Vetting Information

6/2026

Contact us

Telephone: +27 83 381 6428

Email: esme@healthcarenavigator.co.za

Website: www. healthcarenavigator.co.za

What you should know…

- The Enforcement Notice imposed by the Information Regulator outlines several violations committed by Central Johannesburg TVET College regarding the Protection of Personal Information Act (POPIA).
- The College, among others, unlawfully shared employee background check reports and failed to officially register its Information Officer or report the resulting security breach.
- To rectify these privacy failures, the Information Regulator has ordered several corrective measures, including issuing a formal apology, establishing a comprehensive POPIA compliance framework, and conducting mandatory staff training.
- Failure to follow these directives could result in a heavy fine or criminal prosecution.
- This enforcement action serves as a reminder to responsible parties to align their personal information handling practices with the legislated privacy standards.

A compliance framework is an essential element of POPIA Compliance

Table of Contents

1. Unlawful Sharing of Vetting Information

The Information Regulator recently issued an Enforcement Notice against Central Johannesburg TVET College ("the College") following complaints by three individuals. Failure to comply with the Enforcement Notice will be a criminal offence, that could potentially result in a fine and/or imprisonment for up to 10 years.

The College was placed under administration due to governance failures. Several employees had failed to declare their criminal records and possible conflicts of interest, such as doing business with the employer. The College had to investigate and address these problems. All employees declared their previous criminal records and interests, and Verification Reports were obtained from a third party to strengthen governance. The Acting Chief Financial Officer had erroneously included the complainants' Verification Reports in the folder containing finance policies, and this information was sent by email to several employees. Only names, identity numbers, dates of birth, and contact numbers were shared. An email was subsequently sent to all employees to alert them that the complainants' personal information had been shared by mistake, that an investigation was launched to understand the circumstances of the error, and that corrective action had been taken.

2. Non-Compliance

The Information Regulator found that the College:

- did not implement adequate **accountability** measures,
- unlawfully **further processed** and disclosed personal information,
- did not maintain appropriate **security safeguards**, and
- failed to **notify** both the Information Regulator and affected individuals of the security compromise, as POPIA requires.

The transgressions can be summarised as follows:

Accountability	Further Processing Limitation	Security Safeguards	Notification of Security Compromises
• Colleged failed to register its Information Officer or any Deputy Information Officer • Information Officer is responsible for ensuring compliance with POPIA. • College failed to comply with certain conditions for the lawful processing of personal information	• Sharing of the Verification Reports with unauthorised staff constitutes further processing • Sharing of information incompatible with the original purpose of collection • No data subject consent for sharing of information	• College failed to implement appropriate organisational measures to prevent unlawful access to the information • Sensitive verfication reports should be separated from general finance policy folders	• Information Regulator and affected persons were not notified of the security compromise as required by POPIA

2. Corrective Action

The Information Regulator ordered the College to take the following corrective actions:

Registration	Register the Information Officer and Deputy Information Officers with the Regulator and provide proof within 31 days
Formal Notification	Formally notify both the Regulator and the affected data subjects of the security compromise within 31 days
Apology	Submit a written apology to the complainants, email it to all employees, and publish it through all other communication channels within 31 days
Disciplinary Action	Take appropriate action against the employee who unlawfully shared the personal information and provide proof within 60 days
Compliance Framework	Submit a POPIA Compliance Framework (including privacy, retention, incident response and information privacy and security policies) within 31 days (120 days if it must be developed from scratch)
Training and Awareness	Conduct internal POPIA training for all employees and submit copies of training material and proof of attendance to the Regulator within 90 days.

3. Key Lessons for Responsible Parties

The enforcement action reinforces several compliance principles:

- Personal information, particularly special personal information, should not be disclosed or further processed without a lawful basis.
- Appropriate accountability measures and security safeguards must be maintained.
- Security compromises must be reported as required by POPIA.
- A POPIA compliance framework must be in place.
- Information officers (and deputy information officers, if applicable) must be registered with the Information Regulator.
- POPIA awareness campaigns and training of staff should be conducted from time to time.