Surveillance Policy

1. Objectives

The objectives of this policy are to:

(a) ensure transparency in the University's surveillance activities;

(b) set out clear protocols for assessing any new surveillance activities or any material change to existing surveillance activities;

(c) set out approval processes for the use or disclosure of surveillance information; and

(d) clarify the roles and responsibilities for the assessment and approval of surveillance activities.

2. Scope

2.1 Scope

This policy applies to surveillance of University staff, contractors, students, honorary appointees, volunteers, or others attending University premises, using University assets or University computing and network facilities, or engaging in University activities.

2.2 Exclusions

This policy does not apply to activities (including the use or disclosure of information obtained in the course of those activities) that:

(a) are undertaken to protect or ensure the integrity, security, availability and service delivery of University computing and network facilities;

(b) are required to be undertaken by law, a government agency or a regulator, or are undertaken to provide assistance to a law enforcement agency where reasonably necessary;

(c) are undertaken to protect the University or Australia from foreign interference in line with the *Guidelines to Counter Foreign Interference in the Australian University Sector* released by the University Foreign Interference Taskforce;

(d) are undertaken to detect or respond to suspected breaches of contract (except for employment contracts);

(e) involve the collection of personal information incidentally when using University computing and network facilities or other technologies for non-surveillance activities, for example:

(i) use of video or audio technology for teaching, assessments, public lectures or recording of meetings;

(ii) use of data to evaluate and improve University programs;

(iii) use of data to assist with staff development;

(iv) use of data to monitor course attendance and progress, including provision of wellbeing or academic support to students;

(v) use of data to manage and maintain academic integrity and quality in examinations and assessments,

except if that personal information is or will be used to investigate or respond to a reasonable suspicion of actual or potential breach of University regulations, rules or polices, in which case it will be treated as surveillance information for the purpose of this policy;

(f) involve de-identified or anonymous data, except if that data is re-identified or will be matched with other data or information (for example, to identify or make inferences about an individual) and that data is then used to investigate or respond to a reasonable suspicion of actual or potential breach of University regulations, rules or polices, in which case it will be treated as surveillance information for the purpose of this policy;

(g) are undertaken by or on behalf of the University when managing a claim in its capacity as a self-insurer under the *Workplace Injury Rehabilitation and Compensation Act 2013* (Vic) or *Accident Compensation Act 1985* (Vic);

(h) are undertaken for legitimate University business continuity purposes;

(i) are undertaken to protect or ensure the integrity of University financial transactions and the use of University resources, in accordance with financial oversight protocols and internal control standards;

(j) are undertaken as part of the University's internal audit function and in accordance with the University's Internal Audit Charter; or

(k) are undertaken as part of a research project that is approved and conducted in compliance with a University research policy.

3. Authority

This policy is made under the *University of Melbourne Act 2009* (Vic) and the Vice-Chancellor Regulation and supports compliance with:

(a) *Charter of Human Rights and Responsibilities Act 2006* (Vic);

(b) *Health Records Act 2001* (Vic);

(c) *Privacy and Data Protection Act 2014* (Vic);

(d) *Public Records Act 1973* (Vic); and

(e) *Surveillance Devices Act 1999* (Vic).

4. Policy

4.1 Conducting surveillance

Surveillance must be conducted in accordance with this policy.

4.2 Surveillance activities

The University may engage in the following types of surveillance:

(a) **audio surveillance:** surveillance using any device that can record a conversation or words spoken between people;

(b) **optical surveillance:** surveillance using a fixed, portable, or remote controlled camera. Some camera surveillance may also include audio surveillance (if the camera can receive or record sounds);

(c) **data surveillance:** surveillance using University computing and network facilities that monitor or record the information (data) input or output, or monitor how a computer or

network is being used (for example, monitoring access to and use of restricted premises, networks or facilities, network data, emails, and websites visited). Some data surveillance may also include audio or optical surveillance (if the device includes a camera or microphone that is approved for use for a surveillance activity); and

(d) **tracking surveillance:** surveillance using an electronic device, where the primary purpose of the device is to determine the geographical location of an object (such as a GPS tracking device installed in a vehicle or portable asset).

4.3 Approvals for surveillance activities, and uses or disclosures of surveillance information

(a) **Approved surveillance activities:** Surveillance activities approved by the University will be maintained in a 'Register of Approved Surveillance Activities'. Surveillance information obtained from those approved surveillance activities can be used and/or disclosed consistent with that register.

(a) **Additional surveillance methods:** The use of any new type of device for surveillance activities, implementation of a new method of surveillance, or a material change to the way in which an existing device or method is used to pursue a surveillance activity must be approved under section 5.2 of this policy.

(b) **Additional uses or disclosures of surveillance information:** The use or disclosure of surveillance information outside those uses and disclosures described in the Register of Approved Surveillance Activities must be approved under section 5.4 of this policy.

5. Procedural principles

5.1 Request for approval of surveillance activity

(a) A request to use any new type of device for surveillance activities, or implement a new method of surveillance, or make a material change to the way in which an existing device or method is used to pursue a surveillance activity must include:

(i) details of the proposed surveillance activity;

(ii) where, when and how the proposed surveillance activity will be carried out, and whether it will be continuous or intermittent;

(iii) the intended purpose of the proposed surveillance activity, which must be a legitimate University purpose;

(iv) whether the proposed surveillance activity is reasonably proportionate taking into consideration its proposed purpose and the privacy impacts on individuals;

(v) how any new surveillance information will be managed, including the intended uses and disclosures of the resulting surveillance information; and

(vi) how affected individuals will be notified about the proposed surveillance activity.

5.2 Approval of surveillance activity

(a) Approval of a request for a proposed surveillance activity under this section may only be granted by any two of the following University staff, one of whom must be a member of the Vice-Chancellor Advisory Group (VCAG), and neither of whom may also be person making the request.

(i) Chief Information Officer;

(ii) Executive Director, Enterprise Performance Group;

(iii) Vice-President (Administration & Finance) and Chief Operating Officer;

(iv) Deputy Vice Chancellor (Education) for academic-related purposes only;

(v) Deputy Vice Chancellor (Research) for research-related purposes only;

(vi) Provost;

(vii) Vice-Chancellor.

(b) An approver must not approve a request under this section unless they are reasonably satisfied that:

(i) the proposed surveillance activity:

(A) is appropriate, having regard to the legitimate purposes of the University;

(B) is reasonably proportionate taking into consideration its proposed purpose and the privacy impacts on individuals;

(C) does not discriminate on the basis of a protected attribute; and

(D) is consistent with the University's obligations under the *Surveillance Devices Act 1999* (Vic);

(ii) a Privacy Impact Assessment has been completed for the proposed surveillance activity where required by the Privacy Policy (MPF1104);

(iii) relevant human rights have been properly considered; and

(iv) appropriate collection notices and operational procedures are, or will be, in place for the surveillance activity.

(c) An approver may impose conditions or limitations on their approval under this section.

5.3 **Request for approval to use or disclose surveillance information**

(a) A request to use or disclose surveillance information must include:

(i) a description of the surveillance information requested;

(ii) whether the proposed use or disclosure of the surveillance information will be ongoing or time limited;

(iii) the intended use or disclosure of the surveillance information, which must be for a legitimate University purpose;

(iv) how affected individuals were notified about the use or disclosure of the surveillance information;

(v) whether the proposed use or disclosure of the surveillance information is consistent with the University's obligations under the *Surveillance Devices Act 1999* (Vic);

(vi) whether the proposed use or disclosure of the surveillance information is reasonably proportionate taking into consideration its proposed purpose and the privacy impacts on individuals; and

(vii) who will have access to the surveillance information.

(b) A request to use or disclose surveillance information for purposes other than those set out in the Register of Approved Surveillance Activities must be endorsed by one of the following University staff:

(i) Chief Information Officer;

(ii) Executive Director, Enterprise Performance Group;

(iii) Director, Health and Safety;

(iv) Physical Security Manager, Campus Operations and Delivery;

(v) Executive Director, Workplace Relations and Integrity, who may endorse a request for staff-related purposes only;

(vi) Deputy Registrar, Student and Scholarly Services, who may endorse a request for student-related purposes only;

(vii) an Associate Director in the Office of Research Integrity and Ethics (Research Integrity, Research Ethics, or Research Governance and Compliance), who may endorse a request for research-related purposes only;

(viii) Executive Director, Risk and Assurance; or

(ix) other senior staff as approved by the Vice-President (Administration & Finance) and Chief Operating Officer.

5.4 **Approval to use or disclose surveillance information**

(a) Approval of a request to use or disclose surveillance information for purposes other than those set out in the Register of Approved Surveillance Activities may only be granted by one of the following University staff, who must not also be the person making or endorsing the request:

(i) Provost;

(ii) Vice-President (Administration & Finance) and Chief Operating Officer;

(iii) Chief Information Officer;

(iv) Executive Director, Enterprise Performance Group;

(v) Chief People Officer;

(vi) Executive Director, Workplace Relations and Integrity, who may approve a request for staff-related purposes only;

(vii) Academic Registrar and Executive Director, Student and Scholarly Services, who may approve a request for student-related purposes only;

(viii) Executive Director, Office of Research Management, who may approve a request for research-related purposes only;

(ix) Whistleblower Disclosure Coordinator under the Whistleblower Protection Policy (MPF1346); or

(x) other senior staff as approved by the Vice-President (Administration & Finance) and Chief Operating Officer or Provost.

(b) An approver must not approve a request to use or disclose surveillance information unless they are reasonably satisfied that:

(i) the proposed use or disclosure of surveillance information:

(A) is appropriate, having regard to the legitimate purposes of the University;

(B) does not discriminate on the basis of a protected attribute;

(C) is consistent with the University's obligations under the *Surveillance Devices Act 1999* (Vic); and

(D) is reasonably proportionate in the circumstances;

(ii) relevant human rights have been properly considered; and

(iii) applicable University policies and operational procedures will be followed for the access, use or disclosure of surveillance information.

(c) An approver may impose conditions or limitations on their approval under this section.

(d) An approver may give a standing approval under this section.

5.5 **Procedural requirements**

(a) The requestor must:

(i) keep a record of the approver's decision made under section 5.2 or section 5.4; and

(ii) provide appropriate details to the Chief Information Officer to enable the Register of Approved Surveillance Activities to be updated.

(b) Surveillance activities that are approved in accordance with this policy to be carried out for a testing or feasibility purpose (for example, a time limited pilot) will not be added to the Register of Approved Surveillance Activities. If approval is granted to fully implement the piloted activity, the activity must be added to the register, including any appropriate amendments to the approval.

(c) Surveillance activities and the use and disclosure of surveillance information must be conducted in accordance with this policy, associated procedures and applicable legal requirements.

5.6 **Storage and retention of surveillance information**

Surveillance information will be stored and retained in accordance with the University's Retention and Disposal Authority.

6. Roles and responsibilities

	Role/Decision/Action	**Responsibility**
6.1	Maintain the Register of Approved Surveillance Activities	Chief Information Officer
6.2	Approve a request to: (a) use a new type of device for surveillance activities; (b) implement a new method of surveillance; or (c) make a material change to the way in which an existing device or method is used to pursue a surveillance activity.	Any two of the following (one of whom must be a member of the Vice-Chancellor Advisory Group (VCAG)): (i) Chief Information Officer; (ii) Executive Director, Enterprise Performance Group;

		(iii) Vice-President (Administration & Finance) and Chief Operating Officer; (iv) Deputy Vice Chancellor (Education) for academic-related purposes only; (v) Deputy Vice Chancellor (Research) for research-related purposes only; (vi) Provost; (vii) Vice-Chancellor.
6.3	Conduct a Privacy Impact Assessment in respect of a surveillance activity where required by the Privacy Policy (MPF1104)	Director, Information Governance Services
6.4	Endorse a request to use or disclose surveillance information for purposes other than those set out in the Register of Approved Surveillance Activities	(i) Chief Information Officer; (ii) Executive Director, Enterprise Performance Group; or (iii) Director, Health and Safety; (iv) Physical Security Manager, Campus Operations and Delivery; (v) Executive Director, Workplace Relations and Integrity, for staff-related purposes only; (vi) Deputy Registrar, Student and Scholarly Services, for student-related purposes only; (vii) an Associate Director in the Office of Research Integrity and Ethics (Research Integrity, Research Ethics, or Research Governance and Compliance), for research-related purposes only; (viii) Executive Director, Risk and Assurance; or (ix) other senior staff as approved by the Vice-President (Administration & Finance) and Chief Operating Officer.
6.5	Approve a request to use or disclose surveillance information for purposes other than those set out in the Register of Approved Surveillance Activities	(i) Provost; (ii) Vice-President (Administration & Finance) and Chief Operating Officer; (iii) Chief Information Officer;

		(iv) Executive Director, Enterprise Performance Group; (v) Chief People Officer; (vi) Executive Director, Workplace Relations and Integrity, for staff-related purposes only; (vii) Academic Registrar and Executive Director, Student and Scholarly Services, for student-related purposes only; (viii) Executive Director, Office of Research Management, for research-related purposes only; (ix) Whistleblower Disclosure Coordinator under the Whistleblower Protection Policy (MPF1346); or (x) other senior staff as approved by the Vice-President (Administration & Finance) and Chief Operating Officer or Provost.

7. Definitions

In this policy:

(a) **business continuity** means the ability of appropriate University staff to maintain or restore operations during, or in anticipation of, a disruption (for example, accessing a user's University account, files, or systems when a user is on leave or otherwise unavailable, or taking reasonable actions to respond to a disaster or cyber incident);

(b) **protected attribute** has the meaning given in section 6 of the *Equal Opportunity Act 2010* (Vic) and means:

(i) age;

(ii) breastfeeding;

(iii) employment activity;

(iv) gender identity;

(v) disability;

(vi) industrial activity;

(vii) lawful sexual activity;

(viii) marital status;

(ix) parental status or status as a carer;

(x) physical features;

(xi) political belief or activity;

(xii) pregnancy;

(xiii) profession, trade or occupation;

(xiv) race;

(xv) religious belief or activity;

(xvi) sex;

(xvii) sex characteristics;

(xviii) sexual orientation;

(xix) an expunged homosexual conviction;

(xx) a spent conviction;

(xxi) personal association (whether as a relative or otherwise) with a person who is identified by reference to any of the above attributes;

(c) **surveillance** means surveillance by a method described in section 4.2 of this policy or approved under this policy;

(d) **surveillance information** means data or information obtained, recorded, monitored or observed as a consequence of surveillance;

(e) **University computing and network facilities** means computers, computer systems, data network infrastructure, wireless network access facilities, email and other communications and information facilities and related services, together with associated equipment, software, files and data storage and retrieval facilities which are owned or operated by or on behalf of the University and form part of the central facilities or the local facilities;

(f) **University premises** means the University's campuses or any other premises occupied by the University;

(g) **University research policy** means:

(i) Animal Care and Use Policy (MPF1383);

(ii) Human Research Ethics and Safeguards Policy (MPF1385); and

(iii) Biorisk Management Policy (MPF1384).

8. Policy approver

Vice-President (Administration & Finance) and Chief Operating Officer.

9. Policy stewards

Chief Information Officer

Executive Director, Enterprise Performance Group.

10. Review

This policy is due to be reviewed by [TBC].

11. Version history

Version	Approved By	Approval Date	Effective Date	Sections Modified
1	[TBC]	[TBC]	[TBC]	New policy