St. Peter's Catholic School

MANAGEMENT PRACTICE AND PROCEDURES
IN RESPECT OF CCTV SURVEILLANCE SYSTEM

1 Introduction

This document sets out the Management Practice and Procedures that will be adopted with respect to any CCTV system operated by St. Peter's Catholic School in order to comply with the Data Protection Act 1998.

For the purpose of this policy, any recordings, either images or audio made by the 'CCTV System' will be referred to as 'content'.

2 System Operator

2.1 For the purpose of the Data Protection Act 1998 the Data Controller for the CCTV system operating within the St. Peter's Catholic School premises at Whitefields Road, Solihull is the Headteacher.

2.2 For the purpose of this policy, the designated CCTV operators are staff who hold the following positions within the School;

- Business Manager
- ICT Manager
- Site Manager
- Assistant ICT Manager
- ICT Technician
- Site Operatives
- Persons temporarily designated the role of 'CCTV Operator' by any person listed above.

3 Purpose of the System

3.1 The system will be used for:

(a) The prevention and detection of crime.

(b) The safety and security of staff or members of the public working or visiting the premises.

(c) The monitoring of conduct in accordance with the School's Disciplinary Policy.

4 The System

4.1 The CCTV system will comprise a multi camera system having the capability to record images and audio together with date, time and camera location information.

4.2 Cameras are located externally to facilitate access control to the building and monitoring of areas in the immediate proximity to the building. The School will make every effort to ensure that the siting and operation of any external cameras will not invade the privacy of any domestic premises, however, if they do then appropriate steps will be taken to safeguard the privacy of those affected, for example, privacy masking on recordings / live feeds.

4.3 Cameras are also located inside of the School buildings where there is a genuine operational need, which conforms with the purpose of the system, as defined in chapter 3. The siting and operation of any internal cameras will be such that they will not invade the privacy of any sensitive areas, for example: changing rooms, toilets, medical rooms etc. If they do then appropriate steps will be taken to safeguard the privacy of those affected, for example, privacy masking on recordings / live feeds. Cameras may be located within the classroom environment and / or staff workspaces, in addition to general passageways and communal areas.

4.4 Express permission for the installation of cameras that will invade privacy in sensitive areas will be obtained from the Headteacher in writing before any camera is installed.

4.5 The system has been designed to allow content to be recorded and viewed in real time. Any content that is viewed in real time will be at locations identified as suitable by a CCTV operator, and the purpose for doing so will conform with the purpose of the system, as defined in chapter 3.

4.6 A defined CCTV monitoring station is located in the ICT Support room. The purpose of the monitoring station is:

- A preventative measure to deter poor conduct and any criminal activities from taking place.
- An effort to increase transparency of the system so that Pupils, Staff and Visitors are aware of the camera locations.

5 Signing

5.1 High visibility signs will be placed so that any person whose may be recorded by the system is made aware of the operation of a CCTV system and the reason for its use, as far as practicable.

5.2 Signs will be clearly visible, of an appropriate size and contain the following information:

- The identity of organisation operating the system.
- The purpose of the system.
- Contact details of the organisation operating the system.

5.3 An example of a sign that complies with the above can be found in Appendix 1.

6 Retention of CCTV Content

6.1 Content recorded by the system will be retained for a maximum period of 45 calendar days following the date of the recording.

6.2 The retention period (6.1) may be extended indefinitely, but no longer than necessary, where content is required for the purposes of crime investigation or internal evidential purposes.

6.3 Media that holds content during the retention period will stored securely.

6.4 Access to recorded content held during the retention period will be restricted to the Head Teacher and the designated CCTV operators.

6.5 On expiry of the retention period (6.1) all recordings will be erased prior to the media being reused.

6.6 At periods to be set by the ICT Manager, and in line with the supplier's recommendations, test viewing of the content should take place to ensure that the quality of the recorded content is acceptable. Any media found to provide unacceptable content must be replaced.

6.7 Any media on which content has been recorded that is no longer required must have all content erased and the media destroyed safely and securely. Details of the destruction will be documented eg media reference number; date of destruction; destruction method; signature.

6.8 The School Business Manager has the responsibility for the maintenance of the CCTV System. The ICT Manager has the responsibility for the day to day running of the CCTV system and content management.

7 Access to Content by Staff

It is important that access to content recorded by the CCTV system is restricted and carefully controlled, not only to maintain the rights of the individual, but also to ensure that the integrity of any evidence is preserved should any recorded content be required for evidential purposes.

7.1 Access to content by members of staff will only be allowed if such access is compatible with the reason/purpose for which the content was originally obtained for.

7.2 Only the Head Teacher and the designated CCTV operators are permitted to make a copy of, or remove, any media containing content.

7.3 Any member of staff who violates these practices and procedures, whether intentional or inadvertent, may be liable to disciplinary action.

8 Access to and disclosure of content to a Third Party (e.g. Police or legal representatives)

It is important that access to and disclosure of content recorded by the CCTV system is restricted and carefully controlled, not only to maintain the rights of the individual, but also to ensure that the 'chain' of evidence is preserved should such content be required for evidential purposes.

It is also essential that disclosure of content to a third party is compatible with the reason/purpose for which the content was originally obtained.

8.1 Disclosure of content to a third party will only be made in line with the purpose of the system, for example:

- Police, other prosecution agencies and other relevant legal representatives where the content may assist with the prevention or detection of a crime or the prosecution of an offender.

8.2 All requests made by a third party for access to content will be documented eg date/time; full details of person making the request; purpose of the request.

If access is denied, details should be documented.

If access is allowed, details of the media accessed (reference number) and the extent of the access should be documented.

8.3 If a third party requires to remove any media containing content the signature of the person must be obtained and the details of the person handing over the media must also be documented.

8.4 Viewing of any media on which content has been recorded should take place in a private area and at least one member of staff who is not captured in the recording itself will remain in the viewing area whilst the third party viewing is taking place to ensure that no unauthorised copies of the content are made, for example via smartphones.

9 Access to content by a Pupil, Parent or Visitor

Content from which an individual may be identified falls within the remit of personal data as defined by the Data Protection Act 1998. As with any form of personal data the individual (Data Subject) whose has been recorded is entitled under Section 7 of the Data Protection Act 1998 to make a request for access to and be given a copy of the content held (Data Subject Access Request).

The same rules apply to content as apply to personal data held on paper or computer files, namely that an individual is only entitled to access content, which features only them.

Recorded content is subject to the same third party rules as per paper/computer files.

9.1 All Data Subject Requests must be made in a permanent form eg pro-forma, letter or e-mail. As well as giving their details (name and address) the person making the request must provide sufficient information to enable the Data Controller to locate the content being requested eg date/times, location and possibly a recent photograph to aid identification.

9.2 The person making a request should be given access to, or a copy of, their image(s) within 40 days of receipt of a valid request. They should also be given information explaining:

- Their rights under the Data Protection Act 1998.

- A description of the type(s) of content recorded, the reason for recording of the content, the retention policy and the disclosure policy in relation to those images.

9.3 If the Data Subject requests to view the recorded content arrangements to view the content should take place in a private area and at least one member of staff who is not captured in the recording itself will remain in the viewing area whilst viewing is taking place to ensure that no unauthorised copies of the content are made, for example via smartphones.

9.4 The Data Protection Act 1998 provides for the Data Controller to make a maximum charge (currently £10) for an access to records request. Solihull MBC does not make a charge.

9.5 The Data Protection Act 1998 provides for withholding access to recorded content under specific conditions. Any decision to withhold/deny access must be approved by the Head Teacher (it is recommended this is following consultation with Solihull MBC's Corporate Information Security Manager). All decisions to withhold/deny access must be fully documented.

10 Training

10.1 All members of the school's staff will be made aware of the system, its purpose and the Management Practice and Procedures, through high visibility signage and this policy.

10.2 Staff who may be called upon as part of their duties to operate the system will be given appropriate training to enable them to use the system. Staff who may be called upon to operate the system should also receive training to ensure that they are aware of their responsibilities with respect to:

- The School's security policy.
- The School's disclosure policy.
- The rights of the individual in relation to their recorded images.

11 Covert Monitoring

11.1 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, is taking place

- Where there are grounds to suspect serious misconduct; where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

11.2 In these circumstances authorisation must be obtained in writing from the Headteacher.

11.3 Covert monitoring must cease following completion of an investigation.

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

Appendix 1:

CCTV IN OPERATION

Video and audio are being monitored for the prevention and detection of crime, for the safety of pupils, staff and members of the public and for the monitoring of conduct in accordance with the School's Disciplinary Policy.

The system is operated by St. Peter's Catholic School.

For further details, contact 0121 705 3988.

Appendix 2:

St. Peter's Catholic School

ACCESS TO OR DISCLOSURE OF RECORDED CONTENT TO A THIRD PARTY

Date/time of Request:

……

DETAILS OF PERSON MAKING REQUEST

Full Name:	
Designation:	
Organisation:	
Address:	
Tel No:	

REASON FOR REQUEST

Request: **Denied** **Allowed**

Decided by:

Reason(s):

VIEWING

Date/Time:	
Details of media viewed:	
Viewed in the presence of:	

Removal of Media containing Recorded Content

I the above named person certify that I have taken possession of media reference number ……. for the purpose stated above. I certify that it will only be used for this purpose and that it will be returned to St. Peter's Catholic School when no longer required.

Signed: …… Date: ……