POPIA FOR UCT RESEARCHERS
Frequently Asked Questions (FAQ)

The Protection of Personal Information Act 4 of 2013 (POPIA) came into full effect on 1 July 2021. The Act governs all research activities involving identifiable personal information. Whether it's conducting surveys, collecting personal information, or analysing records, compliance with POPIA is essential. To assist with these requirements, we've compiled a list below of frequently asked questions and answers regarding the handling of personal information in research.

Did you know?
We have a specific email address where you can send your research questions, specifically relating to POPIA compliance. popia@uct.ac.za

Want to read more?
For an update on the ASSAf Code's status, see section 7, 'What is the ASSAf Code of Conduct for Research' below.

TABLE OF CONTENTS

1. WHAT DO I NEED TO KNOW ABOUT POPIA?

In short, POPIA applies to your research if you:

- collect research data from or about an identifiable, living individual or an existing organisation; and
- you collect, use, store (or otherwise 'process') that personal information in South Africa.

Want to read more?
See 'The Scope of the Code' in the draft ASSAf Code. It explains what identifiable personal information is, what is considered processing, and how to determine whether it is taking place in South Africa.

1.1. What is personal information?

Personal information can be linked to an identifiable living individual or an existing juristic person (e.g., a company or other kind of organisation).

POPIA provides the following examples:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and the birth of the person;
- information relating to the education or the medical, financial, criminal, or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or another particular assignment to the person;
- the personal opinions, views, or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person.

As you can see, personal information is a very wide concept, but POPIA permits the use of personal information for research purposes. In many ways, it is more lenient than existing ethical rules (e.g., the National Health Act (NHA). There are just certain principles that you, as a researcher, must follow.

Want to read more?
See section 1 of POPIA for the definition.

1.2. When is personal information considered identifiable?

Personal information is considered identifiable when it can be linked to an identifiable living natural person. If there is a reasonable possibility that the information, on its own or in combination with other information, can identify an individual, it is considered identifiable personal information.

Want to read more?
See 'Annexure A: When personal information is identifiable' in the draft ASSAf Code, which explains identifiable personal information, how to de-identify or anonymise the data, and what is expected of responsible parties.

1.3. I am doing health-related research, does POPIA or the NHA apply?

Both may apply.

The National Health Act (NHA):

It focuses on regulating and promoting health-related matters, the provision and management of health services, the protection of health information, and patient rights. Of note the NHA mandates the National Health Research Ethics Council (NHREC) to develop norms and standards, and these are considered to have a regulatory status. The NHREC 2024 Guideline can be found here.

Protection of Personal Information Act (POPIA):

- Safeguards the privacy and confidentiality of all personal information (not just health-related information) and ensures the responsible and lawful processing of personal information.
- When doing health-related research, there is an overlap between POPIA and the NHA, so both of these acts need to be considered in your research.
- The NHA focuses on the ethical considerations of health-related information, while POPIA focuses more on the legal rules around collecting and managing personal information.

For example:
One of these overlaps is the type of consent required. In POPIA, consent may be required for a particular purpose. This consent must be voluntary, specific, transparent, capable of withdrawal, and obtained through an opt-in basis. The NHA has an ethical and responsible informed consent requirement for medical treatment, procedures or participation in a study.

So, you may need both types of consent, depending on the type of research you are doing.

Want to read more?
See 'What are the consent requirements under POPIA' in section 3 below for more information on consent.

1.4. What type of research will be subject to POPIA?

POPIA applies whenever identifiable personal information is processed in South Africa.

If your research involves living human participants or existing organisations, POPIA will apply if you:

- directly collect personal information from a research participant (e.g., in an interview or a survey);
- observe or monitor an identifiable research participant's behaviour;

- harvest a research participant's personal information from a publicly available source, including social media;
- reuse personal information collected for another purpose; or
- obtain personal information from another organisation.

You can see that you do not have to interact with the research participant directly for POPIA to apply. POPIA's application is much broader than the National Health Act (NHA) because it applies to all disciplines, not just health research.

Just because POPIA applies does not mean you cannot continue your research. POPIA recognises that the privacy of research participants has to be balanced against the public interest in research.

Did you know?
Considerations still apply even when observing individuals at a distance where they aren't directly identifiable. This might be less of a concern if you are in a public setting, such as a football match, where individuals generally have a lower expectation of privacy. However, if your observations are in a context where individuals have a higher expectation of privacy, such as politicians in a nightclub, and you describe them in detail that could make them identifiable, POPIA regulations will still be relevant. It's essential to assess the context and ensure that any collected information respects the privacy and consent of the data subjects involved.

Want to read more?
Section 1 of POPIA defines 'data subject' as the person to whom personal information relates.

1.5. What are the eight conditions for lawful processing that must be complied with?

1.5.1. Condition 1: Accountability

The party responsible for using personal information must show that they do so legally. They need to explain why they are collecting the personal information, how they are using it, who they are sharing it with, how they are protecting it, and how long they'll keep it.

1.5.2. Condition 2: Processing limitation

Lawfulness of processing
Personal information must be processed lawfully and reasonably without infringing the data subject's privacy rights.

Minimality
Only adequate, relevant, and non-excessive information must be processed for its intended purpose. Do not collect more information than what is necessary.

Consent, justification and objection
Processing personal information requires consent, a legal obligation, or justification. Data subjects can withdraw consent or object to processing.

Collection directly from a data subject
Personal information must be collected directly from the data subject unless they consent to collection from another source.

1.5.3. Condition 3: Purpose specification

Collection for specific purposes
Personal information must be collected for a specific, lawful purpose related to the responsible party's functions.

Retention and restriction of records
Records should not be kept longer than necessary and must be destroyed or de-identified when no longer needed.

1.5.4. Condition 4: Further processing limitation

Further processing of personal information must be compatible with the original purpose of collection, considering factors like relevance and data subject impact.

1.5.5. Condition 5: Information Quality

The responsible party must ensure that personal information is accurate, complete, and up to date in relation to its processing purpose.

1.5.6. Condition 6: Openness

Documentation
Maintain documentation of all processing activities.

Notification to the data subject when collecting personal information
Inform data subjects about the collection details and purposes before or during collection so they are informed when they consent.

1.5.7. Condition 7: Security safeguards

Security measures on integrity and confidentiality of personal information
Implement reasonable measures to protect personal information from loss, damage, or unauthorised access.

Information processed by operator or person acting under authority
Operators must process personal information only with authorisation from the responsible party and keep it confidential.

Security measures regarding information processed by operator
Ensure operators have appropriate security measures and notify the responsible party of any breaches.

Notification of security compromises

Notify the Information Regulator and affected data subjects of any personal information breaches.

Did you know?
UCT has an information security compromise response plan. You can find out more, including how to report a data breach here.

1.5.8. Condition 8: Data subject participation

Access to personal information
Data subjects can request confirmation of, access to, and details about their personal information held by the responsible party.

Correction of personal information
Data subjects may request corrections or deletions of inaccurate or outdated personal information.

Manner of access
Requests for personal information must be handled in accordance with applicable provisions ensuring reasonable access.

Want to read more?
See sections 8 to 25 of POPIA for the eight conditions of lawful processing.
For more information on exemptions, see sections 37-38 of POPIA.

Also, see the Information Regulator's guidance note on exemptions.

1.6. What does legitimate interest mean as a legal justification and how do I test it adequately?

Legitimate interest under POPIA allows an organisation to process personal information if it has a legitimate reason to do so. The legitimate interest assessment involves weighing up the purpose of the research and who will benefit from it against the interests and fundamental rights and freedoms of the research participant. It also involves assessing whether the processing is necessary (i.e. proportionate) to achieve the purpose and whether it can be achieved in a less intrusive way. It is a balancing act that can only be determined by considering certain factors.

To rely on legitimate interest, you must pass a three-part test:

Purpose:

Identify legitimate interest as one of the legal justifications for processing the personal information. The processing must have a clear and lawful purpose, such as for public health studies, social research, or historical analysis that benefits society at large.

Necessity:

Demonstrate that the processing is necessary for the legitimate interest. Consider if there's a less intrusive way to achieve the same result. If there is, then legitimate interest might not apply.

Balancing:

Weigh the university's interest against the data subject's privacy rights. Consider the nature of the personal information, the way it's being used, and the potential impact on the data subject. Special personal information which is more sensitive than personal information, for instance, would require a much stronger legal justification.

Important:
If you can confidently pass these tests, you may proceed with using legitimate interest as a legal justification for your processing purpose. However, if the tests aren't passed, you must either obtain consent or find another lawful basis for processing the personal information.

Want to read more?
See section 11 of POPIA where legitimate interest is mentioned as a legal justification.

1.7. My research data is anonymous, does that mean I don't have to worry?

If your research data is completely anonymised, you don't have to worry, but you must be sure you understand precisely what that means.

Sometimes, de-identification and anonymisation are used interchangeably, but they are different. Your research is de-identified if you remove and replace obvious personal information with less identifiable information. However, it is still possible to identify the participant by linking the information with a reasonably foreseeable method.

For example:
Researchers removed a student's name from their research but replaced it with 'Participant A.' Researchers de-identified the obvious personal information. However, it is still possible to identify the person through a reasonably foreseeable method by linking the information with a dataset. 'Participant A' is still assigned to a specific person, and who that person is, is still recorded in a dataset somewhere (coded data set).

If the data is completely anonymised, there won't be any personal information linked or way of identifying the person. All the participants will then just be called participants. No specific allocation (such as 'a' or '1') will exist, and there won't be any personal information linked to any person on any dataset.

Want to read more?
See 'Annexure A: When personal information is identifiable' in the draft ASSAf Code, which explains how to de-identify or anonymise personal information.

For guidance on anonymisation techniques, see Article 29, Data Protection Working Party opinion on Anonymisation techniques.

1.8. The identity of my research participants is masked; does POPIA still apply?

Yes, POPIA still applies even if the identity of the research participants is masked. Although using pseudonymised research data is considered a privacy-enhancing technique, POPIA requires compliance regardless of whether personal information is anonymised or pseudonymised.

There is a clear difference between personal information that once existed in your research, which is now de-identified or pseudonymised and personal information that never existed.

If personal information was once used to identify the participants, there is a possibility of re-identifying the personal information through reasonably foreseeable methods. Identifiable personal information, even if masked, will always be subject to POPIA because the likelihood of recovering the personal information exists.

1.9. Does POPIA apply to the research in the social sciences?

Yes! If you collect personal information about living human participants or existing organisations and they are identifiable, POPIA will apply. This is the case even if you do not directly interact with participants or organisations.

POPIA will also apply if you collect information from a public record, the internet, social media platforms, or an archive or reuse it for a different purpose (e.g., information about students collected during their studies). If the participants or organisations are identifiable, POPIA applies.

1.10. All my research data comes from public sources; does POPIA still apply to me?

Yes, POPIA will still apply if you collect research participants' personal information from a publicly available source because publicly available information is still subject to privacy regulations. Research participants still have a right to protect their publicly available personal information.

Want to read more?
See section 12 and 13 of POPIA for details on the collection of personal information.

2. WHAT IF MY RESEARCH EXTENDS TO ANOTHER COUNTRY?

2.1. Does POPIA apply if my research data is stored in another country?

If you conduct research and the data involves processing personal information of living human participants or existing organisations in South Africa, POPIA may apply to your research activities. This is the case even if the data is stored in another country.

POPIA can apply to organisations or individuals outside of South Africa if you process the personal information of South African research participants.

Other data privacy laws may also apply. It depends on where the processing occurs and what the agreement between you and the third party says. The agreement must specify what data protection laws apply to the processing activity. If personal information is transferred to another country, and their data protection laws are less strict than ours, additional security safeguards must be in place, such as a data sharing agreement with adequate storage and security clauses.

Want to read more?
See the draft ASSAf code 4.3.10 for transborder information flows (personal information sharing between countries).

2.2. Can I share research data with a researcher in another country?

Yes, you can, but only if certain conditions are met. The data can be transferred if the recipient in the foreign country is subject to laws, corporate rules, or agreements that ensure an adequate level of data protection similar to ours in South Africa.
Alternatively, you can share the data if the data subject consents to the transfer or if the transfer is necessary for a contract involving the data subject. If the transfer is for the benefit of the data subject and obtaining consent is impossible (you will have to prove this), the transfer can proceed, provided the data subject would likely have consented.

Want to read more?
See section 72 of POPIA.

2.3. Does POPIA apply if the research is done for a funder or research institution outside South Africa?

It will depend on where you process the personal information because other data privacy laws could also be relevant. It also depends on the terms of the agreement between the parties because they must agree on which data privacy laws apply to the processing activity.

POPIA applies to processing personal information within South Africa, so even if the funder is located outside of South Africa, as long as the processing takes place in South Africa, POPIA applies. You must assess the applicable data privacy laws in the specific jurisdiction of the processing activity and carefully review contractual terms to ensure compliance with the correct data privacy laws.

3. WHAT ARE THE CONSENT REQUIREMENTS UNDER POPIA?

Before we delve into when you need consent, let's clarify what exactly POPIA consent is. Consent is when you get clear, voluntary permission from a data subject to use their personal information. This

must be specific and informed. It means the data subject knows exactly what they're agreeing to and what you're collecting, who you're sharing it with, how long you'll keep it and for what purpose you are collecting and processing the personal information.

Important:
This is consent for processing personal information. Other types of consent, such as informed consent apply to information that is not personal information. You must refer to the National Health Act (NHA) for more information about when these types of consent are required.

3.1. Do I always need to ask for consent to process personal information in my research?

No. Consent is just one legal basis for processing personal information. You must have consent or another legal justification to process a data subject's personal information.

You can process personal information without consent if you have another legal justification such as:

- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
- processing complies with an obligation imposed by law on the responsible party;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

If you're relying on consent as a legal justification to process a data subject's personal information, you need to prove that you obtained it from them directly for that specific purpose. The data subject can withdraw their consent at any time, but this won't affect any processing you did before the withdrawal or any processing based on other legal grounds.

Want to read more?
See section 11 of POPIA.

3.2. Can a data subject change their mind after they have already given me their consent?

Yes. Data subjects have the right to withdraw their consent. If there is another legal justification for processing their personal information you can continue the processing. Remember, they can't withdraw their consent for something if you still have a legal justification to process their personal information.

For example:
If you ask them for their consent to process their personal information because you must provide them with a service according to an agreement you have with them, you already have a legal obligation to do so. You can't ask for consent for something they can't withdraw. They can't withdraw that consent because you already have a legal obligation to provide the service.

Did you know?
If you can't allow them to withdraw their consent because you have another legal justification to process their personal information, then you shouldn't have asked for their consent in the first place.

Want to read more?
See section 11(2)(b) for information about consent withdrawal and 11(3) for objection to processing.

3.3. If a data subject withdraws their consent, do I have to destroy the information I have about them?

Not necessarily. You can keep personal information only as long as needed for the purpose it was collected. You can retain it longer if required by law or if it's necessary for historical, statistical, or research purposes, provided there are safeguards in place. Once the information is no longer needed, it should be securely destroyed or de-identified.

Want to read more?
See section 14 of POPIA for retention and restriction of records.

3.4. What information about the processing must I provide the data subject when I ask for their consent?

When collecting personal information, you must inform the data subject about:
what information you're collecting and from where;

- the responsible party's name and contact details;
- the purpose of the collection;
- whether providing the information is voluntary or mandatory;
- the consequences of not providing the information;
- if the information will be transferred abroad and what protections are in place; and
- their right to withdraw their consent or object to processing.

3.5. When is it not necessary to ask for a data subject's consent for my research?

POPIA allows research to proceed without consent if it meets the legitimate interest criteria which is one of the legal justifications for processing personal information. This could be something like public health studies, social research, or historical analysis that benefits society at large.

Want to read more?
See section 27(1)(d)(i) of POPIA.

If getting consent from every data subject is nearly impossible or requires a disproportionate effort, research can proceed without it. This often applies to large-scale studies where tracking down every individual for consent would be an unreasonable burden.

Want to read more?
See section 27(1)(d)(ii) of POPIA.

Even when consent isn't required, POPIA demands that sufficient guarantees are in place to protect the privacy of the data subjects. This means that researchers must implement strong security measures to ensure that the processing of personal information doesn't invade privacy more than necessary.

Similar rules apply when the research involves children's personal information. If the research serves a public interest and obtaining consent is impractical, the study can proceed without it. Again, provided that privacy is safeguarded.

Want to read more?
See section 35(1)(d) of POPIA.

If the personal information is de-identified so that it can't be linked back to the data subject, it is not necessary to obtain consent. This is often used in large datasets for statistical or academic research.

In some cases, the Information Regulator might authorise processing without consent if it's in the public interest and safeguards are in place.

Want to read more?
See section 27(2).

POPIA does not require consent for research when it's in the public interest when consent is too difficult to obtain (it must be proven), or when strong privacy protections are in place so the personal information cannot identify the data subject. It's all about balancing the need for research with the rights of data subjects.

3.6. Do I need to obtain consent to process special personal information?

The general rule is yes, you need to obtain consent, as special personal information requires additional safeguards because of its sensitive nature.

But there are exceptions:

Legal obligations:

You don't need consent if processing special personal information is necessary to comply with a legal obligation or to exercise or defend a legal right.

Public interest:

If the processing is in the public interest and the Information Regulator gives you permission (as long as there are appropriate safeguards), you can proceed without consent.

Research, statistics, and historical purposes:

If you're using special personal information for research, statistical, or historical purposes and it's impractical to obtain consent (you must prove this), you might not need to obtain consent, as long as you've put strong privacy protections in place.

Deliberately made public:

If the data subject has deliberately made the information public themselves, then you can process it without their explicit consent.

Legitimate interests:

In situations where it's necessary to protect someone's vital interests like in a medical emergency, you can process their special personal information without consent.

Want to read more?
See sections 26-33 of POPIA for more information on special personal information.

Also, see the Information Regulator's guidance note on processing special personal information.

3.7. Do I need consent to process a child's personal information?

Yes. To process a child's personal information, you need the prior consent of a competent person, usually a parent or guardian.

A child's personal information is also considered special personal information. For the exceptions to this rule, see 'Do I need to obtain consent to process special personal information?'

Want to read more?
See sections 34 and 35 of POPIA for details involving the personal information of children.

For more information on exemptions, see sections 36-38 of POPIA.

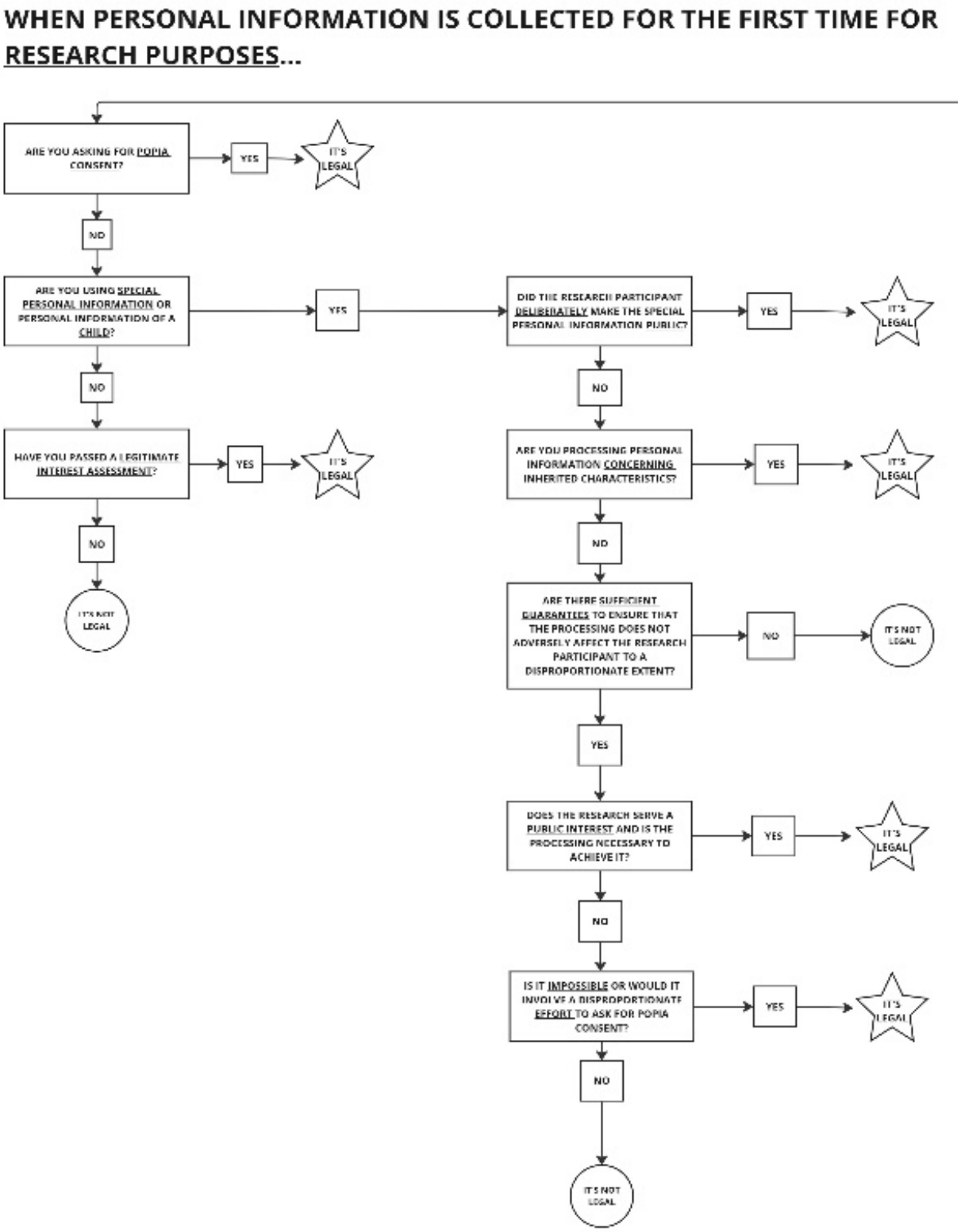
Also, see the Information Regulator's guidance note on processing personal information of children.

3.8. When do I need POPIA consent to reuse personal information?

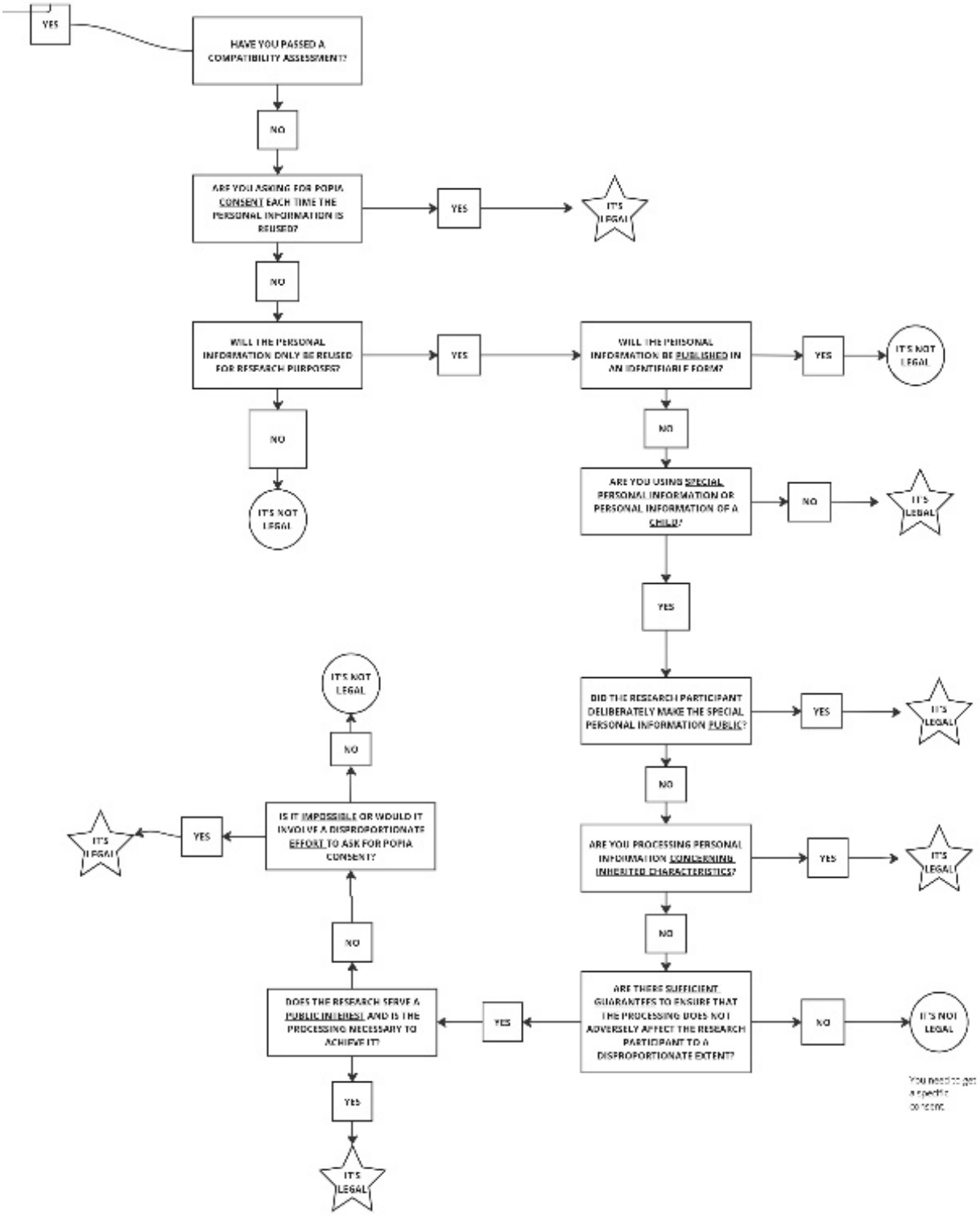
You need POPIA consent to reuse personal information when further processing is not compatible with the original purpose of collection. Section 15(3) specifies instances where consent is not required for further processing, including when the data subject consents, the information is public, processing is necessary for legal obligations, court proceedings, national security, public health or safety, or for historical/statistical research purposes that ensure non-identifiable publication.

Consent is required for incompatible purposes, indicating the importance of alignment between the original purpose of collection and the further processing purpose.

See the below flow chart to determine if your research activity is POPIA-compliant and whether you need consent to reuse personal information:



WHEN PERSONAL INFORMATION IS REUSED FOR RESEARCH PURPOSES...



4. WHAT IF POPIA APPLIES TO MY RESEARCH?

4.1. Who is responsible for POPIA compliance?

Whoever processes personal information has specific responsibilities for the lawful processing of personal information and for keeping the information secure. However, if personal information is processed under the instruction of a university or a university employs you, the university as an organisation is the responsible party. The university will then be responsible for ensuring that the personal information processing activities, including yours, comply with POPIA.

If the university does not employ you and you are an independent researcher, the accountability can shift to you instead of the university.

Who is responsible for compliance will also be discussed in research-related policies such as the Data Privacy Policy, Data Protection Policy, Information Security Policy, Research Data Management Policy, Open Access policy, Intellection Property policy, or even in the agreement between you and the university.

Want to read more?
Section 2 of the draft ASSAf Code explains how to determine who must ensure that research complies with the Code.

Also, see section 1 of POPIA and the draft ASSAf Code Glossary for defining a Responsible party. Section 8 of POPIA deals with Accountability and who must ensure conditions for lawful processing.

4.2. Does POPIA prohibit using personal information for research?

No, POPIA does not prohibit the use of personal information for research purposes. It provides guidance to assist with conducting ethical research. When processing personal information for research purposes, you must balance the public interest with the participant's privacy.

Responsible parties must ensure that processing is necessary and proportional. You must consider legal justifications for processing personal information, especially if it involves special personal information or children's information. If there isn't a legal justification for processing the information, you cannot continue processing it. POPIA explicitly says that processing special personal information is prohibited but allows for the processing for research purposes in section 27(1)(d), with restrictions.

Special personal information can be processed for research purposes if:

- the purpose for processing serves a public interest;
- processing is necessary for the specific purpose; or
- it's impossible or would involve a disproportional effort to ask for consent, but measures are in place to ensure that the processing doesn't harm the person's privacy.

You can also process special personal information if:

- you obtained the research participant's consent to do so;
- processing is necessary to comply with an obligation in law;
- the information is deliberately made public by the participant; or

- you comply with provisions in sections 28 and 33.

Want to read more?
See sections 26, 27, 28, and 38 of POPIA for more information on authorisations.
Also, see the draft ASSAf Code, 'Perform a personal information impact assessment,' to determine whether researchers can process the information for their research.

4.3. Is there a POPIA checklist?

While POPIA is principle-based, you must perform a self-assessment on your research projects to evaluate compliance, identify improvements, and determine necessary security measures.

Here is a short checklist to help ensure that your research is POPIA-compliant:

- did you consider collecting your research data anonymously?
- if anonymous research data collection is not possible, have you considered pseudonymising the identity of the research participants?
- did you complete the POPIA self-assessment?
- did you draft and submit a research data management plan?
- is everybody who has access to the research participants' personal information aware of the risks and their responsibilities towards the personal information they have access to?

Want to read more?
See 4.3 'Perform a self-assessment' in the draft ASSAf Code for a step-by-step guide on performing the assessment.

5. HOW DO I ADEQUATELY SAFEGUARD MY RESEARCH?

It depends. You must take a risk-based approach. If research is 'high risk,' then more controls are justified. You remain responsible throughout the life cycle, from when the research is still in its raw form (research in progress) to any identifiable published research data.

5.1. Who is responsible to secure research data?

It depends. It is your responsibility to keep the research data secure by keeping the personal information safe and processing it in a POPIA-compliant manner. It also depends on whose information technology infrastructure you use to process or store personal information because most of the risks are within your control.

If you use the university's information technology infrastructure:

When you use the university's information technology infrastructure, the university is responsible for implementing and maintaining secure IT systems and access control and providing guidelines and

training for you to follow so you can process personal information compliantly. Refer to internal policies such as the Information Security Management policy and additional policies on incident response procedures so you know what to do and who is responsible for what in case a data breach occurs. You can also refer to funding agreements.

If you use a third party's information technology infrastructure:

An example is when you use cloud services to store personal information. You must check the agreement for responsibility, security, or data protection clauses. The agreement must have a clause on data security to prevent a security compromise. Sometimes, it will provide a detailed list of security measures already in place.

5.2. What techniques can I use to secure my research data?

Some techniques you can use to secure your research data without incurring additional costs for yourself or the university is to:

- anonymise research data;
- use encryption when sharing research data;
- apply the minimality principle in POPIA when collecting personal information;
- use password protection and set strong, unique passwords for computers or cloud storage;
- avoid sharing passwords and change them regularly;
- restrict access to research data;
- store physical research data in locked cabinets or secure areas;
- backup regularly;
- install and regularly update antivirus and anti-malware software on devices;
- use secure deletion methods to ensure research data cannot be recovered;
- avoid using insecure or unapproved tools or software for sharing research data; and
- not leave research data unattended on desks.

Want to read more?
For more tips on securing research data, see the University of Colorado Springs' Research Data Management suggested best practices and visit the University of Oxford's website.

Also, see sections 19 – 22 of POPIA.

5.3. How can I pseudonymise my research data?

To pseudonymise research data as a privacy-enhancing technique, you can:

- remove and replace all identifiable information from your research;
- create artificial identifiers (pseudonyms) to replace the identifiable information that cannot be linked back to the research participants;
- implement measures to prevent the linkage of pseudonymised research data with external datasets; or
- regularly review and update the pseudonyms to add an extra layer of protection.

Want to read more?
It is important to remember that anonymisation and pseudonymisation are different even though there is a comparison between these resources.

See anonymisation and pseudonymisation techniques on the University of Edinburgh's website, KU Leuven and University College London.

For more guidance on anonymisation techniques, see Article 29, Data Protection Working Party opinion on Anonymisation techniques and the ICO Code of Practice on anonymisation.

5.4. I want to give open access to my research data. Is that POPIA compliant?

It depends on the content of the research data you want to give open access to. You can't provide open access if it contains children's personal information, special personal information, or personal information considered high risk. Regardless, you must still ensure that the processing complies with POPIA.

There are certain things you can do to ensure compliance even if you give open access, such as:

- only include necessary personal information and comply with the minimisation rule in POPIA;
- ensure the personal information you collect is obtained lawfully;
- consider anonymising or pseudonymising personal information in the research data to reduce the risk of identification; or
- use encryption, access controls, and regular security assessments.

Want to read more?
See 3.2 'Does POPIA prohibit the use of personal information' above, and section 26 of POPIA.

5.5. Is it POPIA-compliant to publish research data for reuse in a repository?

If you see the word 'reuse,' you must immediately consider further processing. When personal information is collected and used for one purpose but reused for another, it is called 'further processing. 'Publishing research data in a repository would be further processing.

If the personal information is published for reuse, it is not collected directly from the research participant, which is only allowed in certain circumstances.

POPIA also allows for the reuse of personal information for research purposes without consent if the personal information will:

- only be used for research purposes; and
- not be published in an identifiable form.

If not identifiable, research data can be published for reuse in a repository, so the research data must be pseudonymised entirely.

Want to read more?
See the draft ASSAf Code, 4.3.4, for Further processing limitations (secondary use)

Also, see section 15 of POPIA for further processing limitation.

5.6. Why must I secure personal information even if I collect it from a public record (e.g., an archive) or the internet?

Keeping personal information secure, even if obtained from a public record, is essential due to the increased risk and potential for harm associated with gathering information from various online sources. This is also known as aggregate information.

For example:
Suppose you have some personal information about a person from Facebook and some from LinkedIn. Individually, these pieces of information might not reveal much, but if you combine them, you could end up with information that can potentially cause harm to a person's privacy. Combined information could be more valuable to someone with malicious intent, who might use it against your research participant.

Want to read more?
See the International Association of Privacy Professionals' article on how Aggregated data provides a false sense of security.

For more information on the direct collection rule, see Table 7 of the draft ASSAf Code.

Also, here is a real-life example of how a person was identified through aggregate data.

6. WHAT HAPPENS IF MY RESEARCH IS NON-COMPLIANT?

When research is non-compliant, it not only harms the university and significantly affects funding and reputation but also harms the researcher and other researchers' reputations at the university and animal and human participants.

6.1. What are examples of POPIA non-compliance?

Examples of non-compliance with POPIA can include:

- lost or stolen research data;
- not backing up research data or not regularly checking that the information can be retrieved from the backup;
- accidentally or deliberately sending personal information or research data to unauthorised users;
- not de-identifying personal information when it is possible to de-identify the information;
- when there is no access control and unauthorised users gain access to research data;
- not obtaining the necessary consent; and
- not having sufficient systems in place to prevent breaches from occurring.

6.2. What is the potential harm to research participants?

Research participants might face problems different from those of the university and other stakeholders because they are directly affected by your actions. Understanding these potential challenges is essential for ensuring ethical and responsible research practices.

Examples of potential harm research participants could face include:

- loss of trust;
- emotional distress;
- embarrassment;
- financial costs;
- physical discomfort;
- loss of time;
- physical harm;
- loss of privacy;
- unforeseen side effects; and
- psychological harm.

6.3. What are the consequences of POPIA non-compliance?

The consequences will depend on the severity of events leading to non-compliance, but consequences can include:

- administrative fines;
- compensation claims for damages;
- harm to your academic reputation and other researchers at the university;
- reputational damage to the university;
- failure to create or utilise valuable intellectual property;
- lost or wasted funding;
- wasted time and resources;
- fines and lawsuits;
- physical and mental anguish; and
- disciplinary action.

6.4. What must I do if I have a security compromise?

You must check who the responsible party is in the processing activity and notify them of the breach in the event of an unauthorised person accessing or acquiring personal information. Contact CSIRT at UCT.

If you are the responsible party, you must notify the Information Regulator and affected data subjects in the prescribed manner,

Want to read more?
See section 22 of POPIA for information about how and when to notify the Information Regulator or data subjects when a security compromise occurs.

Also, see the Information Regulator's notice published on their website, discussing section 22 of the Act in more detail here.

7. WHAT IS THE ASSAF CODE OF CONDUCT FOR RESEARCH?

The Academy of Science of South Africa (ASSAf) developed a Code of Conduct that governs the protection of personal information by institutions that are members of ASSAF in compliance with POPIA and the Academy of Science of South Africa Act, 67 of 2001.

Want to read more?
See Chapter 7, sections 60-68 of POPIA on 'Codes of conduct in POPIA'.

7.1. What is the status of the Code?

The ASSAf Code is being converted into a POPIA Compliance Framework. Following feedback from the Information Regulator, ASSAf decided to transform the Code into a voluntary POPIA Compliance Framework. This framework will likely serve as industry best practice and may be considered by the Regulator when assessing compliance with POPIA in the research context.
The transition to a voluntary framework means that researchers and research institutions can voluntarily agree to be bound by its provisions. ASSAf seeks to facilitate further discussion and collaboration with stakeholders through webinars and ongoing communication.

Considering the Code was not accredited, and the Framework is still in the draft phase, you must remember that you remain subject to POPIA, and failure to comply will result in serious consequences. Once the Framework is available and published, we will update any reference to the Draft ASSAf code, in this FAQ.

Want to read more?
Visit ASSAf's website to read 'ASSAf Communication to Stakeholders regarding the Framework'- published February 2024, under the Notifications and Documents heading.

Also see Chapter 10 of POPIA, which deals with enforcement notices, which is one of the serious consequences of non-compliance with POPIA.

8. ATTRIBUTION AND ACKNOWLEDGEMENT

This FAQ was developed by Novation Consulting for the UCT Research Data Protection Working Group (RDPWG) and the UCT community of researchers.

The FAQ was formatted to align with UCT style guidelines by the UCT Office of Research Integrity.