Assets and Infrastructure Policy
Subsidiary Policy & Procedure:

Surveillance cameras

Document Control			
Policy Manager:	Strategic Assets Manager	**Date First Approved:**	September 2007
Policy Owner:	Executive Director, Infrastructure & Assets	**Authorised by:**	Executive Director, Infrastructure & Assets
Category:	Operational	**Date Last Revised:**	July 2018
High-Level Policy:	Assets and Infrastructure	**Next Review Date:**	
Relates to NZQA Key Evaluation Question(s):		5. Governance & Management 6. Compliance	

Purpose & Scope

Surveillance cameras (sometimes referred to as CCTV or Closed-Circuit TV cameras) assist us in providing a safe and secure environment for our staff, students and visitors. They exist to help deter incidents of crime on our campuses, assist our management of assets, and provide our stakeholders with a greater sense of personal security.

This policy covers the purchase, placement and operation of all cameras, including the use of mobile, permanent and overt or covert cameras, and those installed for the purpose of investigating specific incidents. It also covers the storage of surveillance footage, and the use of footage in investigations and to respond to emergencies.

Through this subsidiary policy, we apply a consistent approach to the operation of our surveillance cameras to ensure all equipment is compatible, used correctly, and that we are compliant with our legal obligations. This subsidiary policy is part of the Assets and Infrastructure Policy (TBD).

1. Policy Statement

Wintec seeks to provide a safe and secure environment for all students, staff and other stakeholders; along with protecting our assets and other resources.

1.1. Promote the existence of, and awareness behind Wintec's use of surveillance cameras

We utilise surveillance cameras for both prevention and investigation of crime. They form one part of our security infrastructure and are an important part of campus and incident management. Our use of cameras is signposted at key locations around our campuses.

1.2. Actively manage the use of surveillance cameras

We ensure consistent application of high standards in all aspects of management, purchasing, placement and operation of all camera technology, including the storage of surveillance footage.

1.3. Ensure the ethical use of surveillance cameras on campus

Surveillance cameras

We realise that cameras can be perceived as invasive, so we have controls in place to ensure our cameras and the images they capture are used in an ethical and appropriate manner.

1.4. Ensure we are compliant with the Privacy Act 1993

We take our obligations under the Privacy Act 1993 seriously. The privacy of individuals is not impinged at any time, in line with the Privacy Act Principles and provisions

2. Key Roles & Expectations

This subsidiary policy is managed by Strategic Assets Manager, and owned by the Executive Director, Infrastructure & Assets. While Facilities Management maintain additional guidelines and standards, all stakeholders are to be aware of their obligations.

The following roles have responsibilities and expectations:

Students	• be aware of Wintec's surveillance cameras, including mobile cameras • be aware of their rights with regards to privacy • take all reasonable steps to ensure compliance with this subsidiary policy where applicable • report to Wintec security any suspicious behaviour on campus, or any damage to Wintec's surveillance cameras.
All Staff	• be aware of Wintec's surveillance cameras, including mobile cameras • be aware of their rights with regards to privacy • take all reasonable steps to ensure compliance with this subsidiary policy where applicable • report to Wintec security any suspicious behaviour on campus, or any damage to Wintec's surveillance cameras.
Security Services Coordinator	• responsible for the day-to-day management of this policy • consulted with regarding the purchase and installation of all new surveillance cameras • prepare investigations that use surveillance footage/data • seek written approval for the use of covert surveillance cameras from the Strategic Assets Manager • directly supervise the use of covert surveillance cameras • responsible for the safe and secure storage of all surveillance camera footage/data • be the first point of contact for any requests to use or view saved recordings • determine who the relevant parties are in any investigation or when responding to any request to view saved recordings and approve or decline requests accordingly • be present during any viewing of a saved recording by a relevant party or approved representative • maintain a log of all requests for access to saved recordings, and the outcome of each request.
Strategic Assets Manager	• as the Policy Manager, holds responsibility for the implementation of this policy • can approve the use of covert surveillance cameras

	• can be present during any viewing of a saved recording by a relevant party or approved representative • organises the release of any privacy notices and public information releases with regards to the location and use of surveillance cameras at Wintec • promotes awareness of this policy and best practice amongst Wintec staff and students.
Relevant Parties/ Approved Representatives	• parties deemed relevant either by the Security Services Coordinator, or in accordance with New Zealand Laws and Regulations • parties must submit any request to view or obtain footage in writing to the Security Services Coordinator.
Privacy Officer	• investigates any privacy related breaches or complaints in relation to this policy • creates awareness of and monitors compliance with New Zealand's current privacy law, specifically the Privacy Act 1993, and is aware of the potential implications of the Privacy Bill (proposed law), currently before parliament.
Executive Director, Infrastructure & Assets	• as Policy Owner, holds overall responsibility for the implementation of this policy.

3. Measuring Success

The measurements of successful implementation of this policy at Wintec are:

- All students and staff are aware of our surveillance camera subsidiary policy and the intent behind the network of cameras at Wintec.
- The privacy of individuals is not imposed upon at any time, in line with the provisions of the Privacy Act 1993.
- The safety and security for all campus users is maintained, and Wintec campuses are perceived as safe places to work and study.
- Annual review of surveillance cameras is undertaken to determine its effectiveness and viability.
- Annual audit of surveillance technology to ensure it continues to operate smoothly.
- When required, our surveillance cameras are used to support and/or investigate specific investigations/incidents.

4. Supporting Information

4.1. Overt vs Covert Surveillance Cameras

Surveillance cameras serve three main purposes at Wintec: crime prevention; campus and incident management; and incident investigation. While the majority of our cameras are clearly visible, (overt), there are instances where we can chose to use surveillance cameras that are not. These are known as covert surveillance cameras.

Both overt and covert cameras and related surveillance systems can only be purchased and installed in consultation with the Security Services Coordinator and with written authorisation from either the Strategic Assets Manager or Executive Director, Infrastructure & Assets.

4.2. Overt Surveillance Cameras

Cameras which are visible. In addition:

- Signs are located at the entrance gates advising campus users that they are entering an area where they may be under surveillance.
- Signs are located in buildings where overt cameras are located, advising that surveillance cameras are in operation.

4.3. Covert Surveillance Cameras

Cameras which are concealed or disguised as other objects. These cameras are must be:

- Used only for the investigation of a specific incident or series of incidents, offence(s) or event(s).
- Used only under the direct supervision of the Security Services Coordinator. The Security Services Coordinator must record in writing the reason for the investigation and use of covert cameras, a copy of which is sent to the Strategic Assets Manager.
- Limited to surveillance required for the needs of the investigation.

4.4. Both Overt and Covert Cameras

In addition to their specific requirements and uses, both types of cameras must also:

- Not be installed or operated in any location that would be considered intrusive, or an invasion of privacy where people are likely to expect privacy. This includes:
  - Toilets and bathrooms
  - Changing rooms
  - Exterior entrances to health clinics.
- Overt cameras and related surveillance systems are purchased and installed only in consultation with the Security Team Leader with written authorisation from either the Facilities Operations Team Leader or the Strategic Assets Manager.

4.5. Saved Recordings

The footage or data (the recordings) are stored in a password protected secure state and protected from unauthorised access, use, modification and disclosure. Recordings are accessible only to authorised Wintec staff. Unless required for evidential purposes, recordings are to remain on NVR or DVR format until deleted by the system. When they are deleted is determined by the storage space available.

5. Procedures

5.1. Accessing Saved Recordings

Saved recordings may be viewed, only by Relevant Parties, and then only in the presence of one of the following: The Security Services Coordinator, Strategic Assets Manager, Facilities Operations Team Leader, Executive Director Infrastructure & Assets, or Wintec's Privacy Officer; on a strictly confidential basis.

All requests to view saved footage must be made in writing to:

Security Services Coordinator
C/o- Infrastructure and Assets
Wintec
Private Bag 3036
Waikato Mail Centre
Hamilton 3240

Note: Postage is free in New Zealand if you write Freepost 566 on the envelope.

Subject to this policy, the contents of recordings can be shared with Relevant Parties or Approved Representatives in order to progress an investigation.

5.2. Making a Complaint

Complaints relating to decisions made by Wintec's Security Team Leader with regards to accessing footage by students or staff should be made via Wintec's existing complaints processes. See *Section 7. Related Legislation, Regulations, Policies, Guidelines and Forms* for more information.

Where a breach of privacy is believed to have occurred, should be directed in writing, in the first instance to Wintec's Privacy Officer:

Wintec Privacy Officer
C/o- Infrastructure and Assets
Wintec
Private Bag 3036
Waikato Mail Centre
Hamilton 3240

Note: Postage is free in New Zealand if you write Freepost 566 on the envelope.

6. Related Legislation, Regulations, Policies, Guidelines, and Forms

Legislation/Regulations	Policies	Guidelines/Forms
Privacy Act 1993 Privacy Act Principles Public Records Act 2005	Privacy and Personal Information Policy Safety and Wellbeing Policy Asset Management Policy Student Concerns, Complaints and Appeals Policy Child Protection Policy General Formal Complaints and Appeals Policy Discipline Regulations for Students Employee Complaint Management Policy Staff Discipline Policy	Privacy Commissioner: Privacy and CCTV Guide Request of CCTV Footage Checklist (TBD)
Copies of New Zealand Legislation can be found on the New Zealand Legislation Website. You can view Wintec's Policies and Procedures on the Policy Web. This is not an exhaustive list of policies, procedures and legislation.		

7. Key Definitions & Glossary

Approved Representatives	Approved Representatives are those public sector and government agencies (such as the New Zealand Police) who are directly related to the purpose of an investigation (such as investigating a crime) whether by Wintec or one of those agencies, for the purpose of upholding the law (e.g. prosecuting offences). Also includes Wintec staff that have been authorised to access footage. These are strictly limited to the Security Services Coordinator, the Strategic Assets Manager, the Facilities Operations Team Leader, Executive Director Infrastructure & Assets, and the Privacy Officer.
CCTV	Closed-Circuit TV. This is a somewhat outdated term due to changes in technology, but is often used to describe surveillance camera systems/networks. In this context it means any camera employed for security/crime prevention purposes that captures images of individuals.

Surveillance cameras

Covert	Refers to any surveillance cameras that are not signposted and used specifically for an open investigation. They are only used for specific incidents. May be disguised as other objects.
DVR	File format used to store footage/data/recordings made from surveillance cameras.
Incident	Any action by a person or persons which is illegal under New Zealand laws or statutes and/or has caused, or could cause, harm to any person on a Wintec site/campus, or damage to any Wintec asset.
Mobile Cameras	Mobile cameras include cell phones with cameras, body cameras, Go Pro devices and similar technology, other emerging and mobile device capable of capturing and recording still and/or moving images.
Network	In this context, network refers to the systems used to store recordings or data taken from surveillance cameras.
NVR	File format used to store footage/data/recordings made from surveillance cameras.
Overt	Refers to any surveillance cameras that are visible and signposted.
Public Spaces	Refers to any spaces that are completely accessible to the public such as streets, footpaths and public paths which are not directly owned or under the control of Wintec.
Relevant Parties	Relevant Parties are determined by the Security Services Coordinator, and are those considered under the principle of having “essential involvement” in an investigation, to prevent unauthorised disclosure. That is, as few people as is reasonably practical in the circumstances should be able to view any saved recordings/footage/data.
Semi-public Spaces	Refers to any spaces that are accessible to the public during normal operating hours at Wintec. This includes shops and businesses that may operate on Wintec grounds.

Surveillance cameras

8. Records Management

In line with the Public Records Act 2005, Wintec is required to provide an Information and Records Management programme to ensure that authentic, reliable and usable records are created, captured and managed to a standard of best practice, and to meet business and legislative requirements. All records relevant to a specific policy need to be listed in every policy in the following format:

Record	Minimum retention period	Disposal Action	GDA Reference #
Native Avigilon format – Suitable for legal and evidential purposes (non-editable)	Until no longer administratively required	Destroy	3.8.1
MP4 format – Suitable for multi-platform viewing (Not suitable for evidential purposes)	Until no longer administratively required	Destroy	3.8.1
JPEG format – Still image format (single frame capture)	Until no longer administratively required	Destroy	3.8.1
Request of CCTV Footage Checklist	Until no longer administratively required	Destroy	3.8.1

9. Version History

Version	Date Approved	Details
1	September 2007	First Published.
2	July 2014	Split into Parts A and B.
3	June 2017	Updated template to subsidiary policy template, combining Parts A and B into one document. Added Key Roles and Expectations, Measuring Success and Supporting Information sections. Added procedures on accessing saved recordings and making a complaint. Updated Purpose & Scope, Policy Statement, Related Legislation and Glossary sections. Removed minimum retention period for recordings.