



# SECURITY CCTV POLICY

## 1. OVERVIEW

- 1.1 St Augustine College ('the **College**') operates a closed-circuit television ('**CCTV**') surveillance system ('**the CCTV System**') throughout the College premises, including corridors, passageways, staircases, passageways, entrances and foyers, play grounds, open garden, primarily to ensure the safety and security of students, staff and visitors at all times.

## 2. DEFINITIONS

- a) '**Authorised Personnel**' means the persons or categories of persons that the College authorises access to any CCTV material.
- b) '**Data Coordinator**' means any natural or legal person which holds Personal Data, and alone or with others controls the contents and use of personal data.
- c) '**CCTV material**' means any live footage, images and recordings taken by the CCTV
- d) '**CCTV System**' shall mean the security system being operated within the College consisting of cameras and other audio and video recording equipment.
- e) '**Data Subject**' means an individual who is the subject of personal data.
- f) '**Data Protection Laws**' shall mean the relevant Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regards to the processing of Personal Data and on the free movement of such data ('**GDPR**') and the Data Protection Act, Chapter 586 of the Laws of Malta and subsidiary legislation thereto as may be applicable at the time of the Policy and as may be amended from time to time.
- g) '**Law enforcement authority**' shall mean any competent local entity being the Malta Police Force or any governmental department.
- h) '**Personal Data**' means any data relating to an identified or identifiable natural person, meaning one that can be identified directly or indirectly in conjunction with any other information.
- i) '**Rector**' means the person duly responsible for the general affairs and running of the College.

- j) **'Privacy Impact Assessment'** shall mean a documented assessment to analyse what actions and/or new CCTV material can be adopted which are less likely to contravene any of the Data Protection Laws.
- k) **'Technical and organisational security measures'** means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, authorities' disclosure or access and against all other unlawful forms of processing being appropriate to the risks involved.

The terms **'Data'**, **'Data Protection Officer'**, **'Data Subject Access Request'** and **'Processing'** shall have the meaning given to these terms in the GDPR.

### 3. DATA CONTROLLER

- 3.1 The College is the data controller and responsible for any personal data collected, stored or processed under this Policy.
- 3.2 The College has appointed Fr David Cortis osa, as a Data Protection Coordinator hereinafter referred to as **'DPC'** who is responsible for ensuring compliance with Data Protection Laws. The DPC may be contacted via e-mail on [david.cortis@sac.mcs.edu.mt](mailto:david.cortis@sac.mcs.edu.mt).

### 4. PURPOSE OF POLICY

- 4.1 The purpose of this policy is to outline the College's approach to the use of a CCTV system for security purposes across the institution both internally and externally and to comply with the requirements with the relevant Data Protection Laws
- 4.2 CCTV surveillance at the College is intended for the purposes of, but not limited to;
  - a) Creating a safer environment;
  - b) Protecting the College's premises and assets, both during and after College hours;
  - c) Ensuring that College rules are being respected and properly managed;
  - d) Reducing the incidence and fear of crime and anti-social behaviour;
  - e) Preventing and responding effectively to all forms of possible harassment and disorder;

- f) Assisting in identifying, apprehending and prosecuting offenders;
- g) Providing emergency services assistance;
- h) Supporting the Malta Police Force in deterring and detecting crime

4.3 The use of the CCTV will effectively facilitate the implementation of the College's other policies, leading to the resolution of complaints and disciplinary procedures and prosecutions in a more efficient manner.

4.4 The information processed may include images and video recording of personal appearance and behaviour. The information may be about staff, students, visitors, any third party offering a service to the College, members of the public and those inside the premises, entering or in the vicinity of the College. The monitoring of these individuals will be carried out in accordance with Data Protection Laws.

## **5. SCOPE**

5.1 This policy applies to CCTV and other systems which capture images of identifiable individuals and for purposes relating to safety of individuals and security of buildings and property. In furtherance of these purposes, video surveillance may be used to monitor exterior and interior areas of the College's property.

5.2 This policy is binding on all employees of the College and all employees being contractually bound to provide any services to the College. This policy also applies to all persons who may be present for whatever reason, on the College's property.

5.3 The planning and design of the CCTV systems has been accepted to ensure the maximum effectiveness and efficiency, however this does not guarantee to cover or detect every incident occurring within the areas covered. The College's CCTV may capture images and audio recordings.

- 5.4 The CCTV System is intended to satisfy the purposes stated in Clause 3.2 and shall provide, when required, information and images of evidential value for the purposes stated in this Policy. This policy does not cover the use of CCTV and CCTV System for any purposes that are of artistic, administrative, educational or research purposes.

## **6. GENERAL PRINCIPLES**

- 6.1 The College has a statutory responsibility for the protection of its property and equipment as well as providing security to its staff, students and visitors to its premises. The College owes a duty of care under the provisions of Occupational Health and Safety Authority Act, Chapter 424 of the Laws of Malta and associated legislation and utilises CCTV systems as an added mode of security and surveillance.
- 6.2 The use of the CCTV system will be conducted in a professional, ethical and legal manner and only for purposes stated in Clause 3.2. CCTV recordings are monitored and retained in strict accordance with this Policy.
- 6.3 Any information obtained through the CCTV System may only be released when authorised by the Rector of the College. In the event that a law enforcement authority requires any material for a specific investigation, the authority may require a warrant and such request shall be made in writing and the College will immediately seek legal advice.
- 6.4 Video monitoring of public areas for security purposes within the College's premises is limited to uses that do not violate the individual's reasonable expectation to privacy.
- 6.5 The public and College community are made aware of the presence of the CCTV System by appropriate signs and notice of video surveillance which sets out the purposes for processing the CCTV images and recording.
- 6.6 Appropriate procedures shall be created and followed for the use of a CCTV System with regards to recording, viewing and retention of images.

- 6.7 All authorised personnel of the CCTV System shall be appropriately trained.
- 6.8 DG Tech shall be responsible for the operation and management of the College's Security CCTV System at Pietà campus, while MASCO shall be responsible for the operation and management of the College's Security CCTV system at Marsa campus.
- 6.9 Any changes to the purposes for which the CCTV is operated as per Clause 3.2, shall require the prior approval of the Rector of the College.

## **7. OWNERSHIP AND OPERATION**

- 7.1 The CCTV System and all recorded material and copyright are owned by the College and operated by DG Tech and MASCO. The responsible personnel is the Rector of the College.

## **8. RESPONSIBILITIES**

- 8.1 The College shall be responsible for all CCTV operated upon its premises and shall be the Data Controller for the requirements of the GDPR, ensuring full compliance and all obligations are met.
- 8.2 The Rector of the College shall;
- a) Ensure that the CCTV System is implemented in accordance with this Policy;
  - b) Ensure that the implemented system is compliant with this Policy
  - c) Manage and co-ordinate the use and maintenance of the CCTV System for safety and security purposes;
  - d) Be responsible for the CCTV materials and any release thereof;
  - e) Maintain a record of access to or the release of tapes or any material recorded or stored in the system;
  - f) Ensure that the areas covered by the CCTV System, both internally and externally, are compliant with this Policy and any recording is taken with due regard to the individuals' privacy, taking into consideration that no infringement is likely to take place;

- g) Ensure that cameras are non-intrusive in terms of their positions in view of any neighbouring residential houses or other domestic areas;
- h) Give consideration to any complaints lodged by any student or member of staff regarding the possibility of an invasion of privacy or confidentiality due to the location of any CCTV System equipment.
- i) Ensure that when a zoom facility on a camera is being used, a second person is present to guarantee that no invasion of privacy has occurred;
- j) Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas;

## **9. LOCATION OF CAMERAS**

- 9.1 The College selected locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras which are externally placed are positioned in a way as to prevent or minimize recording of passers-by or the private property of another individual. Cameras are strategically located throughout the College's premises, primarily at corridors, passageways, staircases, passageways, entrances and foyers, play grounds, open garden.

## **10. NOTIFICATION AND SIGNAGE**

- 10.1 The Rector will provide a copy of this CCTV Policy on request to any members of the staff, students, parents and any visitors to the College.
- 10.2 Cameras shall not be hidden from view and adequate signage is placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation.

## 11. ACCESS

### 11.1 Access to CCTV material

11.1.1 For operational purposes, any CCTV material captured by the CCTV System will be monitored in a secure room on the premises and only designated and trained staff shall have access to such material. The Data Coordinator shall authorise and permit the viewing of the CCTV material to any other staff as necessary in connection with a serious occurrence.

11.1.2 Any pre-recorded CCTV should not be downloaded or saved in any form, except in so far as it is saved if it forms part of an investigation into a serious occurrence including any staff, student or visitor's misconduct.

### 11.2 Access by Data Subjects

11.2.1 Any CCTV material, showing a recognizable person, is personal data and is covered by Data Protection Laws. Any person who believes has been filmed by the College's CCTV System may make a Subject Access Request to the College via e-mail [david.cortis@sac.mcs.edu.mt](mailto:david.cortis@sac.mcs.edu.mt) requesting a copy of any information held by the College, subject to any restrictions covered by Data Protection Laws

11.2.2 The College recognizes and acknowledges the rights of Data Subjects to their Personal Data as defined within Data Protection Laws including rights of access, rectification, restriction of processing, erasure, data portability, and restriction of Processing. Data Subjects' rights are not absolute and the College may not be able to entertain these requests if it is prevented to so in terms of the applicable law.



### 11.3 Third-Party Access

11.3.1 Access to any CCTV material is only granted to third parties that are eligible to it by law, including but not limited to any law enforcement body, where any other authority/entity shall request such material by means of a warrant or other form of lawful order. The disclosure of CCTV material will only be made in accordance and in compliance with Data Protection Laws.

## **12. STORAGE AND RETENTION**

12.1 Any images and/or recordings by the CCTV System will be stored in a secure environment with a log of access restricted to authorised personnel. In certain circumstances any material can be viewed by other individual having the authorization from the Rector and/or the Data Protection Officer.

12.2 Any material captured by the CCTV system will be retained for a maximum of 7 days, except in the case where such material identifies an issue and is retained for the purposes of an investigation.

## **13. SECURITY**

13.1 The College CCTV System is controlled by a security company contracted by the College. The College has a written contract with the security company in place, detailing the areas to be monitored, the time-period for storing data.

13.2 The College and the Security Company shall implement and maintain appropriate technical and organizational security measures, considering the nature, scope and context and purposes against unauthorised access, disclosure, copying, modification, storage or reproduction of material captured by the CCTV System and against unlawful loss, destruction, alteration or disclosure of such material.

## 14. COMPLAINTS AND FEEDBACK

- 14.1 Any complaints or concerns about the use of CCTV at the College should be directed to the Data Protection Coordinator and/or College Executive Board. Any member of the staff, students, parents, visitors or any other member of the public can address any concerns either via telephone on 21246613 (Pieta) or 21236367 (Marsa) or via e-mail at [college@sac.mcs.edu.mt](mailto:college@sac.mcs.edu.mt). Alternatively, the College's Data Protection Officer may be contacted via e-mail [david.cortis@sac.mcs.edu.mt](mailto:david.cortis@sac.mcs.edu.mt).

## 15. IMPLEMENTATION AND REVIEW

- 15.1 This policy shall be reviewed every scholastic year and updated as necessary by the Senior Leadership Team, while approved by the College Executive Board.
- 15.2 New CCTV systems will be introduced in consultation with staff and the board of management, whilst undergoing a privacy impact assessment prior to the implementation of any new CCTV equipment.
- 15.3 The date from which the policy will apply is the date of adoption by the Rector of the College. The implementation of the policy will be monitored by the Rector of the College.
- 15.4 **This policy is being adopted from 15 July 2019**