

CLOSED CIRCUIT TELEVISION (CCTV) POLICY

Introduction

St Germans Primary School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for children, staff and visitors, and to prevent the loss or damage to school property.

The system comprises of a number of dome cameras and does not have sound recording capability.

The CCTV system is owned and operated by the school and the deployment of which is determined by The Bridges Federation's Senior Management Team (SMT).

The CCTV is monitored centrally from Server room by The Headteacher (School Data Controller) or Head of School. The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the Schools' communities.

The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images are covered by the Data Protection Act 1998. This policy outlines the school's use of CCTV and how it complies with the Act.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

This policy sets out the purposes of the system and the procedures to be followed when managing the system.

This system will be reviewed annually.

Statement of Intent

The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at: http://www.ico.gov.uk/~media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

CCTV warning signs will be clearly and prominently placed at all external entrances to the school, including school gate. Signs will contain details of the purpose for using CCTV (see appendix B).

The planning and design has endeavoured to ensure that the Scheme 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.

Siting the Cameras

Cameras are sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Covert Monitoring

The school may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from a member of the SMT.

Covert monitoring must cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

Storage and Retention of CCTV images

Recorded data will not be retained for longer than is necessary. 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.

Access to CCTV images

The system operates from the secure Server Room. Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Subject Access Requests (SAR)

Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

The Federation school will respond to requests within 40 calendar days of receiving the written request and fee.

A fee of £10 will be charged per request.

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

Access to and Disclosure of Images to Third Parties

There will be no disclosure of recorded data 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 data (e.g. investigators).

Requests should be made in writing to the Headteacher.

The data may be used within the Schools' Discipline and Grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Complaints

Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

Control

This CCTV system and the images produced by it are controlled by the Headteacher who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).

The Bridges Federation has considered the need for using CCTV at St Germans Primary School and has decided it is required for the prevention and detection of crime and for protecting the safety of children, staff and property. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

Further Information

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- www.ico.gov.uk

- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 1998

Appendix A – CCTV Signage

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for enquiries



Appendix B – Data Protection Act

The Data Protection Act 1998: Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
 - at least one of the conditions in Schedule 2 is met, and
 - in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles, for further information refer to the Data Protection Act