Lawnswood Campus

CCTV Policy

2019

Review Date: Autumn 2022

Please read
Governors as Management Board
Schools as PRUs

Signed by the Chair of the Management Board: …… Date:……

CCTV Policy and Operational Procedures

Contents

1. Introduction

The purpose of these procedures is to provide assistance in the operation, management and regulation of the CCTV systems in place at Lawnswood Campus.

The CCTV system is owned and operated by Lawnswood Campus, the deployment of which is determined by the Centre's Senior Leadership Team and Management Board.

These procedures follow the ICO "Code of Practice for Surveillance Cameras and Personal Data', the Data Protection Act 2018 (GDPR) guidelines and the Campus's Data Protection Policy which is available to view on the Lawnswood Campus website.

1.1 Exemptions

The use of cameras (non-surveillance) for domestic purposes is exempt from the Data Protection Act e.g. a video of pupils participating in school performances (Christmas/drama productions, etc.), school sports events recorded for the parent/carer's own family use.

The use of cameras or other recording devices (not CCTV) by the news media or for artistic purposes, such as for film making, are not covered by these procedures as an exemption within the DPA applies to activities relating to journalistic, artistic and literary purposes.

2. Lawful Processing

Lawnswood Campus has responsibility for the safeguarding of children and staff who are present onsite under the requirements of Keeping Children Safe in Education (statutory guidance). The Centre owes a duty of care under the provisions of the Health and Safety at Work Act 1974 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment to support these responsibilities.

The use of CCTV, and the associated images and any sound recordings made by Lawnswood Campus is covered by the Data Protection Act 2018.

These procedures outline the Centre's use of CCTV and how it complies with the Act. We have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate to the needs that we have identified. We have also considered less privacy intrusive methods of achieving this need where possible.

The use of CCTV to control the perimeter of the Centre's buildings and entrances/exits for security purposes has been deemed to be justified by the Management Board

3. Objectives of the CCTV System

The system is comprised of fixed cameras located around the site both externally and internally for the purpose of capturing images of intruders or of individuals damaging property or removing goods without authorisation and/or instances of poor behaviour, for example. CCTV systems will not be used to monitor the quality of teaching in Centres, classrooms will only be accessed why an incident has occurred. CCTV will be used for the purpose of:

- protecting the Centre buildings and assets, both during and after Centre hours;
- increasing the personal safety of staff, students and visitors;
- reducing the fear of crime;

- reducing the risk of 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;
- protecting members of the public; and
- ensuring that the Centre rules are respected so that the Centre can be properly managed.

4. Roles and Responsibilities

The Data Protection Officer will be responsible for monitoring compliance with these procedures.

Heads of Centre are responsible for all day-to-day leadership around data protection matters.

All authorised operators and employees with access to CCTV images will be made aware of these procedures prior to access being granted to CCTV systems. All operators have also received training in the data protection responsibilities of employees in Centre. In particular, they have been made aware of:

- What the Centre's arrangements are for recording and retaining information
- How to handle the information securely
- How to recognise a subject access request and what to do if they receive one
- What to do if they receive a request for information from an Official Authority, for example, or the Police.

Monitoring for security purposes will be conducted in a professional, ethical and legal manner. Any use of CCTV systems for other purposes is strictly prohibited.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with existing policies adopted by the Centre including the Data Protection Policy.

The Centre's procedures for video monitoring prohibit monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc. The system is in place to monitor suspicious behaviour and not individual characteristics.

CCTV monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by law.

Cameras will be used only to monitor activities around the external areas of the Centre and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the Centre, together with its visitors.

Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000 (RIPA).

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police.

The planning and design has endeavoured to ensure that the surveillance system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the ICO Code of Practice, have been placed at all access routes to areas covered by the Centre's CCTV.

Information obtained through the CCTV system may only be released when authorised by the Head of Centre or Data Protection Officer. Any requests for CCTV recordings/images from the Police will be logged by the Centre and the Data Protection Officer. If a law enforcement authority is seeking a recording for a specific investigation, any such request should be made in writing.

5. Operation of the System

- The CCTV system will be administered and managed by eServices, in accordance with the principles and objectives expressed within these procedures.
- The day-to-day management will be the responsibility of eServices and the Site Team during the day, out of hours and at weekends.
- The system is network based and can be accessed from a number of devices.
- Access to specific Centres will be managed by software permissions
- The CCTV system will be operated 24 hours each day, every day of the year.
- Regular functionality/maintenance checks on all cameras will be performed at every Campus ICT meeting, currently held on a Friday and over the lunchtime period.

5.1 CCTV Control / Monitors

Viewing of live images on monitors in the Centre is usually restricted to the operator and any other authorised person where it is necessary for them to see it, e.g. to monitor access/egress points around the site.

Devices should be carefully positioned when viewing CCTV so that they are only visible to staff. Parent/carers and members of the public are not allowed to access areas where CCTV monitors are visible.

Recorded images are also viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy is restricted to authorised personnel.

On the Campus, the control of the CCTV system is network based, so can be accessed from a variety of secure locations.

- eServices will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional. A scheduled task at each and every Lawnswood ICT Group meeting during Friday Lunchtimes.
- CCTV Contractors wishing to access or control the system will be subject to particular arrangements as outlined below.
- CCTV Operators must satisfy themselves over the identity of any contractors accessing CCTV systems and the purpose of the visit. Where any doubt exists, access will be refused.
- All devices with access to CCTV should be secured at all times.
- Other administrative functions will include maintaining CCTV footage and network storage, filing and maintaining occurrence and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Siting of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify.

The Centre has endeavoured to select locations for the installation of CCTV cameras which are the 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 the Centre may include the following:

- Protection of Centre buildings and property: The building's perimeter, entrances and exits.
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas.
- Video Patrol of Public Areas: Parking areas, main entrance/exit gates.
- Criminal Investigations (carried out by the Police): Robbery, burglary and theft surveillance.

The following points were considered when the CCTV cameras were installed:

- Camera locations were chosen carefully to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.
- The cameras have been sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- Cameras are suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- We have checked that a fixed camera positioned in winter will not be obscured by the growth of plants and trees in the spring and summer.
- Cameras are sited so that they are secure and protected from vandalism.
- The system will produce images of sufficient size, resolution and frames per second.

7. Covert Surveillance

The Campus will not engage in covert surveillance.

Certain law enforcement agencies may request to carry out covert surveillance on Centre premises. Such covert surveillance may require a Court Order. Accordingly, any such request made by law enforcement agencies will be requested in writing. The covert surveillance activities of public authorities are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

8. Notification – Signage

The Centre will provide a copy of these CCTV Procedures on request to staff, students, parents/carers and visitors to the Centre. These procedures describe the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use.

The Centre is required to notify individuals when they are in an area where a surveillance

system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Signs will be:

- clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);
- include basic contact details such as a simple website address, telephone number or email contact; and
- of an appropriate size.

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 the Centre property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

All staff will be made aware of what to do or who to contact if a member of the public makes an enquiry about the surveillance system.

9. Retention, Viewing and Storage of Images

9.1 Retention

The Data Protection Act 2018 does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose.

The Data Protection Acts states that data "shall not be kept for longer than is necessary for"

the purposes for which it was obtained. As a data controller, the Centre needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a calendar month (30 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue. Footage will be retained only within the network storage. It will be overwritten automatically as the disk space is used up. To account for the long summer holiday of 6 weeks, the system will retain footage for up to 8 weeks before being automatically deleted over the summer holiday period.

9.2 Viewing & Storage

All viewing events are recorded automatically by the software – it logs: user names; all session activities in terms of log in and out; session type: playback or export and the time viewed.

Recorded material will be stored in a way that maintains the integrity of the information on the system's network. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose.

Recorded material is stored in a secure network location. Access to recorded material is restricted to the Senior Leadership Team. Passwords to access the system will not be disclosed.

Access will be restricted to authorised personnel as above. Supervising the access and maintenance of the CCTV system is the responsibility of the Headteacher and Lawnswood ICT Group. The Headteacher may delegate the administration of the CCTV system to another staff member.

In certain circumstances, the recordings may also be viewed by the Data Protection Officer and other individuals in order to achieve the objectives set out above e.g. the Police, other members of the teaching staff, representatives of the DfE, representatives of the HSE and/or the parent of a recorded student. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

9.3 External Drive Procedures

In order to maintain and preserve the integrity of the data used to record events from the network storage and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- The use of external drives / DVDs should be avoided.
- CCTV footage can be shared from a cloud location providing security measures are in place
- Police favour the method of recording footage device to device using smart technology. Where possible this should be the preferred method of sharing.

10. Disclosure of Images

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the Centre where these would reasonably need access to the data (e.g. investigators). In relevant circumstances, CCTV footage may be disclosed:

- To the Police where the Centre is required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the 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 the Centre property, or
- To the HSE and/or any other 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/carers will be informed. The data may be used within the Centre's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures; 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 the Centre; or
- To individuals (or their legal representatives) subject to a court order; or
- To the Centre's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Only the Senior Leadership Team or Data Protection Officer are allowed to make external disclosures of CCTV footage.

Data will never be placed on the internet and will not be released to the media. Information may be released to the media for identification purposes, but this must NOT be done by anyone other than a law enforcement agency.

Once we have disclosed information to another body, such as the Police, they become the Data Controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures.

10.1 Requests by the Police

Information obtained through video monitoring will only be released when authorised by the Headteacher following consultation with the Data Protection Officer. If the Police request CCTV images for a specific investigation, any such request made by the Police should be made in writing.

- Data may be viewed by the Police for the prevention and detection of crime, authorised officers of the Local Authority for supervisory purposes, authorised demonstration and training.
- A record will be maintained of the release of data to the Police or other authorised applicants. A register will be available for this purpose.
- Viewing of data by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under Part 3 of the Data Protection Act 2018.
- Should images be required as evidence, a copy may be released to the Police under the procedures described previously in these procedures.
- The Police may require the Centre to retain the stored Data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Data Protection Officer. In these circumstances, data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

10.2 Other Requests to view CCTV Footage

All other requests to view CCTV footage should be made in accordance with the Lawnswood

Data Protection Policy, this is available upon request or is downloadable from the website: https://www.lawnswood.org.uk/policies

11. Breaches of the Procedures (including security breaches)

- Any breach of these procedures by Centre staff will be initially investigated by the Data Protection Officer, in order for him/her to take the appropriate disciplinary action.
- Any serious breach of the procedures will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.
- Information obtained in violation of these procedures may not be used in a disciplinary proceeding against an employee of the Centre, or a student.

12. Monitoring and Review

Routine performance monitoring, including random operating checks, may be carried out by the Senior Leadership Team, eServices or Data Protection Officer.

These procedures will be regularly reviewed by the Data Protection Officer. This is to ensure the standards established during the setup of the system are maintained.

Similarly, there will be a periodic Management Board review, at least annually, of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified. The review will take into account the following:

- Is it addressing the needs and delivering the benefits that justified its use?
- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include our commitment to the recommendations in the ICO Code of Practice and include details of the ICO if individuals have data protection compliance concerns?
- Is a system of regular compliance reviews in place, including compliance with the provisions of the ICO Code of Practice, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

The periodic review will also ensure all information is sufficiently protected to ensure that it does not fall into the wrong hands. This will include technical, organisational and physical security. For example:

- Sufficient safeguards are in place to protect wireless transmission systems from interception.
- The ability to make copies of information is restricted to appropriate staff.
- There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.
- Where information is disclosed, it is safely delivered to the intended recipient.
- Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information.
- Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.
- The process for deleting data is effective and being adhered to.
- If there has been any software updates (particularly security updates) published by the equipment's manufacturer that they have been applied to the system.

13. Complaints

- Any complaints about the Centre's CCTV system should be addressed to the Data Protection Officer DPO@lawnswoodcampus.co.uk
- Complaints will be investigated in accordance with the Centre's Complaints Policy.

14. Review

- This policy will be reviewed every 3 years or if the CCTV system is upgraded, whichever comes first.