NORTH, WEST AND HEBRIDES
A TUATH, AN IAR IS INNSE GALL

CCTV Plan

Lead Officer (Post):	Head of Infrastructure
Responsible Office/ Department:	Infrastructure / Resources & Enterprise
Responsible Committee:	Audit and Risk Management
Review Officer (Post):	
Date plan approved:	08.12.25
Date plan last reviewed and updated:	NA
Date plan due for review:	08.12.27
Public face / College internal facing only:	Public face
Date of Equality Impact Assessment:	Not required

Table of Contents

CCTV Plan 1
Purpose 3
Scope 3
Lawful Basis and Principles 3
Roles and Responsibilities 3
Acceptable Use of the System 4
Access to Footage and Disclosure 4
Retention and Disposal 4
Security and Technical Controls 4
Related Policies 4
Review 5
Version Control and Change History 6

Purpose

This Plan sets out UHI North, West and Hebrides' (UHI NWH) approach to the operation and management of its CCTV systems.

The purpose of CCTV is to support the safety and security of staff, students, visitors and property; assist in the prevention and detection of crime; and support the investigation of incidents where proportionate and lawful.

The Plan applies to all locations where the organisation operates CCTV and to all staff with responsibilities relating to its use.

Scope

CCTV systems are in operation on the following campuses or centres:

- **Fort William campus**, Carmichael Way, Fort William, PH33 6FF
- **Stornoway campus**, Stornoway, Isle of Lewis, Outer Hebrides, HS2 0XR

Lawful Basis and Principles

CCTV systems process personal data. Their operation must comply with *UK GDPR*[1], the *Data Protection Act 2018*[2] and the *Data (Use and Access) Act 2025*[3]

UHI NWH processes CCTV footage primarily on the basis of legitimate interests, ensuring the use of surveillance is necessary, proportionate, and balanced against individuals' rights.

All processing of data follows the data protection principles, including lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, security and accountability.

Detailed requirements are set out in the *Data Protection Policy*.

Roles and Responsibilities

The **Head of Infrastructure** is nominated as the responsible person to oversee the operation of CCTV, ensure compliance with this Plan.

At each location authorised staff - as listed below - are granted delegated authority to access or retrieve footage, and only for a legitimate organisational purpose. All staff must follow existing *Information Security* and *Data Protection* policies when handling CCTV data.

- **Fort William campus**:
    - Engagement Lead Facilities Team Leader, Student Services Manager, Director of Enterprise & Engagement

[1] https://www.legislation.gov.uk/eur/2016/679/contents
[2] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[3] https://www.legislation.gov.uk/ukpga/2025/18/contents

- **Stornoway campus**:
  - Engagement Lead, Facilities Team Leader, Head of Student Services, Head of Infrastructure

Acceptable Use of the System

Cameras are installed in locations where there is a justified need for monitoring. They are not used for continuous monitoring of employees or students without clear justification and consultation.

CCTV is not used for any form of covert surveillance unless authorised under law and only in exceptional circumstances.

Signage is displayed to ensure individuals are aware of CCTV operation and the purpose of collection.

Access to Footage and Disclosure

Requests for CCTV footage are handled in accordance with the UHI NWH's data protection and information governance processes.

- Subject access requests are processed under the *Data Protection Policy*.
- Police or legal disclosures must follow the processes as established in the *UHI NWH Personal Data Disclosure Procedure* and be authorised by the designated person.
- Footage will only be disclosed where lawful, necessary and proportionate, and where doing so does not compromise the rights of others.

Retention and Disposal

CCTV recordings are retained only for the minimum period necessary to fulfil their purpose. Standard retention periods and disposal requirements are set out in the *University Partnership Retention and Disposal Policy*.

Footage required for an active investigation may be retained for longer where justified and documented.

Security and Technical Controls

All CCTV equipment and stored footage will be protected by appropriate technical and organisational measures. This includes secure system configuration, controlled access, password protection where appropriate, and regular review of system security.

Additional requirements are defined in the *Information Security Policy*.

Related Policies

This Plan is designed to be a concise statement of how UHI NWH manages its CCTV system. It should be read alongside the existing policies, which set out the wider regulatory, safeguarding,

information-governance and conduct requirements that apply to the use of CCTV and any personal data it captures. These include:

- *Data Protection Policy* – sets out our obligations under UK GDPR, including lawful bases for processing, individual rights, subject access requests and data minimisation.
- *Information Security Policy* – outlines the security controls, access restrictions and technical measures that also apply to CCTV equipment and stored footage.
- *University Partnership Retention and Disposal Policy* – defines the retention periods and disposal arrangements that apply to CCTV recordings.
- *UHI Freedom of Information* – explains how the organisation responds to FOI requests; CCTV footage will only be disclosed in accordance with that policy and applicable exemptions.

A full set of UHI NWH policies are available at www.nwh.uhi.ac.uk/en/about-us/policies-and-procedures. These existing policies remain authoritative. The CCTV Plan does not replace or override any other policy; instead, it works alongside them to ensure that the use of CCTV is proportionate, transparent, and compliant with all organisational and legal requirements

Review

This Plan will be reviewed at least every two years, or sooner if required by changes in legislation, technology or organisational policy.

Version Control and Change History

Version	Date	Approved by	Amendment(s)	Author
1				D Rattray