MAGDALEN COLLEGE SCHOOL

CCTV POLICY

School Procedure

INTRODUCTION

Closed Circuit Television Systems (CCTVS) are installed in Magdalen College School Brackley. New CCTV systems will be introduced where a need is identified. The system and their operation will be reviewed regularly in consultation with staff and governors.

1. PURPOSE OF POLICY

"The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external areas of the premises under the remit of Magdalen College School.

CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external areas of the premises. The system is set to operate 24 hours 7 days a week. CCTV surveillance at the School is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, pupils and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

2. SCOPE

This policy relates to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material in Magdalen College School Brackley premises.

3. GENERAL PRINCIPLES

Magdalen College School has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and visitors to its premises. Magdalen College School owes a duty of care under the provisions of Data Protection Act 2018 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community by integrating the best practices governing the public and private surveillance of its premises.

The school is registered with the Information Commissioner Office and will seek to comply with the requirements relating to Data Protection.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring normal employee activity or performance. If a CCTV camera has recorded a specific incident under investigation, recordings may be used in both student and staff investigatory and potentially disciplinary proceedings to provide evidence as appropriate.

Information obtained through the CCTV system may only be released when authorised by the Headteacher, following consultation with the Chair of the Governors. Any requests for CCTV recordings/images from Police will be fully recorded and legal advice will be sought if any such request is made. (See "Access" below). If a law enforcement authority, such as Police, is seeking a recording for a specific investigation, Police may require a warrant and accordingly any such request made by Police should be requested in writing and the School will immediately seek legal advice.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the School, including the provisions set down in equality and other educational and related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within School premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the Magdalen College School. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Act 2018.

4. JUSTIFICATION FOR USE OF CCTV

The Data Protection Act 2018 requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. The use of CCTV to control the perimeter of the school buildings for security purposes has been deemed to be justified by the governors. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation. CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, locker areas, the Headteacher has demonstrated that there is a proven risk to security and/or health and safety and that the installation of CCTV is proportionate in addressing such issues.

5. LOCATION OF CAMERAS

Magdalen College School has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas in Magdalen College School may include the following:

- ***Protection of school buildings and property:*** The buildings' perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- ***Verification of Security Alarms:*** Intrusion alarms, exit door controls, external alarms
- ***Video Patrol of Public Areas:*** Parking areas, Main entrance/exit gates, Traffic Control

- ***Criminal Investigations (carried out by Police):*** Robbery, burglary and theft surveillance

6. COVERT SURVEILLANCE

Magdalen College School will not engage in covert surveillance.

Where Police requests to carry out covert surveillance on school premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by Police will be requested in writing and the school will seek legal advice.

7. NOTIFICATION – SIGNAGE

The Headteacher will provide a copy of this CCTV Policy on request to staff, students, parents and visitors to the school. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to Magdalen College School.

WARNING
CCTV (Image & Voice Recording) cameras in operation

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, school gates
- reception area
- at or close to each internal camera

8. STORAGE & RETENTION

The Data Protection Act 2018 states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. The images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (e.g the Police, Senior Staff, Leader of Learning). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

9. ACCESS

The recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to recordings will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only. In relevant circumstances, CCTV footage may be accessed:

- By Police where Magdalen College School is required by law to make a report regarding the commission of a suspected crime; or
- Following a request by Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Magdalen College School property, or
- To the Local Authority or any statutory body charged with child safeguarding; or
- To assist the Headteacher in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; 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 Magdalen College School, or
- To individuals (or their legal representatives) subject to a court order.
- To the School's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Requests by Police: Information obtained through video monitoring will only be released when authorised by the Headteacher following consultation with the Chair of the Governors. If Police request CCTV images for a specific investigation, Police may require a warrant and accordingly any such request made by Police should be made in writing and the School should immediately seek legal advice.

Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the Data Protection Officer.

A person should provide all the necessary information to assist Magdalen College School in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the School.

In giving a person a copy of their data, the School may provide a still/series of still pictures, a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

10. RESPONSIBILITIES

The Headteacher will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Magdalen College School
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Magdalen College School
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at Magdalen College School is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to or the release of images or any material recorded or stored in the system
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events.
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that images are stored in a secure place with access by authorised personnel only
- Ensure that images recorded are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil.)
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- Ensure that where Police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Chair of Governors.

11. IMPLEMENTATION & REVIEW

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take into account changing information or guidelines (e.g. from the ICO, Police, Department for Education, legislation and feedback from parents/guardians, students, staff and others.)

APPENDIX 1 - DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Act – The Data Protection Act 2018 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All School staff must comply with the provisions of the Data Protection Act when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under the Data Protection Act.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Act places responsibilities on such entities in relation to their processing of the data.