DOC NUM: 810.1

CCTV POLICY

GLENARD UNIVERSITY RESIDENCE

VERSION 2.0

STATUS: APPROVED

2 JUNE 2021

BROSNA EDUCATIONAL CENTRES CLG
6 Clare Street, Dublin 2, D02 EF82
www.brosna.ie

TABLE OF CONTENTS

1 INTRODUCTION

Glenard University Residence ("Glenard"), a centre operated and managed by Brosna Educational Centres CLG ("Brosna") and located at 36 Roebuck Road, Dublin 14, is committed to providing a safe and secure environment for its staff, residents and all those who attend activities run in Glenard. To this end Glenard has installed a single camera Closed Circuit Television (CCTV) surveillance system to monitor the use of the residence's side entrance door.

The aim of this Policy is to describe the purpose of the CCTV system in Glenard and to provide guidelines to regulate the management, operation and use of the system in a way that enhances security while at the same time respecting the expectation of reasonable privacy of those who work and live in Glenard or attend activities run by the residence (i.e. staff, residents and visitors).

This Policy is informed by the principles set out in the General Data Protection Regulation ("GDPR"), Data Protection Law and the Freedom of Information Act 2014 together with guidance issued by the Office of the Data Protection Commissioner [1]. This Policy will be periodically reviewed in order to ensure that the CCTV system continues to comply legal and regulatory requirements.

Brosna manages Glenard and is solely responsible for its CCTV system. Brosna is, therefore, the data controller for any personal data recorded by the system. Any questions or requests for information relating to this Policy should be emailed to office@brosna.ie and marked for the attention of Anne Brady. Alternatively such requests may be posted to : Anne Brady, Brosna Educational Centres CLG, 6 Clare Street, Dublin 2, DO2 EF82.

2 OVERVIEW OF THE CCTV SYSTEM

1. Glenard operates a single non-covert internal CCTV camera. Specifically:
   - An internal camera fixed to the wall of an internal corridor which leads to the residence's side entrance door
   - The camera is pointed at the side entrance and the camera's coverage area is limited to the side door entrance and part of the internal corridor where the side door is located.
   - Appropriate signage is located both internally and externally at the side entrance where the CCTV is located
2. The camera does not cover any bathrooms or access doors to bathrooms
3. The camera does not cover internal work areas or office spaces
4. The camera is connected to a Network Video Recorder (NVR) which is located in a secured press in the residence
5. The NVR is connected to the residence's local area network. Logical access is restricted and suitably protected. The Residence Manager and her nominated deputy are the only ones with access to the system
6. The CCTV system does not employ face recognition technology

3 PURPOSE OF CCTV[1]

The CCTV camera has been installed primarily for security reasons. There is an unmanned side entrance to the residence located towards the rear of the building which provides residents with an additional entry point to the building via keypad access and is used regularly throughout the day and may also be used outside normal business hours. The side entrance is primarily used by residents but may also be used by visitors to access the oratory which is also located in this part of the building.

The CCTV system has been installed in order to:

- enhance the security of the Residence;
- assist in the maintenance of a healthy & safe environment for residents of, and visitors to, the Residence;
- safeguard the Residence's assets and the property of residents;
- act as a deterrent to potential intruders;
- facilitate the prosecution of criminal and/or legal proceedings; and
- support the investigation of staff and/or student disciplinary offences under the Residence's House Rules and, in particular, breaches of House Rules which have health & safety implications for residents and visitors

The personal data collected by the CCTV system shall only be used for the above purposes.

4 LEGAL BASIS FOR USE OF CCTV

Brosna has a legal and a moral obligation to ensure that Glenard is a safe and healthy environment for staff, residents and visitors. The CCTV is one of the measures that Brosna has put in place to meet its obligations in this regard. The impact on privacy is considered to be minimal and is deemed to be proportionate to the duty-of-care that Brosna has to those who work in, live in and visit the residence.

5 NECESSITY & PROPORTIONALITY

1. Article 5.1(c) of the GDPR requires that data is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". After due consideration, the use of CCTV to monitor the side entrance to the residence for security purposes and health & safety reasons has been deemed to be justified by Brosna.
2. Given that this entrance is used by both residents and visitors, is unmanned and is not in view from the main road, the CCTV system is considered a necessary and proportional measure to the secure this entry point to the Residence.

[1] Ref: Article 5 (1) (b) of GDPR that personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*"

6 NOTIFICATION & SIGNAGE

A copy of this CCTV Policy is available to staff, residents and visitors to the residence. This policy describes the purpose and location of CCTV monitoring, and contact details for those wishing to discuss CCTV monitoring and guidelines governing its usage.

The CCTV camera is non-covert and signage is suitably located both externally at the side entrance and on the wall in the internal corridor where the CCTV is located to alert users of the side entrance of its presence.

Figure 1: CCTV Signage used at Glenard University Residence

7 RETENTION SCHEDULE

Article 5.1(e) of the GDPR states that data shall be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are published.*" The images captured by the CCTV system are retained for a maximum of 30 days, except in the following cases:

(a) the footage relates to a possible security incident and is retained specifically in the context of an investigation into that incident
(b) the footage relates to an identified health & safety issue and is retained specifically in the context of an investigation into that issue
(c) the footage is in scope of a data subject access request
(d) the footage has been accessed by, or released to, a third party e.g. An Garda Síochána or Brosna's insurance company

In general, unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will not be retained for more than 30 days after the date of recording. Recordings will be automatically overwritten after 30 days.

When a recording is required to be held in excess of the retention period referred to above, the Residence Manager, or her nominated deputy, will be responsible for authorising the retention of the a recording.

Recordings held in excess of the retention period will be reviewed on a three monthly basis and any recordings not required for evidential purposes will be deleted.

Access to retained CCTV recordings is restricted to the Residence Manager and other persons authorised by the Residence Manager who need to have access in accordance with their role and with the purposes of the system.

8 ACCESS TO CCTV RECORDINGS

8.1 STORAGE

The retained recordings are stored in a secure press and access is restricted to authorised personnel only. Logical access to CCTV recordings is protected with a suitably strong password which is only shared with authorised personnel.

8.2 ACCESS TO CCTV RECORDINGS

Supervising access to, and maintenance of, the CCTV System is the responsibility of the Residence Manager or her nominated deputy. When CCTV recordings are being viewed, access is limited to authorised individuals who need to have access in accordance with their role and with the purposes of the system. CCTV footage may be accessed for the following reasons:

- By the Residence Manager, or her nominated deputy, when a matter relating to unauthorised access through this entrance is suspected
- Following a request by An Garda Síochána when a crime, or suspected crime, has taken place and/or when it is suspected that illegal behaviour has taken place
- For data access requests by a data subject under the GDPR
- For Brosna's insurance company where the insurance company reasonably requests access in order to pursue a claim of theft from, and/or damage, to the residence or any of its occupants.

8.3 ACCESS REQUESTS BY DATA SUBJECTS

On written request, any person whose image has been recorded on CCTV has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording still exists (i.e. has not been deleted from the system) and provided also that an exemption/prohibition does not apply to the release e.g. in the case where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject will be informed in writing of the reasons for refusal.

Where the image/recording identifies one or more third parties, those images may only be released if they can be redacted and/or anonymised in such a way that the third parties cannot be identified.

To exercise their right of access, a data subject must make an application in writing to Brosna. Footage requested before normal deletion by the system will be retained for the purposes of the access request. A fee shall not be charged for responding to such a request, unless deemed necessary and reasonable based on administrative costs incurred. Brosna will provided the requested images within one month of receiving the access request. However, in the case of a complex access request e.g. requiring redaction and/or anonymization of the images, the time may be extended up to a maximum of three months.

Access requests should be made to by email, marked for the attention of Anne Brady, to office@brosna.ie or in writing to Anne Brady Brosna Educational Centres CLG, 6 Clare Street, Dublin 2, D02 EF82.

A data subject requesting access to personal data recorded by the CCTV system must provide all the necessary information to assist Brosna 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 will not be considered to be personal data and Brosna may elect not to provide it to the data subject requesting access. In giving a data subject a copy of his/her data, Brosna may provide a still or series of still images. However, images of other individuals will be obscured or redacted before the data is released. The relevant image or images will be provided on a disk or other suitable medium.

8.4 Provision of CCTV Images to An Garda Síochána

With respect to requests from An Garda Síochána for recorded footage, the Office of the Data Protection Commissioner recommends that requests for copies of CCTV footage be only granted to when a formal written (or fax) request is provided to the data controller stating that An Garda Síochána are investigating a criminal matter. For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request. A log of all such requests from An Garda Síochána requests will be maintained by Brosna as the data controller.

Note that there is a distinction between a request by An Garda Síochána to view CCTV footage and to request to download copies of CCTV footage. Requests to view footage onsite can be made verbally subject to identification being provided with no requirement for a written request.

9 Responsibilities

Glenard's Management Committee, acting on behalf of Brosna, will assume the following responsibilities:

- Ensure that the use of the CCTV system and the data that it generates is in accordance with this policy
- Oversee and manage the use of CCTV monitoring for safety and security purposes
- Ensure that the existing CCTV is evaluated for compliance with this policy at least annually
- Review the camera location and ensure that the release of any information and/or recorded CCTV materials is in full compliance with this policy

- Maintain an access control list (ACL) of all personnel who have physical or logical access to the CCTV system and the data that it generates including data that access was granted and revoked
- Maintain a record of all data subject access requests, related correspondence and release of footage
- Maintain a record of access to, or the release of, footage or any material recorded by, or stored in the system, to third parties

10 MAINTENANCE OF THE CCTV SYSTEM

From time to time the CCTV system will require maintenance by a security company. The security company has no remote access to the CCTV system and does not process the data but may have access to personal data in the event that on-site maintenance is required.

When maintaining the system, the security company will be required to have appropriate security measures in place to prevent the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The security company has been made aware of its obligations relating to the security of personal data on Glenard's CCTV system.

11 IMPLEMENTATION & REVIEW

The policy will be reviewed as required in light of any legislative or other relevant developments, and shall take into account updated guidelines from the Data Protection Commissioner and/or An Garda Síochána. In any case, this policy will be reviewed at least once every two years.

11.1 DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required at least in the following cases:

- a systematic and extensive evaluation of the personal aspects of an individual, including profiling;
- processing of sensitive data on a large scale;
- systematic monitoring of public areas on a large scale

After due consideration, Brosna has determined that a DPIA is not required for the Glenard CCTV System for the following reasons:

- there is very limited personal data in scope
- there is no sensitive personal data in scope
- processing of personal data is performed on a very limited scale

12 ENQUIRIES

Enquiries concerning Brosna's use of its CCTV system or the disclosure of CCTV images should be emailed to office@brosna.ie and marked for the attention of Anne Brady. Alternatively, enquiries may be submitted in writing and posted to Anne Brady, Brosna Educational Centres CLG, 6 Clare Street, Dublin 2, D02 EF82.

13 REFERENCES

[1] *Guidance on the Use of CCTV – For Data Controllers*, Data Protection Commission, October 2019. Available at https://www.dataprotection.ie/en/guidance-landing/guidance-use-cctv-data-controllers

APPENDIX A: DEFINITIONS

Access Request – A request by a data subject to as data controller for the disclosure of their personal data under Section 3 and / or Section 4 of the Data Protection Acts.

Audio recording – The use of equipment for recording of voice and sound.

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. It includes in this policy the recording of sound.

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).

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

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 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.

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. The Council 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 Subject – An individual who is the subject of personal data.

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.