Jordanhill School

CCTV Policy

INTRODUCTION

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 environs of the premises under the remit of Jordanhill School.

CCTV systems are installed (both internally and externally) on the school's premises for the purposes of

- protecting the school buildings and school assets, both during and after school hours
- supporting secure access systems
- promoting the health, safety and well-being of staff, pupils and visitors
- ensuring that the school rules and polices are respected so that the school can be properly managed
- minimising crime and anti-social behaviour (including bullying, theft and vandalism)
- supporting the Police in a bid to deter and detect crime

GENERAL PRINCIPLES

Jordanhill 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, pupils and visitors to its premises. Jordanhill School owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 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 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. Information obtained through the CCTV system may only be released when authorised by the Rector (or his delegated/appointed senior management colleagues).

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school, including Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, 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.

CCTV systems will not be used to monitor normal teacher/pupil classroom activity in school.

All CCTV systems and associated equipment will be required to be compliant with this policy.

Data Protection

Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Acts 1988 and 2003 and the school's Data Protection Policy.

Images captured by the CCTV system will be retained for a maximum of 40 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 access restricted to authorised personnel.

Section 2(1)(c)(iii) of the Data Protection Acts 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 Board of Managers.

LOCATION OF CAMERAS

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

- **Protection of school buildings and property:** The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, refuse areas and receiving areas for goods/services. This list is not exhaustive

- **Monitoring of access control systems:** Monitor and record restricted access areas and entrances to buildings and other areas

- **Verification of security alarms:** Intrusion alarms, exit door controls, external and internal alarms

- **Video patrol of public areas:** parking areas, main entrance/exit gates, traffic control

- **Criminal investigations (carried out by the police):** Robbery, burglary, theft and other relevant surveillance

COVERT SURVEILLANCE

Jordanhill School will not engage in covert surveillance unless it can reasonably justify the need to.

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

NOTIFICATION – SIGNAGE

The Bursar will provide a copy of this CCTV Policy on request. This policy describes the purpose and general location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. Adequate signage will be placed around the school campus and will also be prominently displayed at the entrance to Jordanhill School property. Signage shall include the name and contact details as well as the specific purpose(s) for which the CCTV cameras are in place.

An example of typical signage:

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, school gates
- reception areas
- other internal or external areas deemed appropriate to support awareness

Signage is not intended to be excessive.

RESPONSIBILITIES

The Board of Managers and Senior Management Team will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Jordanhill School
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring is consistent with the highest standards and protection
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Ensure that nominated personnel maintain a record of access (e.g. an access log) to release tapes or any material recorded or stored in the system
- Ensure that images are duplicated for release only when compliant with Data Protection and other legislation
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by the Police]
- Give consideration to both pupil 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
- Co-operate with the Health & Safety Officer of Jordanhill School in reporting on the CCTV system in operation in the school
- 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 are stored for a period not longer than 40 days and are then erased unless required as part of an internal investigation, criminal investigation or court proceedings (criminal or civil) or other bona fide use
- Ensure that camera control is solely to monitor suspicious behaviour or conduct, 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 the Police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Convenor of the Board.

Day-to-day responsibility may be delegated to the Bursar, IT manager or other senior officer as appropriate.

IMPLEMENTATION & REVIEW

Implementation of the policy will be monitored by the Rector of the school supported by the senior management team.

The policy will be reviewed and evaluated from time to time within the school's established cycle of policy review. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Information Commissioner, national management bodies, legislation and feedback from parents/carers, pupils and staff).

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 Acts – The Data Protection Acts 1988 and 2003 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 Acts 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 Section 3 and/or section 4 of the Data Protection Acts.
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 Acts place responsibilities on such entities in relation to their processing of the data.

APPENDIX 2 - PRIVACY IMPACT ASSESSMENT

Before the school installs any new CCTV system, it is recommended that a documented privacy impact assessment is carried out.

Some of the points that might be included in a Privacy Impact Assessment are:

- What is the schools purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and pupil safety or crime prevention?
- Is it proportionate to the problem it is designed to deal with?
- Is it intended that CCTV cameras will operate inside and outside of the building?
- Are internal CCTV cameras justified under the circumstances?
- What are the benefits to be gained from its use?
- Can CCTV systems realistically deliver these benefits?
- What future demands may arise for wider use of images and how will they be addressed?
- What are the views of those who will be under CCTV surveillance?
- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, pupils and visitors been assured that the CCTV system will be used only for the stated purposes?
- Does the school's policy on the use of CCTV make it clear that staff will not be monitored for performance purposes?
- Have the views of staff and pupils regarding the location of cameras been taken into account?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- Has appropriate signage been erected?
- Who will have access to the system and recordings/images?
- What security measures are in place to protect the CCTV system and recordings/images?
- Are those who will have authorised access to the system and recordings/images clear about their responsibilities?
- Where appropriate, are the camera monitors kept out of view of staff, pupils and visitors and is access to the camera monitors restricted to a limited number of staff on a 'need to know' basis?
- Does the school have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (40 days) has expired?
- Does the school have a data protection policy? Has is been updated to take account of the CCTV system?
- Does the school have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe)?
- Has the right of access been communicated to staff, pupils and visitors?
- Has the school communicated its policy on the use of CCTV to staff, pupils and visitors and how has this been done?
- How are new pupils and new staff informed of the school's policy on the use of CCTV?