



THE ROYAL BELFAST ACADEMICAL INSTITUTION

School CCTV Policy

Version	Date	Revision Author	Summary of Changes
2022.1	22.10.2022	JP	To reflect EANI sample policy June 2022

EXECUTIVE SUMMARY

At the Royal Belfast Academical Institution (the “School”), we believe privacy is important. We are committed to complying with our data protection obligations and to being concise, clear and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

This Policy is intended to reflect the school’s use of CCTV through following best practice advice from the Information Commissioner’s Office (ICO). We will review and update this CCTV Policy regularly in accordance with our data protection obligations.

Any queries in relation to this Policy or any of the matters referred to in it should be submitted to the Principal at prinsec@rbai.belfast.ni.sch.uk.

The following policies, procedures and documents are also relevant to this Policy:

- School Data Protection Policy
- Disposal of Records Schedule
- Privacy notices <http://rbai.org.uk/Page/Data-Protection/4891/Index.html>

1. Introduction

1.1 The Royal Belfast Academical Institution (“the School”) has in place CCTV surveillance. We use CCTV cameras to view and record individuals on and around our premises in order to maintain a safe environment for our pupils, staff and visitors. However, we recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with Data Protection Act 2018 and the UK GDPR.

1.2 CCTV systems are installed on the school premises; therefore this Policy applies to teaching staff, non-teaching staff, volunteers, pupils, parents/carers, contractors and other visitors to the school, including members of the public. All staff, pupils and visitors should have a reasonable expectation of being captured on CCTV on a daily basis.

1.3 The purpose of this Policy is to:

- a) set out why and how we will use CCTV, and how we will process data recorded by CCTV cameras
- b) ensure that the legal rights of data subjects, relating to their personal data, are recognised and respected
- c) assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence
- d) explain how to make a subject access request in respect of personal data created by CCTV.

2. Purpose of CCTV

2.1 The School has identified a need for CCTV. We have outlined below the reasons we use CCTV around our site:

- a) to protect pupils, staff and visitors by deterring, preventing and detecting wrongdoing/incidents
- b) to protect the school buildings and assets by deterring, preventing and detecting wrongdoing/incidents
- c) without prejudice, to protect the personal property of pupils, staff and visitors.
- d) to assist in managing pupil behaviour within the school

*This list is not exhaustive and other purposes may be or become relevant.

3. Who is Responsible for this Policy

- 3.1 For the purpose of the Data Protection Act 2018 and the UK GDPR, the School is the Data Controller of the CCTV surveillance system. The School's ICO Registration number is: Z4867008.
- 3.2 The School Board of Governors and Principal have overall responsibility for the effective operation of this policy. The Principal is the primary contact for the day-to-day application of this policy therefore any questions in relation to this policy should be referred to the Principal in the first instance.
- 3.3 This Policy will be reviewed by the Senior Leadership Team. The School will also review the ongoing use of existing CCTV cameras in the School, in line with the policy review schedule, to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction in line with all relevant ICO guidance and seek to comply with its best practice suggestions.
- 3.4 Any and all future changes to CCTV systems or the addition of CCTV systems (or other surveillance systems) will be subject to the completion of a satisfactory Data Protection Impact Assessment (DPIA).

4. CCTV System Overview

- 4.1 The School's CCTV system is capable of recording 24 hours per day, 7 days per week. Images will be recorded and retained on a rolling basis of approximately 30 days, unless the School is required by law to retain them and/or it is necessary for the school to retain any footage as part of the investigation of an incident. In the case of the latter the relevant footage will be stored securely until it is no longer required for the purpose for which it was retained. Otherwise, the CCTV System will automatically delete the images it records after approximately 30 days.
- 4.2 If a third party notifies the School that it intends to seek a court order for production of CCTV footage held by the school, the School will delete the footage after 12 months if it has not received a court order for production during that period (and will inform the relevant third party of its intention to do so).
- 4.3 The CCTV system monitors are located at the locations identified in Appendix 1. Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. CCTV cameras will only cover School buildings/premises (internal and external), car parks and public areas on the school site.
- 4.4 CCTV will not cover external public areas other than paths and roads immediately beside the school premises, which will be limited to the degree possible by positioning of cameras.

4.5 CCTV operating staff will be limited to a small number of individuals appointed by the Board of Governors, who will be required to be conversant with the School's CCTV Policy and Data Protection Policy when appointed. CCTV Operating Staff will also be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

4.6 In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure the Network based CCTV recorder on premises will be operated in a locked room with restricted access, and with password protection on the system to limit access to only approved personnel.

4.7 In order to inform people that they are under surveillance we will display clear CCTV signage appropriately around the School premises in the locations where CCTV cameras have been positioned. The signage will be easy to read, well-lit and positioned in places where they can be easily seen by individuals.

4.8 The School CCTV systems do not have audio recording.

5. Viewing and Disclosure of Footage

5.1 Access to CCTV images is restricted to those staff authorised to do so in accordance with the purposes of the system.

5.2 The individuals authorised to request and view CCTV material are:

- SLT
- Assistant Bursar
- House Masters
- Resident School Steward

More than one person must be present when viewing CCTV.

5.3 CCTV recordings will be viewed in a regulated area by the appointed personnel only, unless a member of SLT explicitly gives permission for another individual to be there, however their presence must be in relation to the content of the images e.g. to identify an individual.

5.4 Only the authorized persons listed in 5.2 can request that CCTV footage is viewed, to gather information relating to an allegation wrongdoing or an incident. The request for CCTV to be viewed should include:

- i. Date and time span during which the alleged wrongdoing/incident took place
- ii. Information to identify the individual, if necessary
- iii. Location of the camera, if known.

5.5 All occasions of CCTV footage being viewed must be logged. The Bursar will maintain the record. See Appendix 2.

5.6 Permission to copy footage must be given by the Principal or Bursar.

5.7 The School may receive requests for 'copies' of images captured on the CCTV system from individuals/external organisations. Such agencies must provide proof of legitimacy for their request showing, e.g a subject access request, or in response to a Court Order. All requests for disclosure to the PSNI must be on PSNI Form 81. The Principal will consider these requests in line with the purpose of the CCTV system and the Data Protection Act (1998). Where footage is being released, it must encrypted prior to release.

5.8 Any request for images by an individual data subject which relate to themselves or a third party acting on their behalf, i.e. "*Subject Access Requests*" should be made directly to the School using the form available at <http://rbai.org.uk/Page/Data-Protection/4891/Index.html>. Such requests will be processed in line with Data Protection Legislation. Identification and/or a sufficient 'form of authority' will be sought by the school upon receipt of such a request. Where images include third parties, the school may not be in a position to release the image/footage where doing so would place them in breach of Data Protection Legislation. Requests will be processed on a case by case basis and the 'right of access' granted when appropriate.

5.9 A register will be maintained of the release of CCTV footage to the police or other authorised applicants.

6. Complaints

6.1 Any complaint regarding the School's CCTV will be dealt with in line with the School's Complaints Policy.

6.2 You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The ICO's contact details are as follows:

The Information Commissioner's Office – Northern Ireland
3rd Floor
14 Cromac Place,
Belfast
BT7 2JB

Telephone: 0303 123 1114

Email: ni@ico.org.uk

Definitions

For the purposes of this policy, the following terms have the following meanings:

CCTV: means cameras designed to capture and record images of individuals and property.

Data: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data subjects: means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

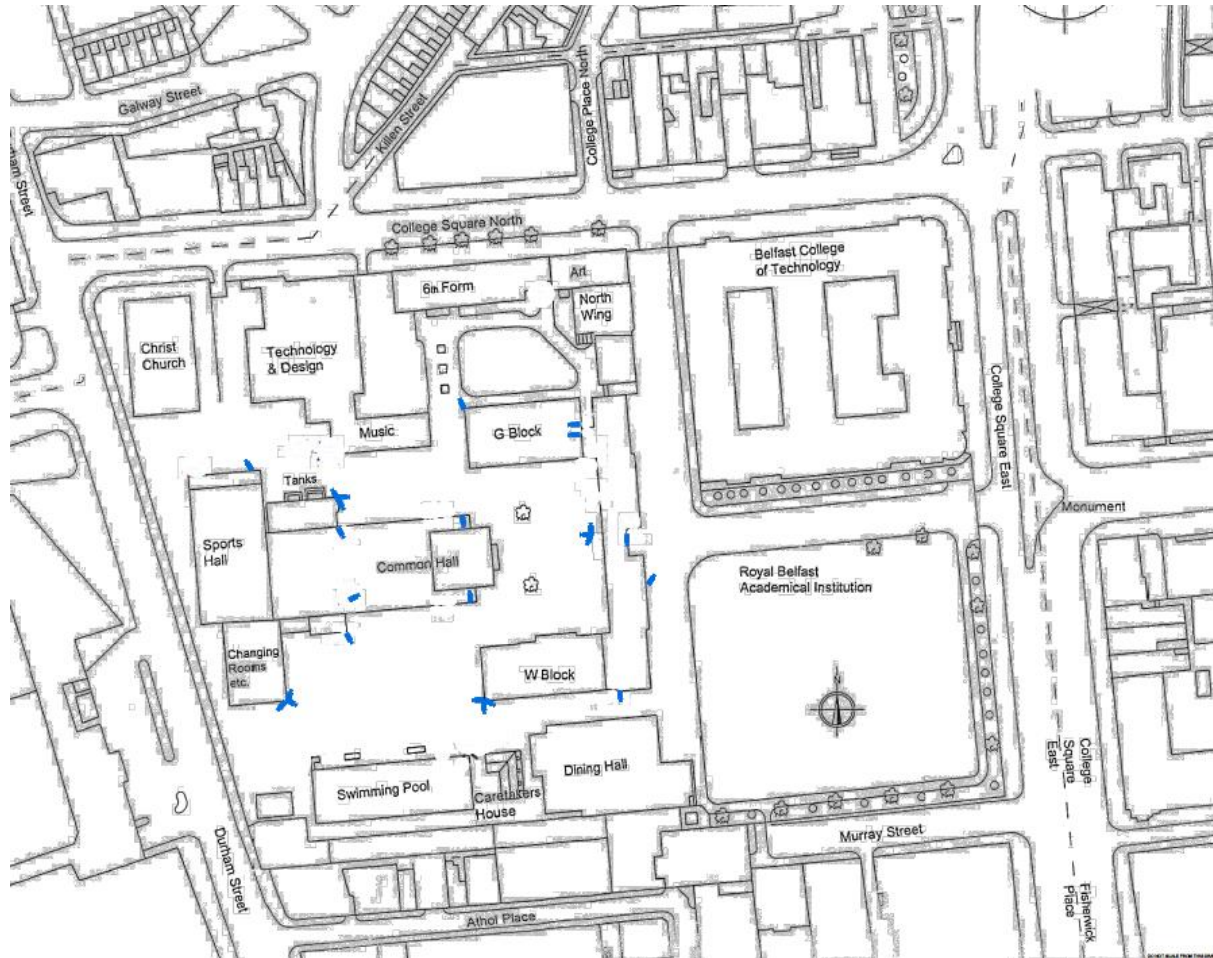
Data controllers: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law.

Data users: are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

Data processors: are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Processing: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.



Person 1 viewing Footage	Person 2 viewing Footage	Date footage viewed	Date and time span viewed during which the alleged wrongdoing/incident took place	Overview of wrongdoing/incident being investigated	Cameras viewed	Is a copy to be requested?