WERKSMANS
ATTORNEYS

06 October 2026

PRIVACY POLICY

KULULEKO NPC

Date: 06 October 2026

Version: 1.0

The Central 96 Rivonia Road
Sandton 2196 Johannesburg South Africa
Private Bag 10015 Sandton 2146

Docex 111 Sandton
Tel +27 11 535 8000

www.werksmans.com

TABLE OF CONTENTS

1 INTRODUCTION AND IDENTITY OF THE RESPONSIBLE PARTY 1
2 ABOUT KULULEKO NPC AND OUR PROJECTS 2
3 PERSONAL INFORMATION WE PROCESS ACROSS OUR ACTIVITIES 2
4 TAPP: DRONE AND CCTV SAFETY PROJECT 4
5 CATEGORIES OF PERSONAL INFORMATION COLLECTED BY TAPP 6
6 WHY TAPP PROCESSES PERSONAL INFORMATION 8
7 TAPP'S LAWFUL BASIS FOR PROCESSING 9
8 HOW TAPP LIMITS COLLECTION AND USE 10
9 AUTOMATED PROCESSING AND HUMAN REVIEW 11
10 SHARING OF PERSONAL INFORMATION 12
11 TRANSBORDER INFORMATION FLOWS 13
12 HOW LONG WE KEEP PERSONAL INFORMATION 14
13 HOW WE PROTECT YOUR INFORMATION 15
14 CHILDREN AND VULNERABLE PERSONS 16
15 YOUR RIGHTS UNDER POPIA 17
16 COMMUNITY TRANSPARENCY AND ENGAGEMENT 19
17 WHAT HAPPENS IF THERE IS A DATA BREACH 20
18 CONTACT AND COMPLAINTS 20
19 REVIEW AND UPDATES 21

PRIVACY POLICY

1 INTRODUCTION AND IDENTITY OF THE RESPONSIBLE PARTY

1.1 This Privacy Policy (the "**Policy**") explains how Kululeko NPC ("**Kululeko**", "**we**", "**us**" or "**our**") collects, uses, stores and shares personal information across all of its projects and activities, including every project it runs now or in future, and its websites.

1.2 Kululeko NPC (registration number 2025/793334/08) is a non-profit company and the responsible party under POPIA for all personal information processed through its projects. This means Kululeko decides why and how personal information is collected, how it is used, and is responsible for protecting it.

1.3 This Policy tells you: what information we collect; why we collect it; how we use it; who we share it with; how long we keep it; how we protect it; what rights you have; and how to contact us.

1.4 Information Officer

1.4.1 An Information Officer and a Deputy Information Officer have been designated and registered with the Information Regulator in accordance with POPIA. The Information Officer is responsible for ensuring compliance with POPIA and for handling requests from community members about their personal information.

1.4.2 Contact details:

Detail	Contact
Information Officer	Heidi Botha
Deputy Information Officer	Robert Stephen Nienaber
Email	info@kululeko.org
Postal Address	8 Bird Street, Stellenbosch, 7600
Physical Address	8 Bird Street, Stellenbosch, 7600

2 ABOUT KULULEKO NPC AND OUR PROJECTS

Kululeko works to reduce inequality in South Africa by helping to unlock the township economy. We start by understanding what is holding township communities back, and we respond through a growing number of projects. This Policy applies to all of our projects, including any we start after it is published. Our current projects are:

2.1.1 TAPP: a community safety project that uses drones, CCTV cameras, wearable panic devices and an operations centre. Sections 4 to 9 explain how TAPP processes personal information.

2.1.2 Sakhisizwe: our grassroots community engagement arm. Sakhisizwe works directly with communities through door to door engagement, dialogue circles, community surveys and research, together with volunteers, community champions and partners.

2.1.3 BEE3: a project that proposes a simpler, voluntary alternative to B-BBEE compliance.

2.2 Kululeko also processes personal information in the ordinary course of running a non-profit company, including about its employees, directors, job applicants, volunteers, donors, funders, partners, suppliers and visitors to its websites.

3 PERSONAL INFORMATION WE PROCESS ACROSS OUR ACTIVITIES

3.1 Community engagement through Sakhisizwe

3.1.1 When we engage with communities through door to door conversations, dialogue circles, community surveys and research, we may collect your name and contact details if you choose to give them, your age group and the area you live in, your views, experiences and ideas and, where you choose to share it, information about safety incidents in your area.

3.1.2 You can take part in our surveys and dialogue circles without giving your name. We publish research findings only in anonymised or aggregated form, so that no individual can be identified.

3.1.3 If you share information about your health, religion, political views or experience of crime, we treat it as special personal information. We only process it with your consent, or where another ground in section 27 of POPIA applies. Answering questions is always optional.

3.1.4 We only use photographs or video in which you can be identified with your consent or where another lawful ground can be established and, for children, with the consent of a parent or guardian or where another ground has been provided for in terms of legislation.

3.1.5 We do not include anyone under 18 in surveys or dialogue circles without the prior consent of a parent or guardian.

3.2 Volunteers, community champions, employees and job applicants

We process identity and contact details, CVs, qualifications, references, banking and tax details and, where the law allows and it is relevant to the role, background checks. We use this to recruit, manage and pay people and to meet our legal obligations as an employer.

3.3 Donors, funders, partners and suppliers

We process the names and contact details of individuals and organisation representatives, banking and tax details, agreements and correspondence, to receive and acknowledge donations, issue tax certificates where applicable, report to funders, and manage our relationships with partners and suppliers.

3.4 Our websites

When you use our websites, including kululeko.org, tapp.org.za and sakhisizwe.org.za, we process information you submit through contact or sign-up forms, and technical information such as your IP address, browser type and the pages you visit, some of which is collected through cookies. We ask for your consent before using non-essential cookies such as analytics. If you contact or follow us on LinkedIn, Instagram or Facebook, that platform also processes your information under its own policies.

3.5 Our lawful basis

3.5.1 We process information because you have consented, because it is necessary to conclude or perform a contract with you, because the law requires it, or because it is necessary for our legitimate interests as a non-profit organisation, as permitted by section 11 of POPIA.

3.5.2 Giving us your information is voluntary in most cases. Some information is required, for example payroll information for employees and the details needed to issue a tax certificate. If you do not give us information that is required, we may not be able to employ you, issue a certificate or register you for a panic device.

3.5.3 Some of the information we collect is required or authorised by law, including the Income Tax Act 58 of 1962, the Tax Administration Act 28 of 2011, the Basic Conditions of Employment Act 75 of 1997, the Unemployment Insurance Act 63 of 2001 and the Civil Aviation Regulations.

3.5.4 We usually collect information directly from you. Sometimes we receive it from others, for example incident reports from community members, SAPS case numbers, and various partners..

3.6 Newsletters and direct marketing

We will only send you newsletters, donation requests or other direct marketing by email, SMS, WhatsApp or telephone if you have agreed to receive them. Every message will tell you who it is from and give you a free way to opt out, and you can also opt out at any time by contacting the Information Officer.

4 TAPP: DRONE AND CCTV SAFETY PROJECT

4.1 TAPP is Kululeko's community safety project.

4.2 TAPP uses drones on patrol over defined areas and fixed CCTV cameras installed at viable locations on the peripheral boundary of areas.

4.3 **Routine Patrol: No Recording**

During routine patrol (**"Drones on Patrol"**), the drones observe the area but do not record, store or transmit any video, audio or other personal information. No personal information is captured during routine patrol.

4.4 **Trigger Event Capture**

4.4.1 Data collection happens only when a documented Trigger event occurs, for example, a reported crime, a detected threat, or an emergency requiring response. When a Trigger event is triggered, TAPP may capture live video, still images, audio, thermal and night-vision imagery, geolocation data, timestamps, movement patterns, vehicle information, behavioural indicators.

4.4.2 A triggered event may result in drone dispatch to the location, armed security response, and reporting to the South African Police Service (**"SAPS"**), local law enforcement, medical, fire and disaster-management responders. This depends on the specific situation.

4.5 **Complementary Use of Drones and CCTV**

4.5.1 CCTV cameras are, or will be, installed at viable locations on the peripheral boundary of an area. CCTV provides fixed-point monitoring of the boundary perimeter and immediate surrounds.

4.5.2 The two technologies are complementary: CCTV covers the peripheral boundary of the area, while drones remain necessary to cover the dense interior settlement. The areas where TAPP is operational are known to be dense, semi-informal settlements with closely packed structures, narrow and unpaved pathways, irregular street patterns and limited infrastructure. Across much of the interior, fixed mounting points, cabling, power supply and line-of-sight arrangements are impracticable. Drones provide effective coverage in the environment and remain necessary because of environmental constraints and the physical threats that security personnel may face.

4.6 CCTV Camera Operation

CCTV cameras are installed at fixed positions on the peripheral boundary of operational areas. They capture motion-triggered video footage of the boundary area and immediate surrounds. CCTV footage is transmitted to and monitored from an operations centre. CCTV cameras may also capture still images, location-specific imagery and metadata, including timestamps and camera identifiers.

4.7 Wearable Panic Devices and Gunshot Detection

If you register for a wearable panic device, TAPP collects your name, contact details and address and, when you press the button, your location, so that it can send help. Gunshot detection sensors listen for the sound of gunshots so that TAPP can respond quickly.

4.8 Facial Recognition

TAPP does not currently use facial recognition.

4.9 Drone Operations

TAPP's drones will only be flown by remote pilots licensed by the South African Civil Aviation Authority, under an operator certificate issued in terms of Part 101 of the Civil Aviation Regulations. Drones are set up so that they do not look into homes or private yards.

5 CATEGORIES OF PERSONAL INFORMATION COLLECTED BY TAPP

The type of personal information collected depends on whether the drones are on routine patrol, responding to a Trigger event, or whether the information is captured by CCTV cameras.

5.1 Routine Patrol

During routine patrol, the drones observe the area from the air. No video, audio, images or other personal information is recorded, stored or transmitted.

5.2 Trigger event Capture

When a Trigger event is triggered, TAPP may collect and process the categories of personal information:

Category	Description
Video and images	Live video footage, recorded video and still photographs captured by drone cameras during a Trigger event.
Audio recordings	Sound captured by drone microphones where necessary and proportionate to the Trigger event.
Thermal and night-vision imagery	Infrared and low-light imagery used for detection and response during Trigger events.
Location and movement data	Geolocation coordinates, timestamps and movement patterns of persons and vehicles within the affected area.
Vehicle information (ANPR)	Vehicle registration plate data, vehicle images and driver images captured during Trigger events and checked against NAVIC.
Biometric information (FRT)	If facial recognition is introduced in future, facial images will be captured only where trigger criteria are met during a Trigger event, and only once any prior authorisation required by POPIA has been obtained.
Behavioural and object-recognition data	Automated indicators of suspicious behaviour, loitering, unusual movement, crowding, trespass or intrusion; objects and hazards detected.
Metadata and incident logs	Technical data about the capture (device identifiers, flight logs, operator actions, system timestamps).

5.3 CCTV Footage

CCTV cameras capture video footage on a motion-triggered basis. Categories of personal information that may be collected via CCTV include: video and still images of persons and vehicles in or near the boundary area; vehicle registration plates (where ANPR-enabled); location-specific imagery linked to a fixed camera position; timestamps and camera identifiers; and movement patterns within the camera's field of view. CCTV footage may also incidentally capture special personal information, such as race or ethnic origin visible in imagery.

5.4 Special Personal Information

5.4.1 Some of the information collected during Trigger events may constitute special personal information under POPIA, including:

5.4.1.1 biometric information (facial images and recognition templates);

5.4.1.2 race or ethnic origin, if incidentally revealed in footage;

5.4.1.3 criminal behaviour data, where footage relates to suspected offences.

5.4.2 TAPP processes special personal information only where permitted by law and subject to additional safeguards described in this Policy.

5.5 Children and Vulnerable Persons

Children and vulnerable persons may be incidentally captured in footage during Trigger events. TAPP applies systematic redaction and blurring safeguards to protect their identity. No Facial Recognition Technology is applied to children.

6 WHY TAPP PROCESSES PERSONAL INFORMATION

6.1 POPIA requires that personal information may only be collected for specific, explicitly defined and lawful purposes. The table below sets out the specific purposes for each processing activity under TAPP.

Processing Activity	Purpose
Routine patrol	Deterrence and situational awareness. No personal information is recorded or stored.
CCTV boundary monitoring	Motion-triggered monitoring of the peripheral boundary of an area; deterrence; detection of and response to Trigger events; preservation of evidence; support to SAPS and emergency services.
Incident-triggered capture (video, stills, audio, thermal)	Respond to Trigger events; protect life and property; preserve evidence for investigation; assist emergency response.
ANPR	Identify vehicles of interest linked to Trigger events; assist with stolen vehicle recovery; support SAPS investigations.

Processing Activity	Purpose
Facial Recognition Technology (in future) / biometric identification	Identify persons involved in defined Trigger events where FRT trigger criteria are met; support law enforcement investigations.
Audio recording	Provide situational and evidential context where necessary and proportionate to the Trigger event.
Object recognition	Identify objects or hazards linked to Trigger events (e.g. weapons, abandoned items).
Behavioural analytics	Preliminary identification of suspicious activity, subject to mandatory Human Review before any action is taken.
SAPS/NAVIC disclosure	Report verified incidents and match results to SAPS; preserve evidence for criminal proceedings.
Retention and logging	Accountability, audit, dispute resolution, regulatory compliance.

6.2 Personal information is not used for any purpose other than those set out above. TAPP does not sell personal information, use it for marketing, or share it for commercial purposes unrelated to community safety.

7 TAPP'S LAWFUL BASIS FOR PROCESSING

POPIA requires that personal information may only be processed if there is a lawful reason.

7.1 Ordinary Personal Information

7.1.1 TAPP processes ordinary personal information under section 11(1)(f) of POPIA, which permits processing where it is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

7.1.2 In plain language, this means Kululeko has assessed that TAPP's purposes, community safety, crime prevention, protecting life and property, preserving evidence and assisting law enforcement, are legitimate interests that justify the collection and use of personal information, and that these interests are not overridden by the privacy rights of individuals in the community.

7.2 **Special Personal Information, Biometric Data and Criminal Behaviour Data**

7.2.1 POPIA generally prohibits the processing of special personal information, biometric information and criminal behaviour information unless a specific exemption applies.

7.2.2 TAPP relies on the following legal conditions for processing these categories:

7.2.2.1 Biometric information: processed where necessary for identification purposes in connection with a Trigger event, with appropriate safeguards including human review, access restrictions and automated deletion.

7.2.2.2 Criminal behaviour data: processed where necessary for establishing, exercising or defending a right or obligation in law, including the reporting of suspected criminal activity to SAPS.

7.2.2.3 Race or ethnic origin: not deliberately collected; where incidentally captured, subject to the same safeguards and retention limits as other footage.

7.2.3 Where POPIA requires prior authorisation from the Information Regulator, TAPP will not carry out that processing until authorisation has been granted.

7.3 **Children's Personal Information**

Where children's personal information is incidentally captured during Trigger events, processing takes place only where section 35 of POPIA permits it, for example where it has been deliberately made public or if necessary to establish, exercise or defend a right or obligation in law. TAPP applies additional safeguards including systematic redaction, restricted access and no Facial Recognition Technology application to children.

8 HOW TAPP LIMITS COLLECTION AND USE

8.1 POPIA requires that personal information collected must be adequate, relevant and not excessive. TAPP applies the following measures to minimise the personal information collected and the way it is used:

8.1.1 No recording during routine patrol: drones observe but do not capture or store personal information unless a Trigger event is triggered.

8.1.2 Trigger-only capture: data collection begins only when a documented Trigger event occurs.

8.1.3 Geofencing and exclusion zones: TAPP applies geographic restrictions to prevent capture in sensitive areas.

8.1.4 Privacy masking: where technically feasible, areas not relevant to a Trigger event are masked or excluded from capture.

8.1.5 No continuous audio recording: audio is captured only in connection with specific Trigger events and only where necessary and proportionate.

8.1.6 FRT is activated only when defined trigger criteria are met during a Trigger event.

8.1.7 Vendor and operator restrictions: third-party service providers may only process personal information in accordance with written agreements and instructions.

8.2 Personal information is not used for marketing, profiling for commercial purposes, political monitoring, or any purpose unrelated to community safety.

9 AUTOMATED PROCESSING AND HUMAN REVIEW

TAPP uses certain automated technologies to assist in detecting and responding to Trigger events.

9.1 Automated Technologies Used

The following automated technologies may be used during Trigger events:

9.1.1 ANPR: automatically reads vehicle registration plates and checks them against the NAVIC database.

9.1.2 FRT, if introduced in future: will generate facial recognition templates for comparison against defined watchlists.

9.1.3 Behavioural analytics: identifies patterns such as suspicious movement, loitering, crowding or trespass.

9.1.4 Object recognition: identifies objects or hazards (such as weapons or abandoned items).

9.2 **Human Review Requirement**

9.3 All automated outputs are preliminary leads only. A trained Operations centre operator must review every automated output before any action affecting a person is taken. This means:

9.3.1 No report to SAPS or other authority is made solely on the basis of an automated output.

9.3.2 No security response is dispatched solely on the basis of an automated output.

9.3.3 ANPR match results are verified by a human operator before any further action; all results are subject to documented human review.

9.3.4 FRT match results are verified by a human operator before any identification is acted upon.

9.3.5 False positives are logged, reviewed and used to improve system accuracy.

9.4 You have the right to raise concerns about automated processing or to object on reasonable grounds. See section 15 of this Policy.

10 SHARING OF PERSONAL INFORMATION

10.1 We share personal information only where necessary. For TAPP, the recipients are set out below.

Recipient	Purpose and Basis	Safeguards
Operations centre operators	Monitoring, response and human review of Trigger events.	Role-based access; training; confidentiality obligations.
Data centre service provider	Hosting and storage of TAPP data in South Africa.	Written operator agreement; access restrictions; encryption.
SAPS / NAVIC	Verified incident reporting; stolen vehicle match confirmation; evidence for criminal proceedings.	Data-sharing agreement; human review before any disclosure; purpose limitation.
Local law enforcement and emergency responders	Emergency response where life, safety or property is at immediate risk.	Disclosed only where necessary; limited to information relevant to the emergency.
Other operators (processors)	Technical support, maintenance and analytics under Kululeko's instructions.	Written operator agreements.

10.2 For our other activities, we may share personal information with service providers who support us, such as IT, email, payroll, banking and audit providers, under written agreements; with funders and partners, but only in anonymised or aggregated form unless you have agreed otherwise; and with authorities where the law requires it.

10.3 We do not sell, rent or trade personal information. Personal information is not disclosed for marketing, commercial profiling or any purpose unrelated to our projects.

10.4 TAPP does not make bulk disclosures of personal information. Disclosure is limited to specific, verified incidents.

11 TRANSBORDER INFORMATION FLOWS

11.1 All TAPP data is hosted in South Africa in secure data centres. There are no transborder flows of personal information under TAPP.

11.2 Should we need to transfer personal information outside South Africa in the future, it will:

11.2.1 Obtain Information Officer and board of Kululeko NPC approval before any transfer.

11.2.2 Assess the transfer against the requirements of POPIA section 72 (including whether the recipient country has adequate data protection laws or whether the data subject has consented).

11.2.3 Put in place appropriate contractual safeguards.

11.2.4 Update this Policy to inform the community.

12 HOW LONG WE KEEP PERSONAL INFORMATION

POPIA requires that personal information must not be kept for longer than is necessary for the purpose for which it was collected. When the purpose has been achieved, the information must be deleted, destroyed or de-identified in a manner that prevents reconstruction.

12.1 Retention Periods

For TAPP, the following table sets out how long different types of personal information are kept:

Type of Information	Retention Period	What Happens After
Routine patrol data	No data captured	Not applicable, no personal information is recorded during routine patrol
CCTV footage (routine / non-incident)	30 days from capture	Automatically deleted unless the Information Officer approves an extension for an active investigation, complaint, claim or legal obligation. Where CCTV footage relates to a Trigger event, the incident-triggered retention period applies instead.
Incident-triggered footage (video, stills, audio, thermal, analytics)	120 days from capture	Automatically deleted unless the Information Officer approves an extension for an active investigation, complaint, claim or legal obligation.
ANPR records and match results	48 hours for SAPS confirmation	Automatically deleted after 48 hours unless lawful extension is approved by the Information Officer.
FRT non-match templates	Immediately deleted	Deleted automatically upon determination of no match

Type of Information	Retention Period	What Happens After
FRT confirmed match records	Duration of active investigation	Retained only for the period of the investigation, with Information Officer approval
Human review records	Investigation period plus 12 months	Deleted after the extended period unless required for ongoing legal proceedings
SAPS/NAVIC disclosure records and audit trail	5 years	Deleted or de-identified after 5 years unless required by law.
Audit, access and deletion logs	5 years	Deleted or de-identified after 5 years

For our other activities, we keep personal information only for as long as we need it for the purpose it was collected, or for as long as the law requires, for example tax and employment records. We anonymise community survey responses once they have been analysed.

12.2 **Deletion Safeguards**

12.2.1 Deletion is automated where possible. Manual override of automated deletion is prohibited without written Information Officer approval and documented justification.

12.2.2 Deletion certificates are generated to confirm that personal information has been destroyed in a manner that prevents reconstruction.

12.2.3 Where personal information is retained beyond the standard periods (for example, for an ongoing investigation), the reason for retention must be documented and the retention must be reviewed regularly.

13 HOW WE PROTECT YOUR INFORMATION

13.1 POPIA requires us to take appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised access to personal information.

13.2 The following safeguards are in place:

Safeguard	Description
Encryption	All personal information is encrypted in transit and at rest.
Access control	Role-based access ensures that only authorised personnel can access personal information, based on their specific role and need.
Multi-factor authentication	All access to our systems requires multi-factor authentication.
Segregation of duties	Different personnel handle different aspects of data processing to prevent any single person having unrestricted access.
Audit logging	Tamper-evident logs record all access to and actions on personal information, including who accessed it, when and why.
Export restrictions	Personal information cannot be copied, downloaded or exported from our systems without authorisation.
Testing and monitoring	Regular penetration testing, vulnerability scanning, security patching and continuous monitoring.
Staff training	All personnel with access to personal information receive data protection and security training.
Privacy masking and geofencing	Technical measures to limit capture to relevant areas and to mask areas not related to a Trigger event.
Vendor contracts	Third-party operators are bound by written agreements that require equivalent security measures.

13.3 We will regularly review and update our security measures to respond to new threats and to comply with best practice.

14 CHILDREN AND VULNERABLE PERSONS

14.1 We recognise that children and vulnerable persons require additional protection.

14.2 The following additional safeguards apply:

14.2.1 Children may be incidentally captured in footage during Trigger events. We do not deliberately target children for surveillance.

14.2.2 Systematic redaction and blurring protocols are applied to protect the identity of children in footage.

14.2.3 FRT is not applied to children.

14.2.4 Access to footage containing children is restricted to the minimum number of authorised personnel necessary.

14.2.5 Disclosure of footage containing children is subject to additional review and approval by the Information Officer.

14.2.6 Requests involving a child's personal information must be made by a competent person (parent, guardian or other person with legal authority) and are handled directly by the Information Officer (POPIA s 35: a competent person must act in the best interests of the child).

14.3 Vulnerable persons, including elderly persons and persons with disabilities, are treated with equivalent care and additional safeguards where appropriate.

15 YOUR RIGHTS UNDER POPIA

POPIA gives you important rights over your personal information. This section explains what those rights are and how to exercise them.

15.1 Your Rights

Right	What This Means
Right to be notified	You have the right to be told that your personal information is being collected, why it is being collected, and who is collecting it. This Policy is part of how we meet this obligation.
Right of access	You can ask for a copy of the personal information we hold about you.
Right to correction	If your personal information is inaccurate, incomplete, misleading or not up to date, you can ask to correct or complete it.
Right to deletion or destruction	You can ask to delete or destroy your personal information if it is no longer needed for the purpose for which it was collected, or if we are no longer authorised to keep it.
Right to object	You can object, on reasonable grounds, to the processing of your personal information. If you object, we may no longer process it, unless the law allows us to continue.
Right not to be subject to solely	You have the right not to be subject to a decision that produces legal effects or significantly affects you if that decision is based

Right	What This Means
automated decisions	solely on automated processing. As explained in section 9 of this Policy, we do not make solely automated decisions.

15.2 **How to Exercise Your Rights**

To make a request about your personal information, contact the Information Officer using any of the following methods:

Method	Details
Email	info@kululeko.org
Web / QR portal	www.kululeko.org
In person	8 Bird Street, Stellenbosch, 7600
Post	8 Bird Street, Stellenbosch, 7600

Making a request, objection or correction is free. You can use the forms attached to our PAIA Manual (Form 1 for objections and Form 2 for correction or deletion), or any other written or recorded request that gives us the same information. We will tell you the outcome of a correction or deletion request within 30 days. Requests for access to other records are dealt with under our PAIA Manual, available at www.kululeko.org.

15.3 **What to Include in a Footage Request**

15.3.1 If you are requesting access to footage that may contain your image, please provide:

15.3.1.1 The date and approximate time of the incident or period in question.

15.3.1.2 The location within the area (as precisely as possible).

15.3.1.3 A description of what you were doing or wearing, to help identify relevant footage.

15.3.1.4 Proof of your identity (such as a copy of your identity document).

15.3.2 If you are requesting access to CCTV footage specifically, please also indicate the approximate location along the boundary perimeter and the direction from

which you approached or were present, as this will help identify the relevant camera and footage.

15.3.3 We will acknowledge your request within 5 business days and respond within the period required by POPIA. Where footage contains images of other persons, those persons' images will be redacted before the footage is provided to you.

16 COMMUNITY TRANSPARENCY AND ENGAGEMENT

16.1 We are committed to being transparent with the area and community about TAPP and how personal information is handled.

16.2 The following measures are in place:

16.2.1 Signage at entry points and key locations within the TAPP area, notifying people that both drone patrol and CCTV monitoring are in operation.

16.2.2 QR codes on signage linking to this Policy and to the contact details of the Information Officer.

16.2.3 Our websites, with information about TAPP, this Policy and how to exercise your rights.

16.2.4 This Policy and key information are available in English and in the other languages spoken in the communities where we work.

16.2.5 Community meetings and engagement sessions with residents, community leaders, ward councillors and local organisations.

16.2.6 Annual anonymised reporting on TAPP's operations, including the number and types of Trigger events, data subject requests received and complaint outcomes.

16.3 We welcome questions and feedback from community members. You do not need to make a formal request to ask a question about our work.

17 WHAT HAPPENS IF THERE IS A DATA BREACH

17.1 A Security Compromise (data breach) occurs when personal information is accidentally or unlawfully accessed, lost, destroyed, altered or disclosed to an unauthorised person.

17.2 If we have reasonable grounds to believe that a Security Compromise has occurred, we will:

17.2.1 Notify the Information Regulator as soon as reasonably possible, through the Regulator's eServices portal.

17.2.2 Notify affected data subjects (you) as soon as reasonably possible, unless a law enforcement authority or the Information Regulator directs a delay.

17.2.3 Inform you of the possible consequences, the measures we are taking, and what you can do to protect yourself, and, if known, who accessed your information.

17.3 Notification may be provided by email, SMS, post, public notice or through our websites, depending on the circumstances.

17.4 Kululeko maintains a detailed Incident Response Plan that governs how breaches are detected, contained, investigated, reported and reviewed.

18 CONTACT AND COMPLAINTS

18.1 Contact us

If you have any questions about this Policy, our projects, or your personal information, please contact the Information Officer.

18.2 Complaints

18.2.1 If you believe that your personal information has been misused, or that we have not complied with POPIA, you may:

18.2.1.1 Complain to us by contacting the Information Officer. We will acknowledge your complaint within 5 business days and investigate it.

18.2.1.2 Complain directly to the Information Regulator. You do not need to complain to us first, but we encourage you to raise concerns with the Information Officer so that they can be addressed promptly.

18.2.2 You may lodge a complaint with the Information Regulator (South Africa), which details are as follows -

- Information Regulator: Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191
- Email: enquiries@inforegulator.org.za or POPIAComplaints@inforegulator.org.za for POPIA complaints
- Telephone: 010 023 5200 or Toll free 0800 017 160.
- Postal address: P.O. Box 31533, Braamfontein, Johannesburg, 2017
- Website: www.inforegulator.org.za

19 REVIEW AND UPDATES

19.1 This Policy will be reviewed at least once a year, or sooner if any of the following occur:

19.1.1 A material change in our processing activities or technology.

19.1.2 A new category of recipient or data sharing arrangement.

19.1.3 An expanded purpose, geographic coverage or surveillance capability.

19.1.4 A change in applicable law or regulatory guidance.

19.2 When material changes are made, we will notify the community through our websites, updated signage and QR codes, and community communication where appropriate.