CCTV Policy

Contents

1. Introduction

1.1 Scholars School System is committed to providing a safe and secure learning environment across its campuses and buildings. The SSS therefore operates close circuit television cameras (CCTV) across its campuses and buildings for the security and safety of its staff and students.

1.2 Closed Circuit Television (CCTV) cameras are installed to view and record the activities of individuals overtly at selected locations on SSS premises. The operation of these cameras is a strategic component of the SSS commitment to staff and student safety, security and crime prevention.

1.3 The SSS's use of CCTV is covered by the General Data Protection Regulation (GDPR). Identifiable imagery is considered as personal data under the GDPR and, therefore, this policy is committed to the protection of individuals' rights and privacy. The processing of personal data such as the collection, recording, use, and storage of personal information through the CCTV system will be dealt with lawfully and correctly in accordance with the SSS's Data Protection Policy.

2. *CCTV System*

2.1 The CCTV system adopted includes internal / external; static colour / black and white; full pan, tilt and zoom cameras. Pan, tilt and zoom (PTZ) function is employed only on playback but not in real time live recording mode and area viewed is pre-set and static, especially for all external cameras.

2.2 The vast majority of CCTV cameras are IP based and connected to the SSS IT network. The system records CCTV data in real time to specific Networked Video Recorders (NVR) in secure locations across the SSS estate. For buildings were analogue CCTV system is in use, the camera output is cabled to Video Camera Recorders (VCR's) with real time recording available on motion sensors. The output of the cameras can be relayed between the VCR's and authorised desk top computers via web links on the Universities computer network.

2.3 All CCTV cameras are set to motion detection, which means real time recording will be automated only when there are activities, that is, movement in the area. This ensures the system does not record when there are no activities taking place and guarantee sufficient disk recording space, maximise digital deletion or the recorded data ascribed retention period.

2.4 The Executive member responsible for the system is the Director operations, Centre Managers, HR & Admin officer and the IT Data Administrator. The Scholars School System is the owner of all recorded CCTV data.

3. *Purpose of the CCTV System*

3.1 The purpose of the CCTV system is as follows:

- To enhance "Safety, Security and Crime Prevention on SSS premises".
- Safety of staff, students, contractors and visitors.
- Provide an effective means by which to prevent and reduce crime in the monitored areas through an increased fear of detection and the prevention of offenders.
- Assist in the factual, accurate and speedy reconstruction of the circumstances of incidents.
- To assist the SSS and police in providing a swift response to criminal activity and provide evidential material for court and disciplinary proceedings.
- Protect the SSS assets.
- To assist in supporting SSS Health and Safety policies.
- To assist in the event of an emergency or disaster.

4. *Scope*

4.1 The CCTV system is intended to view, monitor and record activities within SSS premises. It will focus primarily, but not limited to, key entry and exits points to premises, building perimeters, certain communal areas and others parts where CCTV is recommended to mitigate against risks to safety and security.

4.2 Every possible effort has been made in the planning and design of the CCTV system to give it maximum effectiveness. However, it is not possible to guarantee that the system will see every single incident taking place in the areas of coverage.

4.3 The CCTV system must strike an appropriate balance between the personal privacy of individuals using the campuses/buildings and the objective of recording incidents.

4.4 The system will be operated fairly to ensure that all CCTV data is processed in accordance with GDPR, the Data Protection Act 2018 and the SSS Data Protection Policy and only for the purposes to which it is established.

4.5 The system is not intended to invade the privacy of any individual in residential, business or other private premises, buildings or land not belonging to the SSS.

4.6 No sound will be recorded in public places and CCTV is not used to record conversations.

4.7 No images will be captured in areas where individuals would have an expectation of privacy (for example; toilets, washrooms etc.).

5. Signage

5.1 Strategically placed CCTV camera notices at key entry points to SSS premises will advise individuals that they are entering an area which is covered by CCTV cameras.

5.2 The CCTV notice at entrances to Scholars School System and in adjacent areas will contain:

- The name of the Data Controller. (i.e. Scholars School System)
- The purpose(s) of the scheme.
- The contact details for enquiries.

6. Data Protection

6.1 This policy document will be implemented to ensure that the deployment and control of CCTV resources is proportionate and lawful under the terms of the General Data Protection Regulations (GDPR 2018), the Data Protection Act 2018 and the CCTV Codes of Practice issued by the Information Commissioner Office (ICO).

6.2 In summary, personal data should be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

6.3 The lawful basis identified for processing the personal data as part of the CCTV system is legitimate interests.

6.4 This CCTV Policy should be read in conjunction with the following policy documents:

- Scholars School System Data Protection Policy
- Privacy Statement
- Property Services Records Retention Schedule.

7. Responsibilities

7.1 This CCTV Policy should be read in conjunction with the following policy documents: Scholars School System as owner has responsibility for compliance with the purposes and objectives of the system including operational guidance and the protection of the interests of the SSS users and privacy of the individuals whose images are captured on the system. This responsibility is undertaken by the following members of staff.

7.2 Director operation / Centre Managers: The Director Operations / Centre Managers shall have responsibility for the CCTV infrastructure, ensuring there is an adequate maintenance regime, upgrades to CCTV hardware and software, so they are fit for purpose. The Director will support the Head of Admin/HR/Security in developing and maintaining good CCTV data processing and handling practice within the SSS in accordance with the Data Protection Policy and the Information Security Policy.

7.3 Head of Security: The SSS Head of Admin/HR/Security is responsible for the day to day management and control of the CCTV system on behalf of the SSS. Where management of the CCTV system is part of an outsourced contract to a TFM provider, he will work closely with the TFM partner to ensure service and maintenance agreements are carried out as dictated by the TFM contract or industry standard. Only security officers fully trained and who hold any relevant licenses required by regulatory authorities will be permitted to process data from the CCTV system. The Head of Admin/HR/Security will work with the TFM provider of security services and CCTV contracts, to create an awareness of Data Protection Dos and Don’ts to security staff.

7.4 IT Data Administrator and/or Admin Head: IT Data Administrator is responsible for protecting all data on the SSS’s IT systems and will ensure there are appropriate technical and organisational security measures in place to protect CCTV data on the system.

8. Assessment of the Policy

8.1 The Head of Admin/HR/Security will evaluate the system annually to consider the following:

- The assessment of impact upon crime.
- Assessment of areas without CCTV.
- The views of the users.
- Operation of the policy.
- Whether the purposes for which the scheme was established still exist.
- Future functioning, management and operation of the system.

9. Management of the System

9.1 The Head of Admin/HR/Security is responsible for the management of the SSS's CCTV system. This includes the maintenance and operation of the system as well as the protection of the privacy interests of individual members of the SSS and the public from intrusive monitoring.

9.2 The Head of Admin/HR/Security will ensure that all Security staff involved in the recording, observation and capture of images are informed, through training on operating the CCTV system or through other means, of their responsibility to act in an ethical and lawful manner in line with relevant legislation and industry standards.

9.3 For the purpose of viewing CCTV images, an authorised person is defined as an employee or appointed person acting on behalf of Scholars School System who has an operational responsibility for either the prevention, investigation or detection of crime and / or the monitoring of the security and safety of the premises at Scholars School System.

9.4 All reported abuse or inappropriate use of the CCTV system will be investigated and if proven, the SSS will take appropriate measures to eliminate or minimize the risk of reoccurrence. Inappropriate use of the CCTV system will be considered a breach of SSS policy and will be handled accordingly.

10. Access To CCTV Monitors and Monitoring Equipment

10.1 CCTV monitors which display live images may be installed in public areas to show live images of activities in the area. This may be deployed when it is important to emphasise an area is under CCTV surveillance as a deterrent to criminal activities, antisocial behaviour or allay any safety concerns within the area. The monitor displays only a scene or live images which is also in plain sight from the monitor location. Unless specifically designed for these purposes, access to CCTV monitors or display screens will be restricted to persons authorised to view those images.

10.2 All CCTV recording equipment will be located within secure areas and only accessible to authorised personnel.

10.3 Where software application allows remote access to the system for authorised staff via the web link, access rights to the systems will be highly password protected.

11. Recording and Storage of Information

11.1 All recorded material will be treated as confidential and unless required for evidence, will be kept in accordance with this policy.

11.2 The CCTV systems are operated and monitored 24 hours a day, every day of the year.

11.3 CCTV images not to be retained for longer than necessary. Data storage is automatically managed by the CCTV digital recorders which use software programme to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces a minimum of 30 days rotation in data retention.

11.4 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal or disciplinary proceedings), the images will be erased following the expiration of the retention period.

11.5 If CCTV images are retained beyond the retention period, they will be stored in a secure place with controlled access and erased when no longer required.

11.6 Access to the CCTV System and to the captured images will be restricted to authorised staff involved in monitoring or investigation.

12. Access and Disclosure of CCTV Images

12.1 Requests for access to (review), or disclosure of (i.e. provision of a copy), of images recorded on the CCTV systems from third parties (i.e. unauthorised persons) will only be granted if the requestor falls within the following types of person / organisation:

- Data Subjects (i.e. persons whose images have been recorded by the CCTV systems)
- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution agencies (including SSS Managers in the course of Staff or Student disciplinary proceedings)
- Relevant legal representatives of data subjects

12.2 Images from CCTV must not be forwarded to the media for entertainment purposes or be placed on the internet.

12.3 Images will only be released to the media on the authority of the Director Operations and following advice from law enforcement agencies to support police investigations.

12.4 Right of Access: Staff, students and other data subjects about whom the SSS holds or uses personal data have a legal right to access that information and request a copy of the data in permanent form. Any person wishing to exercise their right of access formally should complete the “CCTV Subject Access Form” and submit it along with proof of identity to prevent unlawful disclosure of personal data to: accessrequest@scholarsschool.ac.uk An electronic copy of the CCTV Subject Access Form can be obtained on request.

12.5 By law, the SSS has one month from receipt of the request along with proof of identity, in which to respond to subject access requests. In any event the SSS will endeavour to respond as quickly as possible. In limited circumstances, the SSS may not be able to release personal data because exemptions under the Legislation are applicable, or the disclosure of the data would release personal data relating to other individuals.

12.6 Staff who receive enquiry for personal information from an individual (data subject) or a third party acting on behalf of a data subject, should be directed to complete the CCTV Data Access Request form. All requests should be sent to: accessrequest@scholarsschool.ac.uk

12.7 Where a third party is acting on behalf of a data subject, written authorisation from the data subject must be provided to confirm that the third party is acting on their behalf.

12.8 The SSS has discretion to refuse any third-party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once an image has been disclosed to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with the Data Protection Legislation in relation to any further disclosures.

12.9 It may be necessary for redaction of images on copies of CCTV issued following a subject access request. This is usually to protect third-party data. Where redaction is deemed impossible for example huge video files, the SSS may refuse a CCTV data request if providing this data infringes on the rights to privacy of others.

12.10 The contact point indicated on the CCTV signs around Scholars School System should be available to members of the public during normal business hours.

12.11 Whenever, recorded CCTV images are viewed or copy of data released authorised persons/organisation, a log must be maintained and signed by the issuer and requestor on the SSS Security CCTV management pack.

12.12 All disclosed CCTV data must be safely delivered to the intended recipient ideally by handing over information on a sealed data disc or other media storage device with encryption embedded in the CCTV application software. CCTV recorded data must not be transmitted by email.

12.13 Only the SSS Director Operations and the Head of Admin/HR/Security can authorise the viewing or release of CCTV data.

12.14 Please visit the ICO website for further information on the above rights. You may also contact the Head of HR & Admin for further information.

13. Liaison with the Police Services

13.1 Images may be released to the Police Service or other law enforcement agencies in compliance with Police Act 1996 Section 30(1) and Section 29(3), Section 30(5) of the DPA 1998 now promulgated in the Data Protection Act 2018 and General Data Protection Regulations (GDPR 2018).

13.2 All CCTV data requests from the Police Services or other law enforcement agencies should be referred to the Head of Admin/HR/Security.

13.3 All CCTV data viewed or released to the police must be logged in the SSS security CCTV management register. Visiting police officers must provide their standard issued badge as proof of identity and provide signatures for any CCTV collected.

14. Installation

14.1 The CCTV installations are carried out by Scholars School System.

14.2 Any technological change, which will have a significant effect upon the capacity of the system, will be fully assessed in relation to the purpose and key objectives of the system.

14.3 The SSS reserves the right to deploy/restrict/cease the use of dummy cameras as part of the system subject to applicable laws, ICO code of practice or police directive

15. Staff

15.1 All the Staff involved in the recording, observation and capture of images must act in an ethical and lawful manner in accordance with legislation and must receive adequate training to ensure their understanding of compliance legislation.

15.2 Training will include how to identify suspicious behaviour, when to track individuals or groups and when to take close up views of incidents or people and compliance with Data Protection Act and any other relevant legislation. Staff with access to CCTV data should be particularly careful not to infringe upon the Public's Human Rights. The effectiveness of individual operators will be reviewed periodically.

15.3 Only authorised persons involved in the monitoring or investigation can view CCTV images.

15.4 The CCTV policy as with all other SSS policies and procedures are deemed reasonable management instructions covered by an employee's contract of employment. As a result, breaches of any aspect of this policy may result in disciplinary penalties or be referred to the police as the subject of criminal or civil offence investigation.

15.5 Unless authorised by the SSS Director Operations, only the Head of Admin/HR/Security and their nominees may review stored recordings or down load information for the police or SSS.

16. Complaints

16.1 All complaint and enquiries relating to the CCTV system should be addressed to: Head of Admin/HR/Security, Scholars School System, Smithfield House 24-28 Digbeth Birmingham B5 6BS.

17. Breaches of the Code

17.1 Breaches of the policy and of security will be investigated by the Head of Admin/HR/Security or the Data Protection officer's nominee. Recommendations and corrective action plans will be put in place to remedy any breach which is proven.

17.2 The SSS Director Operations and the Head of Admin/HR/Security are responsible for maintaining a record of CCTV data breaches as part of the policy.

17.3 All breaches of personal data must be reported to the SSS Secretary and Chief Compliance Officer who is the appointed Data Protection Officer for the SSS.

18. Access Request Form

18.1 Under the General Data Protection Regulation (GDPR) you are entitled to request the personal data that we hold about you. Please use the form available on the SSS website to specify the data that you wish to access. Under GDPR we have one month in which to respond to you.