Interim: Privacy and Data Protection Policy

Document summary

Effective date	4 December 2021	**Last updated**	22 November 2021
Document owner	Vice-Chancellor		
Approved by	Council	**Reviewed by**	UCT POPIA Working Group
Enquiries	Vice-Chancellor, vc@uct.ac.za		
Document Ref	ISMS-DOC-A18-5		

Revision and approval history

Review period: This policy must be reviewed every five years.

Version	Revision Type	Amendments	Approved by	Signed	Review date

Table of contents

Purpose

At the University of Cape Town, we value the trust our students, alumni, employees, research participants, partners, service providers, suppliers and other data subjects place in us when they share their personal information with us. Without this personal information, we would not be able to function effectively, so it is crucial that we protect it in accordance with the principles set out in the Protection of Personal Information Act (POPIA) and other privacy regulations. This policy sets out how we achieve that.

We have this policy to help guide our actions so that we keep the personal information of data subjects safe, protect our reputation, and comply with all relevant data protection regulations, including the Protection of Personal Information Act (POPIA).

Definitions

Term	Definition
Data subjects	The person or organisation to whom personal information relates. This includes: • prospective students, students, and alumni; • staff members, job applicants, and functionaries; • service providers, contractors, and suppliers; • partner institutions, and funders; • research participants; • members of the public and visitors.
Incident	An incident includes: • non-compliance with this policy and any procedures relating to it; • contraventions of any data protection legislation such as the POPIA; and • security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.
Processing activities	Processing activities are a collection of interrelated work tasks that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored, or destroyed. A processing activity is important if we could experience critical or high levels of risk if the process or activity is disrupted or could no longer continue.
Personal information	Personal information means any information relating to an identifiable individual (living or deceased) or an existing organisation (a company, public body, etc.). This includes the personal information of all customers, staff members, job applicants, shareholders, board members, service providers, contractors, suppliers, members of the public, and visitors. Examples include: • identifiers, such as a name, identity number, staff number, account number, customer number, company registration number, tax number, photos, videos, or any other unique information that can be used to identify a person; • demographic information, such as race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, religion, conscience, belief, culture, language, and birth; • information relating to physical or mental health, wellbeing, or disability;

	• background information, such as education, financial, employment, medical, criminal or credit history; • contact details, such as physical and postal address, email address, telephone number, online identifier (e.g. a person's twitter handle) or location information; • biometric information: this refers to techniques of identification that are based on physical, physiological, or behavioural characterisation, such as blood-typing, fingerprinting, DNA analysis, retinal scanning, facial recognition, and voice recognition; • someone's opinions, views, and preferences; • private or confidential correspondence and any further correspondence that would reveal the contents of the original correspondence; • views or opinions about a person, such as interview notes and trade references; and • the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject.
POPIA	The Protection of Personal Information Act 4 of 2013 and its regulations.
POPIA Programme	The POPIA Programme is our ongoing efforts to comply with the provisions of the POPIA and includes: • stakeholder consultation; • defining roles and responsibilities; • policy development; • policy implementation; • monitoring and audit; and • continual improvement.
Processing	Any operation or activity or any set of operations concerning personal information, including: • collecting, receiving, recording, organising, collating, storing, updating or modifying, retrieving, altering, consulting, or using; • disseminating by means of transmission, distributing, or making available in any other form; or • merging, linking, restricting, degrading, erasing, or destroying personal information.

International Organisation for Standardisation Reference

This policy aligns with the University's Information Security policy with reference to ISO 27001:2017.

- A.5 Information security policies
    - A.5.1 Management direction for information security
        - A.5.1.1 Policies for information security

- A.18 Compliance
  - A.18.1 Compliance with legal and contractual requirements
  - A.18.1.4 Privacy and protection of personally identifiable information

Applicable to

This policy applies to:

- any activity where we produce or use personal information (processing activities);
- anybody involved in processing activities where we produce or use personal information; and
- all employees, service providers, contractors, researchers and other individuals who have access to personal information.

Policy summary

While all personal information should be protected, we take a risk-based approach to compliance. We prioritise the protection of personal information that is used in our important business activities, and in activities that could have a substantial impact on a data subject's right to privacy.

It is our policy to:

1. Follow the principles of privacy protection that are set out in the POPIA.
2. Conduct personal information impact assessments.

Policy details

1. Follow the principles of privacy protection that are set out in the POPIA

1.1. Classify personal information

We identify and classify the personal information that we use and produce.

1.2. Document processing activities

We document all processing activities to ensure that we can respond to requests from the Information Regulator and requests for information by data subjects or third parties.

1.3. Specify the purpose for processing

We specify and document the purposes for which we process personal information.

1.4. Provide legal basis for processing activities

We ensure that:

- all processing activities have a legal basis; and
- we document the specific legal basis for processing personal information for each activity.

1.5. Keep processing to a minimum

We ensure that:

- we process personal information that is adequate, relevant, and not excessive, considering the purpose of the activity; and

- we de-identify personal information before we start the activity where possible. Where de-identification is not possible, we must consider masking the personal information.

1.6. Obtain personal information from lawful sources

We obtain personal information from lawful sources only.

Lawful sources of personal information include:

- the data subject;
- information that the data subject made public deliberately;
- public records; and
- a source that the data subject consented to.

Other sources may be lawful in special circumstances. If you are unsure, speak to the Deputy Information Officer.

1.7. Process transparently

We disclose all processing activities to data subjects in our privacy notices.

1.8. Ensure personal information quality

We take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.

1.9. Limit sharing

We only share personal information if it is legal to do so and ethically justifiable. We:

- identify all instances when personal information is shared with external organisations or individuals (third parties);
- ensure that sharing personal information complies with data protection legislation and the Third Party Risk Management Procedure;
- enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information;
- conduct a Third Party Risk Management Assessment to determine who is responsible to ensure that contracts are concluded, who must review the contracts, and whether we must take additional steps to reduce the risks created by sharing;
- keep record of personal information sharing activities, including the outcome of assessments, a record of additional steps taken, what personal information was shared and when, and the method we used to share the personal information.

1.10. Keep personal information secure

We protect all personal information that we use and produce against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.

All personal information processing must comply with our Information Security Policy.

1.11. Manage personal information incidents

All employees must report incidents in accordance with our Information Security Management Policy and Incident Management Procedure.

An incident includes:

- non-compliance with this policy and any procedures that relate to it;
- contraventions of any data protection legislation such as the POPIA; and
- security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.

Employees must immediately report:

- any known or suspected incidents; or
- any circumstances that increase the risk of an incident occurring.

Reports must be sent to csirt@uct.ac.za.

Information on how to report incidents is available at: https://csirt.uct.ac.za/report-incident and http://www.icts.uct.ac.za/security

1.12. Manage retention periods

We ensure that all records:

- are managed appropriately and in accordance with any operational or legal rules that may apply; and
- comply with our Records Management Policy.

1.13. Respect data subjects' rights

We respect the rights of data subjects to:

- access their records;
- know who their information was shared with;
- correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information;
- withdraw consent; and
- object to the processing of their information when it is not necessary for the conclusion or performance of a contract or to comply with an obligation imposed by law.

All data subject requests must go through the Data Subject Request Procedure.

For more information on these principles, consult the USAf POPIA Guidelines, available at: https://www.usaf.ac.za/wp-content/uploads/2020/09/USAf-POPIA-Guideline_Final-version_1-September-2020.pdf

2. Conduct personal information impact assessments

Directors and Deans must ensure that a personal information impact assessment is done before we start a new processing activity. The personal information impact assessment must include a risk analysis of the activity.

We must conduct a personal information impact assessment before we:

- continue to process personal information as part of an activity that has not undergone a personal information impact assessment before;
- change an existing processing activity;
- launch a new product or service;
- expand into other countries;

- use new systems or software for processing personal information; or
- share personal information with third parties.

A personal information impact assessment has three phases:

- Identify activities in which personal information is processed.
- Complete the data protection impact assessment questionnaire to document the activity, classify information, and perform a risk-rating for the activity.
- Complete a further investigation and assessment with assistance from the Deputy Information Officer if the activity had a risk rating of high or critical after the personal information impact assessment questionnaire was completed.

All activities that are rated as critical or high risk during the personal information impact assessment must undergo an assessment every three years.

All personal information impact assessments must follow the Personal Information Impact Assessment Guideline.

Policy violations

Breach of policy

Our reputation is our biggest asset. Without our reputation, our relationships with staff, students, researchers, funders, government and other key stakeholders would suffer. In addition, we could face substantial fines, legal action and even criminal convictions.

Consequences of breach of policy

This organisation only works when we all do our part, and all of us want to see the organisation succeed. If you do not comply with this policy, or if you discover that we are not complying with the policy and you do not tell us about it, you could face disciplinary action.

Roles and responsibilities

Role	Responsibilities	Procedure
The Information Officer: The Rector and Vice-Chancellor	The Information Officer is responsible to ensure that the University complies with the Protection of Personal Information Act (POPIA) and other privacy regulations and is accountable to the Information Regulator (or any other privacy regulators or authorities that have jurisdiction over the University). The Information Officer has a co-ordinating function that focuses on the policy-based protection of our information and is the policy owner of this policy. The Information Officer must: • designate Deputy Information Officers to perform the responsibilities set out below, and • must ensure that the Deputy Information Officers have sufficient time, adequate resources and financial means to perform their responsibilities.	<Link to procedure>

	The Information Officer must ensure that this policy receives support from the rest of the University and must intervene.	
Deputy Information Officers: • Registrar • Chief Operating Officer • Deputy Vice Chancellor: Research	Deputy Information Officers must support the Information Officer and are responsible for strategic guidance to the organisation on data privacy risk management. The Deputy Information Officers must: • oversee the implementation of this policy, • develop procedures and standards to support data privacy; • provide advice on the identification and management of data privacy risk; • monitor whether personal information impact assessments are performed when required; • develop and conduct training on information governance and privacy protection risks, • respond to data subject requests and objection; • respond to requests from the information regulators and work with regulators when there is an investigation; • monitor whether this policy is implemented throughout the organisation; • oversee the development and maintenance of the PAIA manual; • co-ordinate UCT's response to information breaches and leaks; • ensure training on information governance and privacy protection risks. The Deputy Information Officers may appoint a team to assist them in discharging their duties. Deputy Information Officers must ensure that this team has the capacity and resources to perform the tasks that have been assigned to them.	<Link to procedure>
Executive Director: ICT Services	The Executive Director: Information and ICT Services supports the Information Officer and the Deputy Information Officers by: • developing Information Technology policies, procedures, standards and guidelines; • providing technical advice on data privacy; • supporting the implementation of this policy through appropriate technology investments; • ensuring that when the organisation invests in information technology which will be used to process personal information, that the technology complies with this policy.	
Director: Legal Services	• provides legal advice on the interpretation of legislation; and	

	• ensures that the appropriate contracts with third parties concluded; • ensures that employees are aware of contractual obligations and their responsibilities; • manages legal risks and provides legal advice when an incident occurs.	
Executive Directors and Deans	Directors and Deans must implement this policy, create or align other policies and processes in their business areas with this policy, and monitor and advocate for compliance within their business areas. In addition, some Directors and Deans are data stewards or owners and have additional responsibilities in terms of the University's Information Security Policy and Data Governance Policy. Directors and Deans must ensure that: • business areas comply with this policy; • a register of information assets used in important information processing activities in their business area is created and maintained; • information used in important information processing activities is classified; • personal information impact assessments are conducted before confidential and personal information is processed; • data privacy-related risks in their business area are managed; and • their business area participates in investigations into incidents.	
Users of information	All users who have access to the organisation's information or information systems must: • adhere to all policies, procedures and guidelines that relate to the use of information; • take part in training initiatives; and • report any actual or suspected incidents.	
Internal and external audit	Internal and external audit provides independent assurance that the organisation's risk management, governance and internal control processes are operating effectively, including compliance with this policy.	

Related links

You must read this policy with:

- UCT Information Security Policy
- Policy and Rules on Internet and Email use
- Information Security Incident Response Procedures