CCTV POLICY

Mount St Joseph Document Control Table			
Document Title :	**CCTV Policy**	**Author name / post:**	**Browne Jacobson**
Version Number:	**1.0**	**Document Status:**	**Approved**
Date Approved:	**May 2018**	**Approved By :**	**SLT Governors**
Effective Date :	**25 May 2018**	**Date of next review:**	**May 2020**
Publication method:	**Staff reference drive**	**Date published**	**May 2018**
Superseded Version:	**New Policy**		

Document History		
Version	**Date**	**Notes on Revisions**
1.0	25 May 2018	Recommended Policy in line with GDPR introduction

1 Policy Statement

1.1 Mount St Joseph uses Close Circuit Television ("CCTV") within the premises of the School. The purpose of this policy is to set out the position of the School as to the management, operation and use of the CCTV at the School.

1.2 This policy applies to all members of our Workforce, visitors to the School premises and all other persons whose images may be captured by the CCTV system.

1.3 This policy takes account of all applicable legislation and guidance, including:

1.3.1 General Data Protection Regulation ("GDPR")

1.3.2 Data Protection Act 2018 (together the Data Protection Legislation)

1.3.3 CCTV Code of Practice produced by the Information Commissioner

1.3.4 Human Rights Act 1998

1.4 This policy sets out the position of the School in relation to its use of CCTV.

2 Purpose of CCTV

2.1 The School uses CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for pupils, staff and visitors

2.1.2 To prevent the loss of or damage to the School buildings and/or assets

2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

3 Description of system

3.1 The CCTV system is owned by the school and comprises 71 fixed and 1 moveable dome cameras that are located around the school site, 56 internally and 16 externally. All cameras record in high definition (1080p) and do have audio recording capabilities but this has been disabled on all cameras.

4 Siting of Cameras

4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The School will make all reasonable efforts to ensure that areas outside of the School premises are not recorded.

4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

4.4 Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilets.

5 Privacy Impact Assessment

5.1 Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the School to ensure that the proposed installation is compliant with legislation and ICO guidance.

5.2 The School will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and Access

6.1 The CCTV system will be managed by the ICT Manager.

6.2 On a day to day basis the CCTV system will be operated by the ICT Technician.

6.3 The viewing of live CCTV images will be restricted to the ICT Manager, ICT Technician and Senior Leadership Team.

6.4 Recorded images which are stored by the CCTV system will be restricted to access by ICT Manager and ICT Technician.

6.5 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

6.6 The CCTV system is checked weekly by the ICT Manager and ICT Technician to ensure that it is operating effectively.

7 Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

7.2 Recorded images are stored only for a period of 28 days unless there is a specific purpose for which they are retained for a longer period.

7.3 The School will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

7.3.1 CCTV recording systems being located in restricted access areas;

7.3.2 The CCTV system being encrypted/password protected;

7.3.3 Restriction of the ability to make copies to specified members of staff

7.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the School.

8 Disclosure of Images to Data Subjects

8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.

8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the School's Subject Access Request Policy.

8.3 When such a request is made the ICT Manager will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

8.4 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The ICT Manager must take appropriate measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals then the School must consider whether:

8.5.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

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

8.6.1 When the request was made;

8.6.2 The process followed by ICT Manager in determining whether the images contained third parties;

8.6.3 The considerations as to whether to allow access to those images;

8.6.4 The individuals that were permitted to view the images and when; and

8.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

Please note that when a subject access request is made then, unless an exemption applies (such as in relation to third party data that it would be unreasonable to disclose)

then the requester is entitled to a copy in a permanent form. We have referred only to "access" as opposed to a "permanent copy" as the School may consider it preferable in certain circumstances to seek to allow access to images by viewing in the first instance without providing copies of images. If an individual agrees to viewing the images only then a permanent copy does not need to be provided. However if a permanent copy is requested then this should be provided unless to do so is not possible or would involve disproportionate effort.

9 Disclosure of Images to Third Parties

9.1 The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

9.3 If a request is received form a law enforcement agency for disclosure of CCTV images then the ICT Manager must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

9.4 The information above must be recorded in relation to any disclosure.

9.5 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10 Review of Policy and CCTV System

10.1 This policy will be reviewed every 2 years.

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed annually.

11 Misuse of CCTV systems

11.1 The misuse of CCTV system could constitute a criminal offence.

11.2 Any member of staff who breaches this policy may be subject to disciplinary action.

12 Complaints relating to this policy

12.1 Any complaints relating to this policy or to the CCTV system operated by the School should be made in accordance with the School Complaints Policy.

CCTV PRIVACY IMPACT ASSESSMENT

1 Who will be captured on CCTV?

Any user or visitor of the school could be captured on the CCTV system including pupils, staff, parents / carers, volunteers, governors and contractors.

2 What personal data will be processed?

Facial Images, behaviour, and all movement will be captured by the CCTV cameras.

3 What are the purposes for operating the CCTV system?

Mount St Joseph uses closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor the school buildings and grounds in order to provide a safe and secure environment for its pupils, staff and visitors, and to prevent loss or damage to school property.

4 What is the lawful basis for operating the CCTV system?

To protect the buildings and its assets. To protect the health and safety of the school members and visitors. To increase personal safety and reduce the fear of crime. To detect, prevent and reduce incidence of property crime, public disorder and offences against people.

5 Who is/are the named person(s) responsible for the operation of the system?

Mr D Cartwright – IT Manager

6 Describe the CCTV system, including:

a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;

b. siting of the cameras and why such locations were chosen;

c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals

Cameras are located at strategic points throughout the premises, principally at the entrance and exit points as well as all corridors around school. There are also external cameras that cover the school grounds. There are signs notifying individuals at strategic points around the school. Cameras are positioned so that they only cover areas of the school buildings and grounds. They do not cover any 'public or private space'. The system does not allow for redacting.

7 Set out the details of any sharing with third parties, including processors

There is no access to the school's CCTV system by external agencies or third parties. If faults develop with the system, appropriate contractor support is sought and the system is repaired appropriately. Rarely requests from the Police to view CCTV will be made.

8 Set out the retention period of any recordings, including why those periods have been chosen

As the recording system records digital images, any CCTV images that are held on the hard drive of the server are deleted and overwritten on a recycling basis and, in any event, are not held for more than 3 months.

9 Set out the security measures in place to ensure that recordings are captured and stored securely

The images are recorded and centrally held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and password protected. Viewing of recorded images takes place in a restricted area to which other employees do not have access when viewing is occurring.

10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

The risks associated with the CCTV system in school is the potential failure to ensure the security of the system. This in turn, leading to images of students, staff and visitors being viewed or distributed unlawfully.

The system is also at the risk of unlawful viewing by the operators.

11 What measures are in place to address the risks identified?

To minimise any risks associated with CCTV recording, the system is restricted to ensure CCTV is only viewed when necessary. The operators are advised to view CCTV only when requested to do so by the Senior Leadership Team. The system has an audit log which records the number of times the system has been viewed and by whom.

The CCTV system is set to record over images every 3 months. Images which have been requested are only stored for 28 days and then erased. These are stored on a secure, password protected drive, assessable only to the Senior Leadership Team.

CCTV is never sent to third parties, however should, for example, the police wish to view the CCTV they are invited in school to do so. Any requests for copies of CCTV are required in writing and are granted only to the Police.

12 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

Parents and pupils where consulted prior to the installation of the CCTV system. No negative feedback was received.

13 When will this privacy impact assessment be reviewed?

The impact assessment is to be reviewed every 2 years in line with the CCTV policy, or when any alterations are made to the current systems.

Approval:

This assessment was approved by the Data Protection Officer:

DPO N Samuel

Date 25 May 2018