



H&I

**PROTECTION OF PERSONAL
INFORMATION (POPI) POLICY**

Index

1. INTRODUCTION	3
2. PURPOSE	3
3. APPLICATION	3
4. DEFINITIONS.....	3
5. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION	5
5.1. Accountability.....	5
5.2. Processing limitations	5
5.3. Purpose specification	6
5.4. Further processing limitation	7
5.5. Information quality.....	8
5.6. Openness.....	8
5.7. Security safeguards	8
5.8. Data subject participation.....	9
6. PROCESSING OF SPECIAL PERSONAL INFORMATION	10
6.2.1. Religious or philosophical belief	10
6.2.2. Race or ethnic origin	10
6.2.3. Trade union membership	10
6.2.4. Political persuasion	10
6.2.5. Health or sex life	10
6.2.6. Criminal behaviour or biometric information	11
7. USING PERSONAL DETAILS FOR DIRECT MARKETING.....	11
8. THE INFORMATION OFFICER	11
9. TRAINING AND AWARENESS	11
10. BREACH OF POPI Act.....	11

Document version control		
Policy version	Date Issued	Authorised
Version 1	01 / 07 / 2021	

1. INTRODUCTION

This POPI Policy is applicable to Haw & Inglis Civil Engineering (Pty) Ltd and incorporates its subsidiaries as detailed below, collectively referred to as “H&I” in this policy document:

- H&I Civil and Building (Pty) Ltd
- H&I Construction (Pty) Ltd
- H&I Plant and Crushing (Pty) Ltd
- HITCO (Pty) Ltd

The Protection of Personal Information Act, Act no. 4 of 2013 (hereinafter referred to as “POPI Act”) balances an individual’s right to privacy by regulating and protecting the processing of personal information. For the purposes of operating its business, H&I collects and utilises certain personal information of individuals (including employees) and companies, with whom it deals with. We therefore recognise that such personal information must be handled appropriately however it may be collected, stored and processed, whether on paper, electronically or other means.

To ensure that personal information is processed lawfully, the following conditions (as set out in the POPI Act) must be met:

- Accountability;
- Processing limitation;
- Purpose specification;
- Further processing limitation;
- Information quality;
- Openness;
- Security safeguards; and
- Data subject participation.

2. PURPOSE

This policy provides guidance in respect of the processing of personal information and ensuring compliance with the POPI Act as well as the individual’s constitutional right to privacy. It further aims to protect individuals against the unlawful collection, retention, dissemination and use of personal information.

3. APPLICATION

This policy applies to all H&I employees as well as third parties who have been granted access to or given personal information via H&I.

4. DEFINITIONS

- 4.1. **Consent** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
- 4.2. **Data subject** means the person to whom personal information relates to.
- 4.3. **Information officer** of, or in relation to,
 - 4.3.1. a public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
 - 4.3.2. a private body means the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act.

- 4.4. **Operator** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- 4.5. **Person** means a natural person or a juristic person.
- 4.6. **Personal information** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
 - 4.6.1. 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 birth of the person;
 - 4.6.2. information relating to the education or the medical, financial, criminal or employment history of the person;
 - 4.6.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
 - 4.6.4. the biometric information of the person;
 - 4.6.5. the personal opinions, views or preferences of the person;
 - 4.6.6. 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;
 - 4.6.7. the views or opinions of another individual about the person; and
 - 4.6.8. 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.
- 4.7. **Processing** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
 - 4.7.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - 4.7.2. dissemination by means of transmission, distribution or making available in any other form; or
 - 4.7.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;
- 4.8. **Public record** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body
- 4.9. **Record** means any recorded information—
 - 4.9.1. regardless of form or medium, including any of the following:
 - 4.9.1.1. Writing on any material;
 - 4.9.1.2. information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
 - 4.9.1.3. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
 - 4.9.1.4. book, map, plan, graph or drawing;

- 4.9.1.5. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
- 4.9.2. in the possession or under the control of a responsible party;
- 4.9.3. whether or not it was created by a responsible party; and
- 4.9.4. regardless of when it came into existence.
- 4.10. **Regulator** means the Information Regulator established in terms of section 39 of the POPI Act.
- 4.11. **Special personal information means** personal information concerning—
 - 4.11.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
 - 4.11.2 the criminal behaviour of a data subject to the extent that such information relates to—
 - 4.11.2.1 the alleged commission by a data subject of any offence; or
 - 4.11.2.2 any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

5. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The POPI Act provides for the following conditions to be met in respect of processing personal information:

5.1. Accountability

- 5.1.1 H&I will implement policies and safeguard measures to protect all information. It is for this reason that the Information Technology systems management policy must be read with this policy to ensure that all personal information is protected at all times.
- 5.1.2 Any and all employees of H&I who are responsible for processing personal information must ensure that s/he and H&I are compliant with the conditions, as set out in the POPI Act and clauses 5.2 to 5.8 below, when processing personal information.

5.2. Processing limitations

- 5.2.1 All personal information must be processed lawfully and in a reasonable manner that does not infringe on the rights of the data subject.
- 5.2.2 Personal information cannot be collected / processed if it is not required for a specific reason / purpose. In requesting personal information, it is imperative that it is obtained for a specific reason (relevant), adequate and is not excessive.
- 5.2.3 In the event that H&I or any employee of H&I, is in possession of personal information, such personal information can and will only be used for the purpose that it was collected. If the information is for a different reason than for which it was originally collected, the individual's consent must be obtained for further processing of such information.
- 5.2.4 Personal information may only be processed if –
 - 5.2.4.1 the data subject consents to the processing;
 - 5.2.4.2 processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

- 5.2.4.3 processing complies with an obligation imposed by law on H&I;
- 5.2.4.4 processing protects a legitimate interest of the data subject;
- 5.2.4.5 processing is necessary for pursuing the legitimate interests of H&I or of a third party to whom the information is supplied.
- 5.2.5 H&I will collect personal information directly from a data subject, unless –
 - 5.2.5.1 the information is contained in or derived from a public record or has deliberately been made public by the data subject;
 - 5.2.5.2 the data subject has consented to the collection of the information from another source;
 - 5.2.5.3 collection of the information from another source would not prejudice a legitimate interest of the data subject;
 - 5.2.5.4 collection of the information from another source is necessary–
 - 5.2.5.4.1 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
 - 5.2.5.4.2 to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;
 - 5.2.5.4.3 compliance would prejudice a lawful purpose of the collection; or
 - 5.2.5.4.4 compliance is not reasonably practicable in the circumstances of the particular case.

5.3. Purpose specification

- 5.3.1 Where personal information is collected, it must be for a specific, explicitly defined and lawful purpose which is related to function or activity of the party collecting the information.
- 5.3.2 H&I will ensure that steps are taken to ensure that data subjects are aware of the purpose of the collection of the information unless the provisions of section 18(4) of the POPI Act are applicable.
- 5.3.3 Personal information may not be retained for periods longer than is required and must be destroyed or deleted as soon as reasonably possible after the purpose for which it was processed has expired.
- 5.3.4 It is acknowledged that legislation may require H&I to retain certain personal information and/ or records after termination of an employee/ contractor/ supplier/ customer and therefore, such information may be retained for the period prescribed by such legislation.
- 5.3.5 The following is a guideline for retention periods in the absence of a specific business case supporting a longer period.

TYPE OF PERSONAL INFORMATION	DURATION OF RETENTION
Application forms/ References and/ or CV's	Duration of employment / 12 months after communicating to unsuccessful candidates
Payroll and tax information	7 years after termination of employment
All leave records	3 years after termination of employment
Remuneration information	7 years after termination of employment

Annual appraisal/assessment records	5 years after termination of employment
Records relating to promotion, transfer, training, disciplinary matters	3 years from termination of employment
References given / information to enable reference to be provided	3 years from reference/end of employment
Summary of record of service e.g., name, position held, dates of employment	7 years after termination of employment
Records relating to accident/injury at work	40 years after termination of employment
Financial information relating to suppliers and customers	7 years
Tender / customer documentation	7 years

- 5.3.6 Where personal information is to be retained for longer than the stated retention period, the designated / responsible individual must document any applicable justification for extending this period which is submitted to the Information Officer.
- 5.3.7 The destruction of personal information must be conducted in a manner which makes it impossible for another party to recreate the documentation and access personal information of a data subject. This will require the responsible H&I representative to either permanently delete electronic information and/ or shred such information.
- 5.3.8 In terms of scanned documents, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.
- 5.3.9 Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

5.4. Further processing limitation

- 5.4.1 Personal information will be collected/ processed for a specific reason/ purpose and therefore any further processing must be compatible with the initial reason for obtaining such information. Should the purpose/ reason for further processing of such personal information be for a different reason than initially acquired, the data subject must provide written consent, if the information is not publicly available.
- 5.4.2 Further processing of personal information will be allowed if the information is used for historical, statistical or research purposes and H&I ensures that the further processing is carried out solely for such purposes and ensures that the information is not published in an identifiable form.

5.5. Information quality

Any personal information which is processed must be complete, accurate and not misleading. Personal information must, where necessary, be updated to ensure that it is relevant in terms of the purpose for which it is collected. For example, an employee's residential address must be updated when s/he moves as it was obtained for the purposes of H&I being able to serve documents on the employee.

5.6. Openness

5.6.1. The party responsible for the collection of personal information, must inform the data subject of the –

5.6.1.1. the information being collected and/ or where such information has been collected;

5.6.1.2. the purpose for which the information is being collected;

5.6.1.3. whether or not the supply of the information by that data subject is voluntary or mandatory;

5.6.1.4. the consequences of failure to provide the information;

5.6.1.5. any particular law authorising or requiring the collection of the information;

5.6.1.6. the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation; and

5.6.1.7. any further information that may be necessary.

5.6.2. It is not necessary for H&I to inform a data subject of the aforementioned detail if the provisions of section 18(4) of the POPI Act applies.

5.7. Security safeguards

5.7.1. All personal information within H&I and/ or its employees' possession must be kept confidential, and the integrity of such information must be secured. This includes ensuring that such information is protected from loss of, damage to or unauthorised destruction as well as the unlawful access to or processing of personal information.

5.7.2. Any H&I employee who is responsible for the processing personal information must ensure that such information is not left unattended and must ensure that it is securely locked away.

5.7.3. Emails and Faxes

5.7.3.1. Employees must pay particular attention to the risks of transmitting confidential/ personal information by email or fax.

5.7.3.2. Ensure that all copies of email and fax messages received, are held securely.

5.7.3.3. Information is not stored on the fax machine, which can be accessed by parties who are not authorised to have access to such information.

5.7.3.4. Permission to send personal information is obtained from the data subject (for example confirmation of employment).

5.7.3.5. Be aware of the risks of sending confidential, personal information by email or fax.

5.7.4. Information can only be disclosed to authorised individuals and the data subject must provide written consent for such information to be disclosed to a third party.

- 5.7.5 Access to personal information is for work purposes only and should only be accessed for legitimate purposes.
- 5.7.6 Where a third party is, for processing purposes, granted with access to personal information (excluding legislative requirements), they will be required to sign an operator agreement which will include the requirement to comply with the requirements of the POPI Act.
- 5.7.7 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, H&I will, in terms of section 22 of the POPI Act, notify the Regulator and subject to section 22(3) of the POPI Act, notify the data subject, unless the identity of such data subject cannot be established.

5.8. Data subject participation

- 5.8.1 A data subject has the right (on proof of identification that s/he is the data subject) request confirmation and/ or a record of and/ or description of any personal information related to the data subject within H&I's possession.
- 5.8.2 The data subject may request that H&I corrects, deletes and/ or destroys any information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. Such requests must be submitted in writing to the Information Officer, with a copy of adequate identification, which will be actioned as soon as reasonably possible. The request can be submitted to the information officer on the following email address: informationofficer@hiconstruction.co.za
- 5.8.3 The data subject also has the right to request that H&I destroys or deletes any personal information that H&I is no longer permitted to retain. This must be actioned as soon as reasonably possible.
- 5.8.4 Templates for the access of personal information (Form 1), correction of personal information (Form 2), Limitation of processing of personal information (Form 3) or the objection of processing of personal information (Form 4) can be found on H&I's website at www.hiconstruction.co.za.

6. PROCESSING OF SPECIAL PERSONAL INFORMATION

- 6.1. The processing of special personal information is prohibited unless:
 - 6.1.1 The data subject provided written consent;
 - 6.1.2 It is necessary for the establishment, exercise or defence of a right or obligation in law;
 - 6.1.3 processing is necessary to comply with an obligation of international public law;
 - 6.1.4 processing is for historical, statistical or research purposes to the extent that the purpose serves a public interest, or it appears to be impossible or would involve a disproportionate effort to ask for consent,
 - 6.1.5 information has deliberately been made public by the data subject.

- 6.2. Further to clause 6.1 above, the following applies to the processing of special personal information:

6.2.1 Religious or philosophical belief

All individuals have the right to their own religious and/ or philosophical beliefs and such information will not be processed by H&I and/ or its employees. H&I will not discriminate or process information in respect of a person/ employee's religious or philosophical beliefs.

6.2.2 Race or ethnic origin

Information about a person/ employee/ third party's race and/ or ethnic origin will only be processed for the purposes of complying with relevant laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination. This will include compliance and for the purposes of the Employment Equity Act, the Broad-Based Black Economic Empowerment Act and Affirmative Action measures and any other legislative requirements.

6.2.3 Trade union membership

H&I and its employees who have access to information about trade union membership will not disclose such information to a third party and/ or will only disclose such information to facilitate a provision in the Labour Relations Act and/ or if it is required in terms of a court order, arbitration award and/ or as any other relevant legislation.

This information cannot be provided to a Trade Union to which the individual is not a member. Furthermore, Trade Unions are not entitled to the personal information of employees/ individuals who do not belong to such a Trade Union. Prior to providing personal information of an employee/ individual, H&I will first verify that the person, requesting such information on behalf of the Trade Union, is authorised to request such information.

6.2.4 Political persuasion

H&I and/ or its employees will not process any information in respect of any employee and/ or individual in respect of their political persuasion

6.2.5 Health or sex life

Information about a person/ employee's health and/ or sex life can only be processed if such processing is necessary for the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject.

Furthermore, information about an employee/ person's health, medical condition/s and/or ability to work can only be processed with the employee/ person's consent and where it is related to his/ her position.

In the event that medical information is required, such information will only be obtained with the persons' written consent and must be in accordance with the relevant employment legislation (which includes but is not limited to the Labour Relations Act, Employment Equity Act, etc.).

6.2.6 Criminal behaviour or biometric information

Information about a person/ employee's criminal behaviour/ record and/ or biometric information can only be processed once the person/ employee has given his/ her written consent and where such information is an inherent requirement of the job. Such information can only be processed by a party who is accredited to process and authorised to provide such information.

7. USING PERSONAL DETAILS FOR DIRECT MARKETING

- 6.3 All individuals have the right to prevent their personal information being used for direct marketing (which includes communications sent by post, over the phone, via email and text) purposes. Therefore, H&I and/ or its employees will not use or distribute personal information for the purposes of direct marketing.
- 6.4 In the event of H&I sharing a person/s personal information for the purposes of direct marketing and/ or to any third party, the person must provide his/ her written consent to share such information.

8. THE INFORMATION OFFICER

- 8.2 The Information Office is responsible for:
 - 8.2.1 The encouragement of compliance with the conditions for the lawful processing of personal information.
 - 8.2.2 Dealing with requests made to H&I in terms of policy and/ or the POPI Act.
 - 8.2.3 Working with the Regulator in relation to investigations conducted at H&I.
 - 8.2.4 Ensuring compliance by the body with the provisions of POPI Act.
 - 8.2.5 To monitor any changes to legislation, practice and technology, and ensure that the minimum standards in terms of this policy is updated where necessary.
 - 8.2.6 Ensure that H&I has access to legislative updates and any guidance related to data protection legislation.
 - 8.2.7 Oversight of the data protection breaches, including decisions as to whether or not affected individuals should be notified.
 - 8.2.8 Have oversight of all breaches and liaise with HR and/ or the Managing Director to ensure that any deficiencies in the control framework are addressed.

9. TRAINING AND AWARENESS

- 9.1. Employees who deal with personal information must undergo training, at least once every two (2) years and/ or whenever there is a significant change to the POPI Act and/ or any relevant regulations.
- 9.2 Senior management must be able to demonstrate, with documentary evidence, the completion or participation in personal information protection training and awareness exercises by all relevant, in-scope employees.

10. BREACH OF POPI Act

In the event that any person breaches this policy and/ or the requirements of POPI Act, such breaches must be reported to the Information Officer and the HR department and may result in disciplinary action which may ultimately result in the termination of his/ her services. Such a breach may also be reported to the Regulator.