GV0235 Table of Changes

Section: Definitions

Notes:

- All instances of plural references have been adjusted to singular for clarity.
- Oxford commas have ben added to the policy throughout.
- Links to other policies and procedures will be updated in the final version.

Clause	Original Provision	Changed Provision	Rationale
1. Purpose	This policy articulates how the university complies with the privacy components of the Freedom of Information and Protection of Privacy Act (FIPPA).	No change.	N/A
2. Definitions	N/A	For the purposes of this policy, the following definitions apply.	Removed numbering of definitions for consistency with UVic policy practices. New intro added for consistency.
Administrative Authority	means individuals with administrative responsibility for Units including but not limited to: Vice-Presidents, Associate Vice-Presidents, Deans, Chairs, Directors, Executive Directors, the Chief Information Officer, and other Unit Heads.	No change.	N/A
Consistent Purpose	Consistent Purpose means a use or disclosure of Personal Information which is consistent with the purposes for which the information was obtained or compiled if the use or disclosure: (a) has a reasonable and direct connection to that purpose, and (b) is necessary for performing the statutory duties of, or for operating a legally authorized program of,	No change.	N/A

Clause	Original Provision	Changed Provision	Rationale
	the Unit that uses or discloses the information or causes the information to be used or disclosed.		
Contact Information	means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.	No change.	N/A
Data	N/A	means digital or physical records, including personal information, held by the university.	Expanding definition of data, including personal information, for the purpose of explaining disclosure below
Delegation Instrument	N/A	means a document outlining the authority for an employee of the University to conduct activities and perform duties required under FIPPA required to be conducted by the head of the public body.	Defining the mention of a delegation instrument within the policy
Disclose	means to transmit or provide, intentionally or unintentionally, Personal Information by any means to an individual	means to transmit, provide, or make available, intentionally or unintentionally, data by any means to a person.	Expanded the definition to include all data types as a disclosure.
Employee	In relation to the university, includes a volunteer and a service provider	in relation to the university, and for the purposes of this Policy and it's associated procedures, each reference herein to Employee includes Officers of the university (E.g. members of Senate and the Board of Governors), faculty members, and volunteers.	Added additional clarity and removed a service provider from the definition of an employee. Though service providers are responsible for UVic data, the inclusion of them in the definition impacts uses of employee later in the policy.
Monitor/Monitored	(verb) means a Surveillance System is used to view live footage of an area without creating a record of that observation.	No change.	N/A
Personal Information	Means recorded information about an identifiable individual other than contact information	No change.	N/A

Clause	Original Provision	Changed Provision	Rationale
Privacy and Access to Information Office	N/A	is the university department under the leadership of the Corporate Privacy Officer, responsible for ensuring compliance with FIPPA and this policy.	Added for clarity.
Privacy Breach	N/A	refers to a confirmed case of unauthorized access to or collection, use, disclosure or disposition of Personal Information. Such activity is considered to be 'unauthorized' if it occurs in contravention of the Freedom of Information and Protection of Privacy Act, or the University's Protection of Privacy Policy (GV0235).	Added for clarity.
Privacy Impact Assessment	means a~~n~~ assessment that the university conducts to determine if a current or proposed system, project, program or activity meets or will meet FIPPA's privacy protection requirements.	means a legally required assessment that the university conducts to determine if a current or proposed system, project, program, or activity meets or will meet the requirements of FIPPA, this policy and its associated procedures.	Clarity of requirements and a reflection that this is now legally required under FIPPA.
Privacy Incident	N/A	means an unconfirmed but potential Privacy Breach.	Added for clarity.
Record	Record (noun) includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.	No change.	N/A
Record/Recorded	(verb) means a Surveillance System used to convert images and/or sound into a record that can be reproduced.	No change.	N/A
Service Provider	N/A	means a third party individual, organization, company, application, contractor, service, or software as service retained under contract to	Added to improve clarity and due to removal from employee definition.

Clause	Original Provision	Changed Provision	Rationale
		provider services or deliver work on behalf of the university.	
Surveillance System	means an analog or digital video recording system (with or without audio) authorized and used by the university intended to monitor or record the activities of people or monitor or record an area that is accessible to the university community or public. For the purposes of this policy and its associated procedures, surveillance does not include the use of personal video equipment or the recording or broadcasting of public events, educational activities, or recordings done through UVic Audiovisual and Multimedia Services.	No change.	N/A
Unauthorized Disclosure	N/A	Means the disclosure, production, or provision of access to Personal Information which is not authorized by the Freedom of Information and Protection of Privacy Act or another applicable statute.	Clarifying what is meant by unauthorized disclosure, as related to a privacy breach or incident
Unit	means academic or administrative areas at the university, including but not limited to: faculties, departments, divisions, offices, schools and centres.	means academic or administrative areas at the university, including but not limited to: • faculties, • departments, • divisions, • offices, • schools, and • centres.	Reformatted.
Use of Personal Information	means employing or handling Personal Information by Employee~~s~~ to accomplish the university's objectives; for example, to: • administer a program or activity; • provide a service; or • determine someone's eligibility for a benefit or suitability for a job.	means the employing or handling of Personal Information by an Employee to accomplish the university's objectives, for example, to: • administer a program or activity; • provide a service; or • determine someone's eligibility for a benefit or suitability for a job.	Linguistic edit

Clause	Original Provision	Changed Provision	Rationale
~~15~~ **3.00 Jurisdiction/Scope**	This policy applies to all Employees ~~(including faculty), students~~ and Units. It applies to all Personal Information in the custody or under the control of the university.	This policy applies to all Employees and Units. It applies to all Personal Information in the custody or under the control of the university.	Students were removed as the policy does not apply to them. Reference to faculty removed as they are employees, as defined by FIPPA.
~~16.00~~ **4.00 Policy**	The university will manage all Personal Information in accordance with the FIPPA, the University Act, ~~collective agreements, contracts, and this and other~~ applicable university policies and associated procedures.	The university will manage all Personal Information in accordance with FIPPA, the University Act, as well as all applicable university policies and associated procedures, collective agreements, and contracts.	Reorganized for clarity and flow.
~~17.00~~ **5.00 Accountability for Personal Information**	The President will designate a senior administrator to act as head under the FIPPA who will be responsible for the administration of the FIPPA and this policy.	The President will designate a senior administrator to act as head under FIPPA who will be responsible for the administration of FIPPA and this policy. The General Counsel is designated by the President as the head of the university for the purposes of FIPPA.	Former 17.01 was moved up for flow. Combines separate section that designates the General Counsel as the head under FIPPA.
~~17.01~~	~~The General Counsel has been designated by the President as the head.~~	N/A	Combined with 5.00
~~18.00~~ **6.00 General Counsel**	As the head, the General Counsel is responsible for the overall co-ordination of privacy and access functions.	No change.	N/A
~~18.01~~ **6.01**	The General Counsel will carry out their duties in collaboration with the University Secretary and the University Archivist, who are responsible for the maintenance of the university's Records management program.	No change.	N/A
6.02	N/A	The General Counsel may delegate their authority under FIPPA, as necessary to accomplish their duties under FIPPA. The Corporate Privacy Officer carries the delegated authority of the General Counsel to lead the Privacy and Access to Information Office, in accordance with	Added to clarify that the CPO is the delegated official for the General Counsel.

Clause	Original Provision	Changed Provision	Rationale
		the terms and conditions as enumerated in the delegation instrument.	
~~19.00~~ **7.00 ~~Chief~~ Corporate Privacy Officer**	In collaboration with the University Secretary, the University Archivist, and the Chief Information Officer, the Chief Privacy Officer is responsible for promoting, monitoring, and reporting on compliance with the FIPPA and with university privacy, records management, and information security policies. The Chief Privacy Officer's responsibilities include: • Providing privacy advice and training; • Providing ongoing assessment of privacy risks; and • Responding to privacy complaints and investigating concerns about privacy issues.	In collaboration with the University Secretary, the University Archivist, and the Chief Information Officer, the Corporate Privacy Officer is responsible for promoting, monitoring, and reporting on compliance with FIPPA as it relates to university privacy, records management, and information security policies. Under this policy, the Corporate Privacy Officer's responsibilities include: • leading the Privacy and Access to Information Office; • providing advice on privacy matters; • providing privacy training; • providing ongoing assessment of privacy risks for the university; • providing guidance and review of Privacy Impact Assessments under s. 27.00; • responding to privacy incidents and complaints; • investigating concerns about privacy issues; and • working with partners across campus towards reconciliation related to data initiatives involving Indigenous communities.	Title change and expanded scope of responsibilities to better reflect the responsibilities assigned under this policy.
~~19.01~~ **8.00**	Where the Chief Privacy Officer establishes that there is a significant privacy risk, the Chief Privacy Officer may investigate and/or recommend to the appropriate Administrative Authority corrective action, suspension, or termination of a project or activity.	Where the Privacy and Access to Information Office establishes that there is a significant privacy risk, in accordance with the university's policies and procedures for managing data risk, the Corporate Privacy Officer may investigate and/or recommend to the appropriate Administrative Authority	Clarifies that the office, under the leadership of the CPO, has delegated responsibility for identifying risk.

Clause	Original Provision	Changed Provision	Rationale
		corrective action, suspension, or termination of a project or activities.	
9.00	N/A	The Administrative Authority must carefully consider the results of an investigation and/or recommended action by the Corporate Privacy Officer when making a decision, in accordance with policies and procedures on data risk and signing authorities.	Added responsibilities under this section for Administrative Authorities.
~~20.00~~ **10.00 Administrators**	Administrative Authorities and managers are responsible for: • ~~making reasonable efforts to~~ familiarize themselves with the requirements in the FIPPA, this policy and its associated procedures, ~~and for making reasonable efforts to communicate these requirements to the Employees in their Units;~~ • ~~making reasonable efforts to~~ ensure that the management of Personal Information in the custody or under the control of their units meets the requirements of the FIPPA, this policy and its associated procedures; • reporting any privacy incidents or breaches of the FIPPA, this policy or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach; and ~~• Conducting risk-based privacy impact assessments under s. 42.00.~~	An Administrative Authority or manager is responsible for: • familiarizing themselves with the requirements in FIPPA, this policy, and its associated procedures; • discussing with the Privacy and Access to Information Office all privacy concerns as they arise; • communicating these requirements to the Employees in their Units; • ensuring that the management of Personal Information in the custody or under the control of their Units meets the requirements of FIPPA, this policy, and its associated procedures; • ensuring that all Employees in their Units complete the annual privacy training; and • reporting to the Privacy and Access to Information Office any privacy incidents or breaches of FIPPA, this policy, or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach.	References to reasonable efforts have been removed, this policy outlines responsibilities, including familiarizing themselves with policy responsibilities and legal responsibilities relevant to job area.

Clause	Original Provision	Changed Provision	Rationale
~~21.00 Employees~~	~~All Employees who collect, access, use, disclose, maintain and dispose of Personal Information are in a position of trust.~~	N/A	Removed due to lack of actionable policy provision, as this is an expected value of any employee.
~~21.01~~ **11.00 Employees**	Employees are responsible for: • treating all Personal Information to which they receive access in accordance with the FIPPA and this policy; • ~~making reasonable efforts to~~ familiarize themselves and to comply with the requirements in the FIPPA, this policy, and its associated procedures; • consulting as necessary with the appropriate authority regarding the requirements in the FIPPA, this policy, and its associated procedures; and • reporting any privacy incidents or breaches of the FIPPA, this policy, or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach.	An Employee with access to Personal Information as a part of their duties are responsible for: • treating all Personal Information they access in accordance with FIPPA and this policy; • familiarizing themselves and complying with the requirements in FIPPA, this policy, and its associated procedures; • completing the annual privacy training; • consulting as necessary with the appropriate authority regarding the requirements in FIPPA, this policy, and its associated procedures; and • reporting to their Administrative Authority, manager, or Access to Information and Privacy Office any privacy incidents or breaches of FIPPA, this policy, or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach.	References to reasonable efforts have been removed, this policy outlines responsibilities, including familiarizing themselves with policy responsibilities and legal responsibilities relevant to job area. Responsibilities related to training added Clarifying who to report breaches to.
~~22.00 Third Parties~~ **12.00 Service Providers**	The university will require a ~~third party~~ service provider whose work on behalf of the university involves the collection, use or Disclosure of Personal Information to abide by this policy, ~~the Privacy Protection Schedule~~, and FIPPA in its handling of personal information on behalf of the university, and may require the service provider to sign a confidentiality agreement.	The university will require a service provider whose work on behalf of the university involves the collection, use, or disclosure of Personal Information to abide by this policy and FIPPA in its handling of Personal Information on behalf of the university, and may require the service provider to sign a	Section reorganized, and references to third parties removed, as well as additional option of adding the Data Protection Schedule.

Clause	Original Provision	Changed Provision	Rationale
		confidentiality agreement or have a Data Protection Schedule attached to a contract.	
12.00	N/A	Any proposed work to be conducted by a service provider must be reviewed by a privacy impact assessment prior to conducting work.	Responsibility to complete a PIA before conducting work added, due to 2021 change in legislative requirements.
~~25.00 Identifying Purpose for Collection~~ **13.00 Collection Notice**	~~The university collects Personal Information as authorized by the FIPPA and the University Act, including collecting Personal Information that relates directly to and is necessary for an operating program or activity of the university.~~	The university is required to collect certain Personal Information from individuals to fulfill its mandate under the University Act. All other Personal Information collected by the university will be authorized by FIPPA, the University Act, or other applicable legislation.	Combination of 25.00 and 25.01
~~25.01~~	~~The university collects Personal Information from students, Employees and others in order to fulfill its mandate under the University Act.~~	N/A	Combined 25.00 and 25.01 to create new 13.00
14.00	N/A	Unless authorized by FIPPA, another enactment, or an individual, the university will provide notice before collecting Personal Information directly from an individual.	Created new provision to outline that notice is required in most circumstances.
~~23.00 Openness about Personal information Policies and Practices~~ – **15.00**	The university will make the following information available to an individual from whom Personal Information is being collected: (a) the purpose for which the Personal Information is being collected; (b) the legal authority to collect the Personal Information; and (c) the Contact Information of someone who can provide details about the collection.	If notice is required, the university will make the following information available to an individual from whom Personal Information is being collected: (a) the purpose for which the Personal Information is being collected; (b) the legal authority to collect the Personal Information; and (c) the Contact Information of someone who can provide details about the collection.	Added to clarify that in circumstances where notice is legally required, notice must include the following.

Clause	Original Provision	Changed Provision	Rationale
16.00	N/A	If an Employee or Administrative Authority is unsure whether notice is required before collecting information, contact the Privacy and Access to Information Office.	Clarifying that an employee should check with the Privacy and Access to Information Office if unsure.
~~24.00~~	~~This policy will be made available on the university website.~~	N/A	Removed due to lack of necessity.
~~26.00 Consent for Collection of Personal Information~~	~~The university will normally obtain either express or implied consent from an individual before collecting Personal Information, but may collect, use or disclose Personal Information without consent in limited circumstances where the FIPPA authorizes such activity.~~	N/A	Removed as consent is not a valid authority for collecting personal information under FIPPA
~~27.00 Limiting Collection of Personal Information~~	~~The university will normally collect Personal Information directly from the individual whom the Personal Information is about, but may collect Personal Information indirectly in limited situations where such collection is authorized by the FIPPA, another enactment, or the individual.~~	N/A	Removed as this is legal nuance best explored during the PIA process and covered under provision 16
~~27.01~~	~~The university may also collect Personal Information indirectly for purposes of:~~ ~~(a) determining suitability for an honour or award, including an honorary degree, scholarship, prize or bursary;~~ ~~(b) a proceeding before a court or a judicial or quasi-judicial tribunal;~~ ~~(c) collecting a debt or fine or making a payment;~~ ~~(d) law enforcement; or~~ ~~(e) any other purposes permitted by law.~~	N/A	Removed as this is legal nuance best explored during the PIA process and covered under provision 16

Clause	Original Provision	Changed Provision	Rationale
~~28.00 Use, Disclosure, and Retention of Personal Information~~ **17.00**	The university uses and discloses the Personal Information in its custody or under its control: (a) for the purpose for which that information was obtained or compiled or for a Consistent Purpose; (b) in a manner to which an individual has consented; (c) as permitted or required by the FIPPA or as authorized or required by other law; (d) for research and statistical purposes; or (e) for archival or historical purposes.	An Employee must only use and disclose the Personal Information in the university's custody or control: (a) for a purpose consistent with the reason the information was collected; (b) in a manner to which an individual has consented; (c) as permitted or required by FIPPA or as authorized or required by other law; (d) for research and statistical purposes; or (e) for archival or historical purposes.	Reorganized sentences for clarity and noted that the responsibility ultimately lays with an employee.
~~29.00~~ **18.00**	Employees must only seek to access and use Personal Information necessary for the performance of their duties.	An Employee must only use, and disclose Personal Information that is necessary for the performance of their duties. An Employee may permit others in their Unit or other university Unit's to access Personal Information if the purpose is consistent with the purpose for which the information was obtained.	Combined 29.00 and 30.00 into a new 18.00 and reorganized to improve flow.
~~30.00~~	~~Employees may allow other Employees to use Personal Information needed for the performance of their duties. Employees may also allow other Employees to use Personal Information if the FIPPA authorizes the use of that Personal Information.~~	N/A	Combined 29.00 and 30.00 into a new 18.00 and reorganized to improve flow.
~~30.01~~ **18.01**	If an Employee is in doubt whether to allow another Employee to use Personal Information, the Employee will consult with their Administrative Authority or manager as necessary.	An Employee must consult their Administrative Authority, manager, or the Privacy and Access Office if they are uncertain whether a purpose is consistent with the purpose the Personal Information was collected.	Sentence restructured to make action oriented.
~~31.00~~ **19.00**	The university will disclose Personal Information to students and individuals or organizations outside the university as permitted by the FIPPA, as authorized or required by an enactment, as permitted by this policy and its associated procedures.	The university may disclose Personal Information to students and individuals or organizations outside the university as permitted by FIPPA, as authorized or required by an enactment, as permitted	Sentence made permissive, in line with legal authorities

Clause	Original Provision	Changed Provision	Rationale
		by this policy, or its associated procedures.	
~~31.01~~ **19.01**	Personal Information shall only be disclosed in compliance with the Procedures for the Management of Personal Information.	No change.	N/A
~~32.00~~ **19.02**	Disclosure of the following information without consent is permitted: ~~(a) an Employee's Contact~~ ~~(b) Information;~~ ~~information about an individual's position, functions, or remuneration as an officer, Employee, or member of the university;~~ ~~(c) names of individuals who have received degrees, the names of degrees those individuals received and the years in which the degrees were awarded; and~~ ~~(d) Personal Information about an individual in an emergency situation or where the General Counsel (or designate) determines that compelling circumstances exist that affect anyone's health or safety, or as permitted by the Procedures for Disclosure of Student Information in Emergency or Compelling Circumstances.~~	Disclosure of the Personal Information without consent is permitted in certain circumstances as required by FIPPA, other legislation, or the advice of the Privacy and Access to Information Office.	Changed to note that it is best for an employee to reach out for advice if uncertain – this reduces the risk of a possible privacy breach.
~~31.02~~ **19.03**	If an Employee is in doubt whether to disclose Personal Information, the Employee will consult with their Administrative Authority as necessary.	If an Employee is in doubt whether to disclose Personal Information, the Employee will consult with their Administrative Authority, manager, or the Privacy and Access to Information Office.	Added to note that an administrative authority may not always be the most appropriate person to ask.
~~33.00~~ **20.00**	Disclosing Personal Information outside Canada must be done in compliance with FIPPA and the Procedures for the Management of Personal Information.	No change.	N/A
~~34.00~~ **21.0 Retention**	The university will retain Personal Information collected from individuals in accordance with the	No change.	N/A

Clause	Original Provision	Changed Provision	Rationale
	FIPPA and the university-wide records classification, retention and disposition plan.		
22.00	N/A	An Administrative Authority or manager is responsible for understanding the Directory of Records and the appropriate retention and disposition schedules as defined by the Records Management Policy.	New provision to outline responsibilities for record retention and disposition.
~~34.01~~ **22.01**	The university will retain Personal Information used to make a decision about an individual for a minimum of one year.	The university will retain all Personal Information used to make a decision about an individual that does not have a retention and disposition schedule for one year.	Adding note about possibly retaining longer if there is a disposition schedule
~~38.00 Ensuring Accuracy of Personal Information~~ **23.00**	The university will make every reasonable effort to ensure that the Personal Information in its custody or under its control is accurate and complete and will allow ~~Employees and students~~ to confirm the accuracy of this information.	The university will make every reasonable effort to ensure that the Personal Information in its custody or under its control is accurate and complete and will allow an individual to confirm the accuracy of their personal information.	Changed language to be more aligned with the rights of any individual under the legislation
~~38.01~~ **23.01**	Procedures for the correction of Personal Information are contained within the university's Procedures for the Access to and Correction of Information.	No change.	N/A
~~39.00 Safeguards for Personal Information~~ **24.00**	The university will protect Personal Information in its custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposition.	No change.	N/A
~~40.00 Individual Access to Personal Information~~ **25.00**	Individuals have a right to access Personal Information about themselves, subject to exceptions under the FIPPA. Access to Personal Information is provided in accordance with the university's Access to and Correction of Information procedure.	No change.	N/A
~~41.00~~ **26.00**	Individuals have a right to request corrections to Personal Information about themselves, subject to exceptions under the FIPPA. Corrections to Personal	No change.	N/A

Clause	Original Provision	Changed Provision	Rationale
	Information are provided in accordance with the university's Access to and Correction of Information procedure.		
~~42.00 Privacy Impact Assessments~~ **27.00**	The Administrative Authority ~~must conduct a risk-based~~ Privacy Impact Assessment for all new systems, projects, programs or activities and substantially modified systems or activities. The nature and extent of the assessment will be based upon the risk.	The Administrative Authority must ensure a Privacy Impact Assessment has been completed for all new systems, projects, programs, or activities and substantially modified systems or activities. The nature and extent of the assessment will be based upon the risks assessed, in accordance with policies and procedures regarding data risk.	Adding responsibilities in line with the 2021 legislative amendments
~~42.01~~ **27.01**	Before committing the university to a project or initiative or before procurement that may entail privacy risks, the Administrative Authority will assess the project or initiative for potential privacy risks.	Before committing the university to a project, program, system, initiative, or activity or before procurement, the Administrative Authority must direct an Employee from their Unit who has appropriate technical knowledge to draft, with guidance from the Privacy and Access to Information Office, a PIA.	Adding responsibilities in line with the 2021 legislative amendments and a requirement that the individual submitting the PIA have sufficient knowledge of the proposal.
~~42.02~~	~~Upon completion of the PIA, an appropriate Administrative Authority, which may be the same Administrative Authority that completed the PIA, will determine whether the project's risk after mitigation shall be accepted, or whether the project should not proceed.~~	Removed.	Removed to make way for new policies or procedures around managing data risk
~~42.03~~	~~In 42.02 the appropriate Administrative Authority will be determined under the Procedures for the Management of Personal Information. This determination will be based on the magnitude of the risk which is determined by impact and likelihood of the risk.~~	Removed.	Removed to make way for new policies or procedures around managing data risk
28.00	N/A	The Privacy and Access Office is the office of primary responsibility for the	Establishing the Office of Primary Responsibility for PIA records to reduce record

Clause	Original Provision	Changed Provision	Rationale
		storage and disposal of Privacy Impact Assessments.	duplication across the university
~~35.00~~ **29.00 Surveillance**	The university may use Surveillance Systems to: (a) improve personal safety on university property by acting as a deterrent or increasing the likelihood of identifying individuals who may commit criminal activity; (b) assist law enforcement agencies with the investigation of any suspected criminal activity; (c) assist with the protection of university assets and infrastructure; or (d) ~~assist with the application of university policies.~~	The university may use Surveillance Systems to: (a) improve personal safety on university property by acting as a deterrent where other practical options have failed or increasing the likelihood of identifying individuals who may have commit criminal activity; (b) assist with, upon the request of law enforcement agencies, the investigation of any suspected criminal activity; (c) assist with the protection of university assets and infrastructure; or (d) aiding in the investigation of violations of the university's Sexual Violence Prevention and Response Policy (GV0245).	Surveillance footage should only be used in very limited circumstances. Provision amended to highlight that not all university policies warrant surveillance as an investigative tool under FIPPA. Also amended language to emphasize practicality and reasonableness when considering alternatives.
~~35.01~~ **29.01**	Surveillance Systems shall not be used to monitor or record areas where the university community or public have a reasonable expectation of privacy.	No change.	N/A
~~35.02~~ **29.02**	The university will deploy Surveillance Systems only as an exceptional step to address real, pressing and substantial problems or risks and only where a less privacy-invasive alternative is not available. Surveillance Systems will be designed to minimize the impact on privacy. The privacy impact of the proposed Surveillance System will be assessed and documented in the Privacy Review Form.	The university will deploy Surveillance Systems only as an exceptional step to address problems or risks identified in section 29.00, where a less privacy-invasive alternative is not practical. Surveillance Systems will be designed to minimize the impact on privacy. The privacy impact of the proposed Surveillance System will be assessed and documented in a PIA.	Clarifying the considerations when looking to deploy surveillance
~~35.03~~ **29.03**	Approval is required prior to installation of a Surveillance System. The General Counsel is responsible for approval of the installation, following	Approval is required prior to installation of a Surveillance System. The General Counsel is responsible for approval of	Clarifying language to reflect current practices

Clause	Original Provision	Changed Provision	Rationale
	input from the Vice-President Finance and Operations and confirmation that the installation is necessary to address real, pressing and substantial problems or risks and that a less privacy-invasive alternative is not available.	the installation, following input from the Vice-President Finance and Operations and Corporate Privacy Officer, and confirmation that the installation is necessary to address real, pressing, and substantial problems or risks and that a less privacy-invasive alternative is not practical.	
~~35.04~~ **29.04**	~~The requisite Vice-President may delegate the day-to-day operations and administration of the Surveillance System in accordance with the Procedures for the Management of University Surveillance Systems.~~	Surveillance Systems shall be operated on a day-to-day basis and administered by the university's Campus Security department.	Moving towards centralization of surveillance under CSEC
~~36.00~~ **30.00**	In accordance with the Procedures for the Management of University Surveillance Systems, the university will provide notice of the use of Surveillance Systems by prominently displaying signage at the perimeter or entrance to the area being monitored or recorded to alert individuals that such systems are or may be in use before they enter any area under surveillance.	No change.	N/A
~~37.00~~ **31.00**	Sections 35.00 and 36.00 apply only to Surveillance Systems installed with notice, i.e., overt surveillance.	Sections 29.00 and 30.00 apply only to Surveillance Systems installed with notice, i.e., overt surveillance.	Section references updated.
~~43.00 Challenging Compliance with the Privacy Policy~~ **32.00**	Individuals are entitled to challenge the university's compliance with this policy.	An Individual is entitled to challenge the university's compliance with this policy.	Language changed to singular.
~~43.01~~ **32.01**	Employees who receive a complaint or inquiry about compliance with the policy should attempt to resolve the issue with the assistance of a supervisor.	An Employee who receives a complaint or inquiry about compliance with the policy should attempt to resolve the issue with the assistance of a supervisor.	Language changed to singular.
~~43.02~~ **32.02**	Individuals may make a formal complaint or inquiry about compliance with this policy by contacting the Privacy and Access Office.	An Individual may make a formal complaint or inquiry about compliance	Language changed to singular.

Clause	Original Provision	Changed Provision	Rationale
		with this policy by contacting the Privacy and Access Office.	
33.00	N/A	Employees (including faculty) must comply with the following procedures associated with this policy:	Directing employees to comply with certain procedures
33.01	N/A	Procedures for Responding to a Privacy Incident or Breach	Policy identified for s.33
33.02	N/A	Procedures for the Management of University Surveillance Systems	Policy identified for s.33
33.03	N/A	Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances	Policy identified for s.33
33.04	N/A	Procedures for the Management of Personal Information	Policy identified for s.33
~~General~~	~~The General Counsel may waive the requirements in sections 22.00 and 42.00 in exceptional circumstances.~~	N/A	Removed.