DEPARTMENT OF EDUCATION, SPORT AND CULTURE

RHEYNN YNSEE, SPOYRT AS CULTOOR

Isle of Man Government

Reiltys Ellan Vannin

CCTV

Policy for Schools and UCM

Glossary

CCTV means Closed-Circuit Television.

Commissioner means the Isle of Man Information Commissioner.

Data Protection Legislation for the purpose of this Policy includes:

- Data Protection Act 2018;
- Data Protection (Application of GDPR) Order 2018;
- Data Protection (Application of LED) Order 2018; and
- GDPR and LED Implementation Regulations 2018.

Department means the Department of Education, Sport and Culture (DESC) including schools, UCM, Villa Gaiety and MSR.

GDPR means the General Data Protection Regulation.

Schools means all primary and secondary schools which are maintained or provided for by the Department of Education, Sport and Culture, in accordance with Section 2(5) of the Education Act 2001, along with the Department's associated educational facilities, such as Thie Ny Shee.

Technical Guidance means the Commissioner's "*Surveillance cameras: guidance for controllers*".

UCM means University College Isle of Man.

Visitor means an individual who is visiting a School or UCM and is not employed to work there or is not a student there. A student who is suspended from School or UCM for misbehaviour may also be referred to as a Visitor.

Contents

Summary

About This Policy

This Policy outlines the way in which CCTV is to be used and managed on the premises of Schools and UCM, with the aim of ensuring that it is used for legitimate purposes and adhering to all relevant legislation, regulations and guidance.

Who is This Document For?

This guidance is for the leaders, staff and the Governing Bodies of all the schools maintained by DESC and the UCM.

It may also be referenced by parents, pupils and the wider public for information.

Key Points

The Island's Data Protection Legislations enacts the provisions from the GDPR which provides the legal framework for collecting and processing personal data, including the following principles:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability.

Effective Date

This document is effective from May 2024. It will be kept under review and updated at least every five years.

Policy

Purpose

CCTV systems are used by Schools and UCM to monitor their premises and contribute to a safe and secure environment for staff, pupils and visitors. The below is a non-exhaustive list of ways in which this is achieved:

- Protecting School and UCM assets, both during and after school hours, against theft or damage;
- Promoting the health and safety of staff, pupils and visitors;
- Safeguarding pupils;
- Monitoring student behaviour;
- Prevention of bullying;
- Detecting and identifying unauthorised persons;
- Reducing the incidence of crime and anti-social behaviour;
- Supporting the police to deter and detect crime;
- Assisting in identifying, apprehending and prosecuting offenders; and
- Assure that School and UCM rules are respected so that they can be properly managed.

Data Protection Legislation requires that the data gathered is "adequate, relevant and not excessive" for the purpose for which it is collected.

Scope

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

Where CCTV is installed within the boundaries of a School or UCM, it is the responsibility of the relevant Headteacher or Principal to justify the installation and usage of CCTV prior to its installation.

This can be achieved through consultation with the DPO and the completion of a Data Privacy Impact Assessment ("**DPIA**").

Given the different needs and circumstances of each School and UCM, each Headteacher and Principal should ensure that a relevant CCTV Usage Policy has been drafted in accordance with the requirements of their premises.

DPIA

The use of the CCTV system must be subject to a DPIA, performed by the Headteacher/Principal, or delegated to a senior member of staff, and signed-off by the DPO.

Where any changes are to be made to the CCTV system, including any updates or additional cameras, the DPIA must be updated and signed-off again by the DPO.

Location of Cameras

The location and usage of cameras will depend on the needs and requirements of each School and UCM.

When determining the location and position of cameras, Schools and UCM must have due regard for individuals' reasonable privacy expectations and only install cameras where they will capture images which are relevant to the purpose for which they are being installed.

Where cameras are installed externally, they must be positioned so that coverage does not include people's houses.

Best efforts must also be made to limit the coverage of public footpaths beyond the premises of the School or UCM; some overspill is acceptable, where it is necessary for meeting the purpose for which the CCTV was installed.

Private Areas

In the interests of safeguarding and protecting the reasonable privacy expectations of individuals, the Department's general position is to not allow the installation of CCTV cameras within changing rooms or toilet areas. However, where there is a belief that criminal conduct may be occurring in the changing rooms or toilets, they may install cameras in such a location so long as they can document and evidence their reasoning in a DPIA, and install appropriate signage to make it clear to users of the facilities that CCTV is in use.

When considering the use of CCTV in such locations, the Headteacher/Principal must consider the following guidance from the Information Commissioner:

"Cameras and listening devices should not be installed in private areas such as toilets and private offices, except in the most exceptional circumstances where serious crime is suspected. This should only happen where there is an intention to involve the police, not where it is a purely internal disciplinary matter."

Interaction with Other Equipment

A further consideration for the location and placement of CCTV is its potential interaction and/or interference with other equipment, e.g. lighting, emergency lighting, and health and safety signage.

Site Policy and Signage

Each School and UCM should produce their own CCTV Usage Policy and make this available upon request to staff, pupils, parents and visitors.

The Policy should be drafted in accordance with their premises and particular needs, and should provide:

- The purpose and location of CCTV cameras on the premises;
- Guidelines for use of the CCTV; and
- A contact for those wishing to discuss CCTV monitoring or access images/recordings.

Schools and UCM must display adequate signage at the entrance to the premises and at each camera location to indicate that CCTV is in operation. Where CCTV is either discreetly located or in a location where it would not ordinarily be located, extra effort should be made to ensure that the signage is visible (e.g. use larger signs or use multiple signs).

Signage must include the contact details of the Data Controller as well as the specific purpose(s) for which the CCTV camera has been installed in each location.

Templates can be found in Appendices 1 (CCTV Signage) and 3 (CCTV Usage Policy).

CCTV Media Storage

The images/recordings will be stored securely on a cloud network, with access being restricted to authorised personnel only.

A log of access to images/recordings must be maintained, and access to the log may be requested by the Department, internal audit, and/or the Information Commissioners, for review at any time.

CCTV Media Access

Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher/Principal, in conjunction with the Data Controller of the school at which CCTV is installed.

Images captured on any CCTV system are defined as sensitive personal data. The handling of such information must be in accordance with the relevant legislation.

The Headteacher/Principal may delegate the administration of the CCTV system to another senior staff member.

In relevant circumstances, CCTV images may be accessed:

- To assist the Headteacher/Principal in establishing facts in cases of unacceptable student behaviour, in which case, the parent(s)/guardian(s) will be informed;
- By the Isle of Man Constabulary who are required by law to make a report regarding the commission of a suspected crime;
- 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 school premises;

- To the Health and Safety at Work Inspectorate and/or any other statutory body charged with child safeguarding;
- 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 school;
- To individuals (or their legal representatives) subject to a court order; or
- To the school's insurance company where the insurance company requires evidence in order to pursue a claim for damage done to the insured property.

When CCTV images are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Subject Access Request (SAR)

Individuals have the right to request CCTV footage relating to themselves under the Data Protection Legislation.

If an individual wishes to submit a SAR, they must include the date, time and location of the images. A response will be issued within one month of receipt of a SAR.

Where access to CCTV footage would prejudice the legal rights of other individuals or would jeopardise an on-going investigation, such access may be refused or the images may be edited to protect the rights of the other individuals.

CCTV Image/Recording Retention

Unless required as evidence for an investigation, or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording or capture. At this point, images and recordings will be overwritten.

Where an image or recording is required to be held in excess of the 30 day retention period, the Headteacher/Principal or their nominated deputy will be responsible for authorising such a request.

Images held in excess of their retention period will be reviewed on a three monthly basis and deleted if not considered necessary for evidential purposes, or for responding to a SAR.

Purchasing CCTV Equipment

If a need for new or additional CCTV equipment is identified, the procurement must be undertaken, or facilitated, by Government Technology Services (GTS). This is required by FPN C.04 of the Financial Regulations, with the following objectives:

- Ensure value for money from ICT;
- Mitigate against risk to the corporate technology infrastructure; and
- Ensure effective planning within the Department and across the shared services.

Other Required Actions

In considering the installation or updating of CCTV equipment, the following will need to be progressed:

Department of Infrastructure – Estates

- Prior to the installation or moving of existing CCTV cameras, the school will liaise with DOI Estates to undertake a Risk Assessment Method Statement ("**RAMS**"). The RAMS assessment is designed to identify any risk or hazards associated with the installation, such as working conditions and building infrastructure, and is mandatory prior to the commencement of any work.

Government Technology Services ("GTS")

When considering the installation of CCTV, the following GTS Technology Code of Practice must be adhered to, in particular:

- CCTV: https://gtsportal.powerappsportals.com/technology-code-of-practice/technology-standards/cctv/
- Cabling: https://gtsportal.powerappsportals.com/Digital-Rulebook/technology-code-of-practice/technology-standards/network/cabling/
- Device Authentication: https://gtsportal.powerappsportals.com/Digital-Rulebook/technology-code-of-practice/technology-standards/network/device-authentication/

Current Sites

A list of DESC sites with CCTV in place can be found in Appendix 4.

Complaints

Complaints concerning the use of CCTV at a School or UCM, or the disclosure of CCTV images, should be made in accordance with the Department's Complaints Policy.

Version Control and Review

The business area that owns this document is **DESC DPO**.

Version	Author	Date	Changes
V0.1	Policy Hub	Sept 2023	First Draft
V0.2		February 2024	Amendments following consultation
V0.3	Policy Hub	April 2024	Final Draft submitted to SLT (Policy Hub Edit)
V0.3		29th April 2024	Final Draft approved by SLT
V1.0		May 2024	Version 1.0 published

Review Date

This document was issued in May 2024 and is due to be reviewed in May 2029.

Appendix 1 – CCTV Template

24 HOUR

CCTV

IN OPERATION

THESE IMAGES ARE BEING RECORDED FOR THE PURPOSE OF:

- **INSERT THE PURPOSES IDENTIFIED ON YOUR DPIA**

FOR FURTHER INFORMATION, PLEASE CONTACT THE SCHOOL:

- **INSERT SCHOOL CONTACT DETAILS**

Appendix 2 – DPIA Template

School/ Division/Team:	
Project Title:	
Lead/Contact Officer:	

Before you start, do you need a Privacy Impact Assessment? (PIA) – complete these pre-screening questions:

(These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

[You can expand on your answers as the project develops if you need to. You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess].

Questions:	**Yes / No**
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	
Will the project require you to contact individuals in ways that they may find intrusive?	

Data Privacy Impact Assessment

Step one: Identify the need for a DPIA

Explain what the project aims to achieve:	
Benefits to the organisation:	
Benefits to individuals:	
Benefits to other parties:	
Other relevant documents related to the project:	
Why the need for a PIA was identified:	

Step two: Describe the information flows

Collection:	
Use:	
Deletion	
Number affected: (anticipated)	
Flow diagram: *(Nb. A simple arrow/flow diagram is helpful, if possible)*	

Consultation requirements (*if applicable)

Practical steps to ensure that risks are identified:	
Practical steps to ensure that privacy risks are addressed:	
Internal consultation with:	
External consultation with:	
Consultation methodology *(link to the relevant stages of the project management process):*	
Dates of consultation	
Consultation 1:	
Consultation 2:	

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation / corporate risk**

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project?

What solutions need to be implemented?

Risk:	Approved solution:	Approved by (Headteacher/Principal or designate):

SIGN OFF

DESC DATA PROTECTION OFFICER

DPIAs should be signed, sent and retained by
> DPO-desc@gov.im <

Data Controller signature (Headteacher/Principal): _____ Date: _____

DPO-DESC signature: _____ Date: _____

SIRO signature: _____ Date: _____

Step six: Integrate the DPIA outcomes back into the project plan

(Who is responsible for integrating the DPIA outcomes back **into the project plan** and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?)

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns:
DESC - DPO

**Extra:*

Linking your DPIA to the GDPR privacy principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR/DPA or other relevant legislation, for example the Human Rights Act.

Principle 1
1. Lawfulness, fairness and transparency **Transparency: Tell the subject what data processing will be done.** **Fair: What is processed must match up with how it has been described** **Lawful: Processing must meet the tests described in GDPR** *[article 5, clause 1(a)]*
Have you identified the purpose of the project?
Yes
How will you tell individuals about the use of their personal data?
School's privacy notice
Do you need to amend your privacy notices?
Yes – to be specific and to highlight CCTV policy for school
Have you established which conditions for processing apply?
Public Task
If you are relying on consent to process personal data, how will this be collected, and what will you do if it is withheld or withdrawn?
N/A

Our organisation (CO) is subject to the Human Rights Act, please also consider:
• Will your actions interfere with the right to privacy under Article 8?
No
• Have you identified the social need and aims of the project?
Yes
• Are your actions a proportionate response to the social need?
Yes
Principle 2
2. Purpose limitations **Personal data can only be obtained for "specified, explicit and legitimate purposes"** *[article 5, clause 1(b)]***. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.**
Does your project plan cover all of the purposes for processing personal data?
Yes
Have you identified potential new purposes as the scope of the project expands?
N/A
Principle 3
3. Data minimisation **Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".** *[article 5, clause 1(c)]* *I.e. No more than the minimum amount of data should be kept for specific processing.*
Is the quality of the information good enough for the purposes it is used?
Yes
Which personal data could you not use, without compromising the needs of the project?
Images along with the position and time stamp will be produced
Principle 4
4. Accuracy **Data must be "accurate and where necessary kept up to date"** *[article 5, clause 1(d)]*

Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.
If you are procuring new software does it allow you to amend data when necessary?
N/A
How are you ensuring that personal data obtained from individuals or other organisations is accurate?
N/A
Principle 5
5. Storage limitations **Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary".** *[article 5, clause 1(e)]* *I.e. Data no longer required should be removed.*
What retention periods are suitable for the personal data you will be processing?
6 weeks unless images are required for other purposes – law enforcement
Are you procuring software that will allow you to delete information in line with your retention periods?
Yes, but the system will overwrite itself over a period
Principle 6
6. Integrity and confidentiality **Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage".** *[article 5, clause 1(f)]*
Do any new systems provide protection against the security risks you have identified?
Cameras should not be wireless but hardwired and the DVR should not normally connected to the internet
What training and instructions are necessary to ensure that staff know how to operate a new system securely?
As part of the installation training will be given on how to use the system.

Appendix 3 – CCTV Template for Schools

<<School Crest>>

CCTV Usage Policy

<<School>>

Version	Revision Author	Sections Changed	Sign-off By	Date
V1.0				xx/xx/2024

Glossary

For the purpose of this Policy, the following terms have the prescribed meanings:

CCTV means Closed-Circuit Television used to capture and record images of individuals and property.

Commissioner means the Isle of Man Information Commissioner.

Data Protection Legislation means:

- Data Protection Act 2018
- Data Protection (Application of GDPR) Order 2018;
- Data Protection (Application of LED) Order 2018; and
- GDPR and LED Implementing Regulations 2018

Data Protection Officer (DPO) means the Department of Education, Sport and Culture's Data Protection Officer.

Department means the Department of Education, Sport and Culture (DESC) including maintained and provided schools, UCM, Villa Gaiety and MSR.

GDPR means the General Data Protection Regulations.

Technical Guidance means the Commissioner's *"Surveillance cameras: guidance for controllers".*

Visitor means an individual who is visiting the school premises and is not employed to work there or is not a pupil there. A pupil who is suspended from the school for misbehavior may also be referred to as a Visitor.

1. Introduction

1.1. <<Name of School>> ("the School") has installed a CCTV system to record individuals on and around the School's premises in order to maintain a safe environment for our pupils, staff and visitors.

1.2. Images of individuals recorded by CCTV cameras are personal data and are processed in accordance with the Data Protection Legislation.

1.3. The purpose of this Policy is to provide:

- The purpose for having CCTV cameras on the premises;
- The locations of the CCTV cameras on the premises;
- Guidelines for the use of the CCTV system; and
- Contact details if you wish to discuss CCTV monitoring and/or access images/recordings.

2. Who is Responsible for this Policy

2.1. For the purpose of the Data Protection Legislation, the Department is the Data Controller of the CCTV system, with Registration Number: R001501

2.2. The Headteacher has overall responsibility for the effective operation of the CCTV system and the implementation of this Policy.

2.3. Any questions with regard to the day-to-day operation of the system should be directed to <<Insert role/name>> in the first instance.

2.4. This Policy, along with the use of the CCTV system, will be kept under review and amended as and when required, in accordance with the Data Protection Legislation and Technical Guidance.

3. Purpose of CCTV on the Premises

3.1. The school has identified the following reasons for installing the CCTV system on the premises: ***These purposes should reflect the purposes identified on your DPIA.***

-
-

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

4. Privacy Impact Assessments

4.1. The use of the CCTV system has been subject to a Privacy Impact Assessment, performed by <<Insert role/name>> and signed-off by the DPO.

4.2. Where any changes are to be made to the CCTV system, including any updates or additional cameras, the Privacy Impact Assessment will be updated and signed-off by the DPO.

5. Location of Cameras

5.1. Cameras will be sited in specific locations relevant to the purposes for which they are installed and in compliance with Data Protection Legislation and Technical Guidance.

5.2. CCTV coverage is restricted to areas that are relevant to meeting the purpose of monitoring. These areas will include:

- School buildings/premises (internal and external);
- Car parks and public areas on the school premises;
- Internal public areas, including corridors, foyers, and large rooms used for public gatherings.

5.3. Best efforts will be taken to avoid capturing public areas external to the school premises.

5.4. Due care is taken to uphold reasonable privacy expectations and it is the presumption that cameras will not be located in areas where individuals have such expectations, including:

- Offices;
- Meeting rooms;
- Classrooms;
- Changing rooms; and
- Toilets.

However, where there is reason to believe that criminal activity is taking place in these areas, the school may install CCTV cameras as a preventative measure against such behaviour.

6. CCTV System Overview

6.1. To meet the School's stated purpose, the CCTV system is capable of recording <<24 hours per day, 7 days a week>>.

6.2. Recorded images will only be accessed in response to a reported incident; they will not be accessed for monitoring purposes. Images will be retained for 30 days from the time of recording, unless the School is required otherwise by law and/or it is necessary for the school to retain recordings as part of an incident investigation. 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.

6.3. CCTV operating staff will be limited to a small number of individuals appointed by the <<Governing Body/Headteacher>>, who will be required to understand this 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.

6.4. 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.

6.5. In order to inform people that they are under surveillance, the school will display clear CCTV signage appropriately in the locations wherein CCTV cameras have been positioned.

6.6. The School CCTV systems audio recording will be disabled as this is may be considered intrusive and unnecessary in most circumstances and could thereby undermine support and confidence. Nor do the School CCTV systems have the ability for facial recognition.

7. Requests for Disclosure

7.1. To Individuals

7.1.1. 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, marked for the attention of the Headteacher. 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.

7.1.2. In order for the school to locate the relevant images, sufficient detail should be provided by the requester, such as date/location and time.

7.1.3. 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.

7.2. To Third Parties

7.2.1. CCTV footage will not be routinely shared with external agencies or bodies, whether statutory prosecution agencies, the judicial system, local government agencies, legal representatives, data subjects or other external bodies except upon receipt of a valid request. For example, it may be necessary for us to share recorded footage in limited circumstances such as where a law enforcement agency is investigating a crime. These images may be disclosed via viewing or by providing a copy of the images.

7.2.2. The School will consider all such requests in line with Data Protection Legislation and release images only where a relevant exemption to the Data Protection Legislation applies.

8. Complaints

8.1. Any complaint regarding the School's CCTV will be dealt with in line with the Department's Complaints Policy, which is available at:

https://www.gov.im/media/1381776/external-complaints-procedure-051023.pdf

8.2. You have the right to make a complaint at any time to the Information Commissioner, the Isle of Man's supervisory authority for data protection issues. The Commissioner's contact details are as follows:

The Information Commissioner
First Floor
Prospect House
Douglas
IM1 1ET

Tel: +44 1624 693260
Email: ask@inforights.im
Website: www.inforights.im

Appendix 4

DESC Sites with CCTV System in Place

Primary School Sites

- Anagh Coar School
- Ashley Hill Primary School
- Ballacottier School
- Ballasalla Primary School
- Bunscoill Rhumsaa
- Henry Bloom Noble
- Jurby Community Primary School
- Kewaigue School
- Manor Park Primary School
- Onchan Primary School
- Peel Clothworkers Primary School
- Scoill yn Jubilee
- St John's Primary School
- St Mary's RC School
- Willaston Primary School

Secondary School Sites

- Ballakermeen High School
- Castle Rushen High School
- Queen Elizabeth II High School
- St Ninian's Lower School
- St Ninian's Upper School

Other Sites

- Pre-School Assessment Centre
- Thie ny Shee
- UCM – Main Campus
- UCM – Thie Ushtey Campus
- UCM – William Kennish Campus
- National Sports Centre
- Villa Gaiety
- Rushen Youth Club
- Castletown Youth Club
- Café Laare