brides is the Head Teacher.

The Lead Person is responsible for ensuring that the guidance from this policy is followed by all staff and pupils.

The Lead Person is to liaise with the Data Protection Officer (DPO) to decide where CCTV is needed and justify its use.

The Lead Person will confer with the DPO about how to ensure the lawful processing of the surveillance and CCTV footage.

Identified Staff

Staff who have been identified by the Lead Person will be responsible for:

- Managing surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Ensuring surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure.
- Accurately recording any request to view or download any footage.
- Accurately recording any footage that has been downloaded and disclosed to a third party such as the police.
- Receiving relevant training from the DPO to understand their responsibilities under the ICO CCTV Code of Practice.
- Identifying a Subject Access Request for any CCTV footage.
- Ensuring any such request is brought to the attention of the Lead Person and DPO before a disclosure is made.

Data Protection Officer (DPO)

The role and responsibilities of the DPO include:

- Dealing with subject access requests (SAR) in line with legislation, for any disclosure of CCTV footage held by the school.
- Ensuring that all identified staff at each school within the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Train all identified staff in the school to understand their responsibilities as set out in the ICO CCTV Codes of Practice and to be able to identify any Subject Access Request.

Siting of Cameras

- Cameras will be sited so they only capture images relevant to the purposes for which they are installed (as described in the introduction above) and care will be taken to ensure that reasonable privacy expectations are not violated. Each school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the GDPR.
- The school will make every effort to position cameras so that their coverage is restricted to the school premises and minimise the recording of passer-by or of another person's private property.
- The cameras will be sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- CCTV will not be used in classrooms.
- CCTV cameras will not be placed in toilets.

Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) will be completed whenever the development or review of a CCTV system is being considered. This is to ensure that the purpose of the system is and remains justifiable.

A DPIA will be reviewed prior to the installation of any additional surveillance and CCTV system equipment. If the DPIA reveals any potential security risks or other data protection issues, the Lead Person will discuss these risks with the DPO and ensure any appropriate safeguards can be put in place.

The DPIA should be carried out by the Lead Person that has responsibility for the CCTV system and the DPO.

If after completing the DPIA the use of a surveillance and CCTV system is deemed too intrusive to privacy, the school will make the appropriate changes or need to seek alternative provision.

Management and Access

Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

A log of any access to view the CCTV recordings will be maintained by each school and must include the time and date of access, the name of the authorised person accessing the recordings and the reason for accessing the information. Please see Appendix A as an example of a template.

There will be no disclosure of recorded footage to third parties other than to authorised personnel such as the police and service providers to the school where these would reasonably need access to the footage (e.g. HR Department, school solicitors for internal investigations, insurance companies in relation to a claim)

In relevant circumstances, CCTV footage may be accessed:

- By law enforcement where the school are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by law enforcement when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the school's property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to the school, or
- To individuals (or their legal representatives) subject to a court order.
- To the school's insurance company where the insurance company requires information in order to pursue a claim for damage done to the insured property.

If a request is received from a law enforcement agency or other service provider for disclosure of CCTV images, the Lead Person or Identified Staff member must obtain an official written request outlining reasons for the request and liaise with the DPO as to whether the disclosure of CCTV is permissible.

No other individual will have the right to view or have access to any CCTV images, unless authorised by the Lead Person.

The CCTV System will be checked every week by the identified staff, to ensure that the system is operating effectively.

Any cameras that present faults will be repaired as soon as possible to avoid any risk of loss of security functionality and potential data breach.

The location of the CCTV recording systems should be located in a secure room and only accessed by the Lead Person and their Identified staff

Storage and Retention

Recorded images will be kept for no longer than 30 days, unless there is a specific purpose for which they need to be retained for a longer period (the specified purpose must be recorded and kept under review so no recording is kept longer than necessary). Images will be deleted from the CCTV server.

While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

All retained data will be stored securely at all times then permanently deleted when no longer required.

Subject Access Request (SAR)

Any individual recorded in any CCTV image is a data subject for the purpose of data protection legislation and has a right to request access to those images, unless an exemption applies under the General Data Protection Regulations.

Any individual who requests access to images of themselves will be considered to have made a Subject Access Request.

When a request is made, the DPO must be informed. The DPO will then assist the Lead Person to ensure the school's SAR Guidance is followed. This needs to take place before reviewing the CCTV footage.

If the CCTV footage contains only the individual making the Subject Access Request, then the individual may be permitted to view the footage. This must be strictly limited to the footage which contains images of the individual making the request.

If the CCTV footage contains images of other individuals, then the Lead Person and DPO must consider whether:

- The request requires the disclosure of images of individuals other than the requester, for example, whether the images can be distorted so as not to identify other individuals.
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained

A record must be kept and held securely of all disclosures, which sets out:

- When the request was received
- The process followed by the Lead Person/DPO in determining whether the images contained third parties
- The considerations as to whether to allow access to those images

- The individuals that were permitted to the view the images, recording the date and time
- Whether a copy of the images was provided, if so to whom and the format of the information
- DPO to also record on the SAR's central register

See Appendix A for a template record of requests

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee can be charged, or an exemption may be applied. The DPO must be consulted prior to charging a fee or application for an exemption.

All requests will be responded to within 30 school days of receiving the request. However, the ability of the school to service such requests may be reduced or impossible due to staff absence and school closure over the school holidays. Teaching school staff with permission to access pupil information are not required to work within school holidays. Administrative school staff may also not be contracted to work outside of term time, rendering the request impossible to fulfil in the absence of staff and school closure.
Should a school holiday closedown period severely affect the school's ability to facilitate the production of the required information, the requestor will be notified and school may extend the period of compliance by a further two months.

Where possible requests should be made in writing to the lead person at the school. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. This should include the date, time and location.

The Trust school the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

Misuse of CCTV System

The misuse of a CCTV system could constitute a criminal offence. Any member of staff who breaches this policy may be subject to disciplinary action.

Monitoring and Review	
Author	Finance & Premises
Created on	February 2023
Last updated on	February 2023
Scheduled review date	February 2028
Signed HT	
Signed Chair	