Register of Approved Surveillance Activities

TABLE 1: Use and disclosure of surveillance information

Surveillance activities and the use or disclosure of surveillance information may only be carried out when reasonably proportionate taking into consideration the proposed purpose and the privacy impacts on individuals.

	Type of surveillance	Surveillance information	Personnel approved to carry out the surveillance	Personnel approved to use and disclose the surveillance information	Approved uses and disclosures of surveillance information
1	Optical surveillance (video or photographic)	Recordings (including live footage, still images and associated audio) from land-based fixed, mobile, or wearable University cameras (including body-worn cameras, cameras in University patrol vehicles, and mobile device cameras)	University security staff or security contractors	• University security staff or security contractors • University staff or contractors who monitor live feeds in the course of their role	1. Use of recordings to: (a) (**health and safety**) respond to or prevent actual or potential public safety incidents including those that may affect the health, safety and welfare of University staff, students and other individuals attending University premises, using University facilities, or engaging in University activities; (b) (**property and facilities protection**) protect University property or facilities, or other people's property on University premises, from actual or potential unauthorised access, use, damage, destruction, theft or trespass; (c) (**public order**) maintain or enforce compliance with University rules, policies or conditions of entry, access or use relating to University premises or facilities; or (d) (**investigations**) conduct or assist in investigation of incidents relating to (a)–(c) above.
				University staff or contractors in the course of their role in the following teams: • Workplace Relations; • Human Resources; • Enterprise Technology; • Health and Safety; • Academic Registrar and Student and Scholarly Services; • Physical Security; and • Office of Research Ethics and Integrity.	2. Use of recordings to: (a) (**health and safety**) protect the health, safety and welfare of University staff, students and other individuals attending University premises, using University facilities or engaging in University activities; (b) (**property and facilities protection**) protect University property or facilities from actual or potential unauthorised access, use, damage, destruction, theft or trespass; (c) (**research integrity**) identify, investigate and manage potential breaches of the Australian Code for the Responsible Conduct of Research or the Responsible Conduct of Research Policy (MPF1318); (d) (**biosecurity**) protect against, identify and investigate biosecurity threats in University research activities; (e) (**academic misconduct**) identify, investigate, or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential academic misconduct; (f) (**special consideration**) inform and support decisions relating to granting special consideration for assessments; (g) (**staff misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential staff misconduct;

Consultation Draft

	Type of surveillance	Surveillance information	Personnel approved to carry out the surveillance	Personnel approved to use and disclose the surveillance information	Approved uses and disclosures of surveillance information
					(h) (**student general misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential student general misconduct; or (i) (**investigations**) identify, assess and investigate potential breaches of University regulations, rules or policies not covered above, and take appropriate action.
2	Audio surveillance	Audio recordings (including a saved or downloaded transcript or captions record of that recording) from the University's Security Control Room, Emergency Operations Centre, or help phones or intercoms on University premises	University security staff or security contractors	University security staff or security contractors	1. Use of audio recordings to: (a) (**health and safety**) respond to or prevent actual or potential public safety incidents including those that may affect the health, safety and welfare of University staff, students and other individuals attending University premises, using University facilities, or engaging in University activities; or (b) (**training and quality assurance**) support training of University security staff or security contractors, and facilitate quality assurance activities relating to University security safety systems.
3	Tracking surveillance	GPS or location tracking data from University vehicles or equipment	• University security staff or security contractors • University staff or contractors in Client Services who manage University vehicles in the course of their role	• University security staff or security contractors • University staff or contractors in Client Services who manage University vehicles in the course of their role	1. Use of GPS or location tracking data to: (a) (**property and facilities protection**) protect University property or facilities, or other people's property on University premises, from actual or potential unauthorised access, use, damage, destruction, theft or trespass.
			University staff or contractors in Client Services who manage University vehicles in the course of their role	University staff or contractors in the course of their role in the following teams: • Client Services who manage University vehicles in the course of their role; • Workplace Relations; and • Human Resources.	2. Use of GPS or location tracking data to: (a) (**staff misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential staff misconduct.
4	Data surveillance	Data from video content analytics software that is limited to accelerated object identification Note: 'object identification' includes vehicles, building or environmental features, equipment, artworks or signs, animals, articles of clothing or bags, or prohibited items (such as weapons) that can be identified algorithmically using patterns or descriptors like shape, colour, or texture. 'Object identification' does not include facial recognition, bodily recognition (such as tattoos or other bodily characteristics), or behavioural analysis of individuals.	University security staff or security contractors	University security staff or security contractors	1. Use of data from video content analytics software (limited to accelerated object identification) to: (a) (**health and safety**) respond to or prevent actual or potential public safety incidents including those that may affect the health, safety and welfare of University staff, students and other individuals attending University premises, using University facilities, or engaging in University activities; (b) (**property and facilities protection**) protect University property or facilities, or other people's property on University premises, from actual or potential unauthorised access, use, damage, destruction, theft or trespass; or (c) (**investigations**) conduct or assist in investigation of incidents relating to (a)–(b) above.

Consultation Draft

Table 2: Use and disclosure of information incidentally collected (see section 2.2(e) of Surveillance Policy)

The use or disclosure of information may only be carried out when reasonably proportionate taking into consideration the proposed purpose and the privacy impacts on individuals.				
	Activity	**Information**	**Personnel approved to use and disclose information**	**Approved uses and disclosures**
1	Video recording	• Recording of an online meeting • Recording of a teaching activity • Recording of an assessment activity • Recording of an interview • Recording of a public lecture • Still images of video recordings	University staff or contractors in the course of their role in the following teams: • Workplace Relations; • Human Resources; • Enterprise Technology; • Health and Safety; • Academic Registrar and Student and Scholarly Services; • Physical Security; and • Office of Research Ethics and Integrity.	1. Use of video recordings to: (a) (**health and safety**) protect the health, safety and welfare of University staff, students and other individuals attending University premises, using University facilities or engaging in University activities; (b) (**property and facilities protection**) protect University property or facilities from actual or potential unauthorised access, use, damage, destruction, theft or trespass; (c) (**research integrity**) identify, investigate and manage potential breaches of the Australian Code for the Responsible Conduct of Research or the Responsible Conduct of Research Policy (MPF1318); (d) (**biosecurity**) protect against, identify and investigate biosecurity threats in University research activities; (e) (**academic misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential academic misconduct; (f) (**special consideration**) inform and support decisions relating to granting special consideration for assessments; (g) (**staff misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential staff misconduct; (h) (**student general misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential student general misconduct; or (i) (**investigations**) identify, assess and investigate potential breaches of University regulations, rules or policies not covered above, and take appropriate action.
2	Audio recording	• Audio recording of an online meeting • Audio recording of a teaching activity • Audio recording of an assessment activity • Audio recording of an interview • Audio recording of a public lecture	University staff or contractors in the course of their role in the following teams: • Workplace Relations; • Human Resources; • Enterprise Technology; • Academic Registrar and Student and Scholarly Services; • Health and Safety; and • Office of Research Ethics and Integrity.	1. Use of audio recordings to: (a) (**health and safety**) protect the health, safety and welfare of University staff, students and other individuals attending University premises, using University facilities, or engaging in University activities; (b) (**research integrity**) identify, investigate and manage potential breaches of the Australian Code for the Responsible Conduct of Research or the Responsible Conduct of Research Policy (MPF1318); (c) (**biosecurity**) protect against, identify and investigate biosecurity threats in University research activities; (d) (**academic misconduct**) identify, investigate or respond to behaviours or incidents (including but not limited to potential non-compliance with University rules or policies) where there is a reasonable suspicion of actual or potential academic misconduct; (e) (**special consideration**) inform and support decisions relating to granting special consideration for assessments;

Consultation Draft

	Activity	Information	Personnel approved to use and disclose information	Approved uses and disclosures
				(f) (**staff misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential staff misconduct; or (g) (**student general misconduct**) identify, investigate or respond to behaviours or incidents where there is a reasonable suspicion of actual or potential student general misconduct.
3	Building or facilities access controls	Personally identifiable building or facilities access data (for example, from staff or student ID cards)	University staff or contractors in the course of their role in the following teams: • Physical Security; • Enterprise Technology; • Academic Registrar and Student and Scholarly Services; • Health and Safety; and • Office of Research Ethics and Integrity.	1. Use of personally identifiable building or facilities access data to: (a) (**health and safety**) protect the health, safety and welfare of University staff, students and other individuals attending University premises, using University facilities, or engaging in University activities; (b) (**property protection**) protect University property or facilities, or other people's property on University premises, from unauthorised access, use, damage, destruction, theft or trespass; (c) (**biosecurity**) protect against, identify and investigate biosecurity threats in University research activities; or (d) (**compliance management**) maintain, investigate, or enforce compliance with University conditions of entry, access, or use relating to University premises or facilities.

Guidelines
1. Approved use of information in this register includes providing that information to another member of University staff for appropriate management action. 2. Types of surveillance information may be used in conjunction with other types of data or information, provided that use or disclosure is for an approved purpose and consistent with the Surveillance Policy and this register. Examples include: (a) Use of video recordings in conjunction with personally identifiable building or facilities access data and/or University computing and network facilities data to: (i) determine the location of an individual or their device for the purpose of investigating unauthorised access to University facilities, where doing so is reasonably proportionate taking into consideration the proposed purpose and potential privacy impacts on the individual; or (ii) validate or verify an individual's identity for the purpose of investigating potential misconduct in circumstances where it is reasonably proportionate taking into consideration the proposed purpose and potential privacy impacts on the individual.

Last updated: [insert date]

Consultation Draft