THE SHARD

Contact Information
202B, 2nd Floor, The Zone @ Rosebank,
Regent Place, 177 Oxford Road,
Rosebank, Johannesburg, 2196
t. +27 87 049 2302
e. info@theshard.co.za
w. www.theshard.co.za

Protection of Personal Information Policy

July 2021

Table of Contents

1. Glossary of Abbreviations and Definitions

The following terms as used in this policy have the following meanings:

Term	Meaning
CIO	Chief Information Officer
Personal Information	Includes but is not limited is not to: General personal information such as: Names, email addresses, phone numbers, gender, nationality, date of birth, race, home address, identity documentation numbers. Sensitive information such as: Previous criminal convictions or any alleged criminal convictions, mental, physical health status, and identity documentation numbers. Job related such as: Job title and previous work experience.
Data Subject	The person to whom personal information relates
Employee	Part or fulltime employee of The Shard, including any contractor with access to The Shard's information systems and its clients' data
Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use. dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information.

2. Purpose

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA"). POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner. Given the importance of privacy, The Shard is committed to effectively managing personal information in accordance with POPIA's provisions.

The purpose of this policy is to set forth rules and guidelines for use and handling of the company's Confidential Data policy by company users including employees, contractors, temporary staff, visitors, and other persons with authorisation to do so.

3. Scope

This policy and its guiding principles apply to all employees, contractors, consultants, temporaries, and other workers at The Shard who make use of the company's confidential data in the rendering of various services to stakeholders. Reference to his and/or her also apply to legal persona as well.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as The Shard's PAIA Manual as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

4. Legal Framework

The Policy will be informed by and not limited to the following legislations:

- Protection of Personal Information Act (POPI), 2013. Act No. 4 of 2013.

5. Policy Requirements

Where appropriate, the organisation will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.
The Shard ensure that it gives effect to the following seven rights.

5.1. The Right to Access Personal Information

The organisation recognises that a data subject has the right to establish whether the organisation holds personal information related to him or her, including the right to request access to that personal information.
An example of a "Personal Information Request Form" can be found under Annexure A.

5.2. The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information.

5.3. The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

In such circumstances, the organisation will give due consideration to the request and the requirements of POPIA. The organisation may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.4. The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5. The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

An example of a "POPI Complaint Form" can be found under Annexure B.

5.6. The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by the organisation.

The data subject also has the right to be notified in any situation where the organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. General Guiding Principles

All employees and persons acting on behalf of The Shard shall at all times be subject to, and act in accordance with, the following guiding principles:

6.1. Accountability

Failing to comply with POPIA could potentially damage the organisation's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Shard shall ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the organisation will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2. Processing Limitation

The organisation will ensure that personal information under its control is processed:

- in a fair, lawful, and non-excessive manner, and
- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

The Shard shall inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.
Alternatively, where services or transactions are concluded over the telephone or electronic video feed, The Shard shall maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

The Shard shall under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information shall be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

An example of a "POPI Notice and Consent Form" can be found under Annexure C.

6.3. Purpose Specification

All of The Shard's operations must be informed by the principle of transparency. The Shard shall process personal information only for specific, explicitly defined and legitimate reasons. The Shard shall inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.4. Further Processing Limitations

Personal information shall not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where The Shard seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, The Shard shall first obtain additional consent from the data subject.

6.5. Information Quality

The Shard shall take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of a Group Life Cover are of the utmost importance), the greater the effort the organisation shall put into ensuring its accuracy.

Where personal information is collected or received from third parties, The Shard shall take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.6. Open Communication

The Shard shall take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.
The Shard shall ensure that it establishes and maintains a “contact us” facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether the organisation holds related personal information, or
- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information. The Shard shall take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

The Shard shall ensure that it establishes and maintains a “contact us” facility, available on its website, for data subjects who want to:

- Enquire whether the organisation holds related personal information, or
- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7. Security Safeguards

The Shard shall manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction.

Security measures also will be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or identity numbers, the greater the security required.

The Shard shall continuously review its security controls which shall include regular testing of protocols and measures put in place to combat cyber-attacks on the company’s IT network.

The Shard shall ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees shall be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses shall also be included to reduce the risk of unauthorised disclosures of personal information for which the company is responsible.

All existing employees shall, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.
The Shard's operators and third-party service providers shall be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

An example of "Employee Consent and Confidentiality Clause" for inclusion in the organisation's employment contracts can be found under Annexure D.

An example of an "SLA Confidentiality Clause" for inclusion in the organisation's service level agreements can be found under Annexure E.

6.8. Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by the company.
The Shard shall ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.
Where applicable, the Shard shall include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. Information Officer(s)

The Shard shall appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

The Shard's Information Officer is responsible for ensuring compliance with POPIA. There are no legal requirements under POPIA for an organisation to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.

Where no Information Officer is appointed, the Chief Executive shall assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the reappointment or replacement of any Deputy Information Officers.
Once appointed, The Shard shall register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

An example of an "Information Officer Appointment Letter" can be found under Annexure F.

8. Specific Duties and Responsibilities

8.1. Governing Body

The Shard's Executive Management cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA.
The Executive Management may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The Executive Management is responsible for ensuring that:

- The Shard appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of the organisation:
  - are appropriately trained and supervised to do so,
  - understand that they are contractually obligated to protect the personal information they come into contact with, and
  - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

8.2. Information Officer

The organisation's Information Officer is responsible for:

- Taking steps to ensure The Shard's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation. For instance, maintaining a "contact us" facility on the organisation's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.

- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.3. Head of IT Audit &CIO

The Shard's Head of IT Audit &CIO is responsible for:

- Ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.

Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

8.4. Managing Directors

The Shard's Managing Directors: are responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

8.5. Employees and other Persons acting on behalf of the Organisation

Employees and other persons acting on behalf of the organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.
- Furthermore, personal information will only be processed where the data subject:
    - Clearly understands why and for what purpose his, her or its personal information is being collected; and
    - Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the organisation will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or

- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the organisation will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the organisation are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The Chief Information Officer shall assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. Policy Compliance

This policy shall be enforced by Information Officer unless otherwise stated in writing. Violations may result in disciplinary action, which may include suspension, restriction of access, or a more severe penalty up to and including termination of employment.

Where a POPI complaint or a POPI infringement investigation has been finalised, the organisation may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, the organisation will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the organisation may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

Additionally, the Information Officer shall schedule periodic POPI audits.

The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout the organisation. For instance, the organisation's various divisions and other associated organisations.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within in the organisation's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

10. Request to Access Personal Information Procedure

Data subjects have the right to:

- Request what personal information the organisation holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation's PAIA Manual.

The Information Officer will process all requests within a reasonable time.

11. POPI Complaints Procedure

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The organisation takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
  - A suggested remedy for the complaint,
  - A dismissal of the complaint and the reasons as to why it was dismissed, and
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer shall review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

12. Policy Review and Amendments

The Shard reserve the right to update or change this policy at any time and employees should check this policy periodically. All stakeholders that continue to use The Shard's service after any modifications to the policy shall constitute an acknowledgment of the modifications and consent to abide and be bound by the modified policy.

This policy shall be reviewed annually and amended as required to ensure that all matters relating to confidential data are compliant with relevant laws and regulations. Policy amendments shall only be approved by the Board upon recommendation by Executive Management.

Updates to this policy and related information shall from time to time be published on The Shard's intranet / be made available to employees and contractors (incl., the third-party service providers).

13. Other Related Resources/Policies

- Data Protection Policy
- Information and Cyber Security Policy
- The Shard PAIA Manual

14. Policy Administration

14.1. Version Information

Policy Name	Version	Compiled By	Date Compiled	Approved By	Approved Date
Protection of Personal Information Policy	V1	M.A.Ndlovu	July 2021		

14.2. Frequency of Review

Frequency of review	Next review date	Last review date
Annually	July 2022	N/A

1. Annexures

Annexure A - Personal Information Request Access Form

Personal Information Request Access Form

Please use blue or black pen and write in BLOCK LETTERS

Applicant's details

Title | Surname | First name(s) | Date of birth (DD/MM/YYYY)

Current residential address

Is your current residential address outside South Africa? Yes No

Address

Suburb | Postcode | Country

Address for delivery of requested information (if different to above) address:

Suburb | Postcode | Country

How should we contact you? Please delete inappropriate from the below:

Home telephone number | Mobile or work telephone number | Email

What information do you want us to provide?

(e.g. I need you to give me a copy of the information included in my employment contract)

I need you to give me:

Your declaration and authority

By signing and sending in this form:

I declare that I am the individual named above or I am their legally authorised representative (and I have attached a copy of the authority); and

I authorize The Shard to share information about me for the purpose of responding to my request and to provide me with information in any form they consider appropriate.

Signature | Date (DD/MM/YYYY)

Annexure B - Personal Information Complaint Form

Protection of Personal Information Complaint Form

Please use blue or black pen and write in BLOCK LETTERS

Applicant's details

Title | Surname | First name(s) | Date of birth (DD/MM/YYYY)

Current residential address

Is your current residential address outside South Africa? Yes No

Address

Suburb | Postcode | Country

How should we contact you? Please delete inappropriate from the below:

Home telephone number | Mobile or work telephone number | Email

What complaints would you like to raise to the Information Regulator?

(e.g. I have been refused access to my personal data or my personal data has been processed illegally)

I need to raise the following complaints against xxx:

Your declaration and authority

By signing and sending in this form:

I declare that I am the individual named above or I am their legally authorised representative (and I have attached a copy of the authority); and

I authorize the Information Regulator to share information about me for the purpose of responding to my complaint and to request from me any further in any form they consider appropriate.

Signature | Date (DD/MM/YYYY

Annexure C – Protection of Personal Information Notice and Consent Form

Protection of Personal Information Notice and Consent Form

Please use blue or black pen and write in BLOCK LETTERS

This document describes how The Shard will lawfully use your personal data for its business-related purposes with regards to your employment relationship with it. Such data will also be used for The Shard's administrative and operational activities. Please read it and return a signed copy to the Administration department confirming that you have understood the contents of the document and give consent to the use of such data as described below.

What constitutes use of your personal data:

Use of personal data will include any collection, storage, protection, disclosure, retention and transfer of your personal data.

Examples of your personal data that may be used**:**

General personal information such as:

Names, email addresses, phone numbers, gender, nationality, date of birth, race, home address, identity documentation numbers.

Sensitive information such as:

Previous criminal convictions or any alleged criminal convictions, mental, physical health status, and identity documentation numbers.

Job related such as:

Job title and previous work experience.

Application of this document:

Consent as described in this document does not apply to use of your personal information by The Shard where such use does not require your consent.

The Shard shall however in all circumstances, ensure that its use of your personal data is compliant will applicable legislation.

Security of your personal data:

The Shard shall ensure that your personal data shall be stored, processed, transferred and or disclosed securely under all circumstances. Controls such as restricting access to personal information and logging such access, use of data encryption technologies and other controls deemed appropriate shall be used to guarantee the security of your data.

How long will your data be retained?

Your data will be retained and used by The Shard for no longer than necessary for the purposes for which it was obtained.

Such data shall be kept up to date were appropriate.

Your rights regarding your personal data:

You have the following rights under applicable data protection laws:

The right to establish whether The Shard holds personal information to relating to you.

The right to have such information corrected or amended.

The right to request access to personal information relating to you held by The Shard.

As well as the right to object (on a legitimate legal basis) the use of such personal data.

Confirmation of consent:

I confirm that I have read, understood and I agree to the use of my personal Information as described above (including sensitive personal Information) by The Shard providers for lawful purposes as described in this document.

I also acknowledge that by signing this document below, I have given consent to the processing of my personal information (including sensitive personal information) by The Shard under circumstances permitted by law.

Name (IN BLOCK) **Signature**

…… ……

Date (dd/mm/yyyy)

……..

Annexure D - Employee Consent and Confidentiality Clause

Employee consent and Confidentiality Clause

Please use blue or black pen and write in BLOCK LETTERS

Definition of terms

The following terms as used in this clause shall have the following definitions:

Employee – means the person (as signed in section 3 below) employed by The Shard

Company – The Shard

Confidential information – means information relating the company including, but not limited to Company's customers, customer lists or requirements, price lists or pricing structures, sales and marketing information, business plans or dealings, Employees or officers, source codes and computer systems, software, financial information and plans, designs, formulae, prototypes, product lines, services research activities, any document marked "Confidential" (or with a similar expression), or any information which the Employee has been told is confidential or which the Employee might reasonably expect the Company would regard as confidential, or any information which has been given lo the Company in confidence by customers, suppliers or other persons.

Agreement by the employee

The Employee will not make or communicate any statement (whether written or oral) to any representative of the press, television, or other media and will not write any article to the press or otherwise for publication on any matter concerned with or relating to the business of the company without obtaining the prior written approval of the Company.

If the Employee is uncertain as to whether any information is confidential or is a trade secret, the Employee will in writing request a ruling from the Company. The Employee undertakes to abide by any ruling made by the Company.

The Employee undertakes that, should the Employee at any stage become aware of any improper disclosure or use of any confidential intimation or trade secret of the Company by another employee of the Company or any other person, the Employee will immediately bring the matter to the attention of the Company in writing.

Consent

I confirm that I have read, understood the above and I agree to comply with the requirements mentioned therein.

Name (IN BLOCK)	**Signature**	**Date**
……	……	……

Annexure E - Service Level Agreement Confidentiality Clause

Service Level Agreement Confidentiality Clause

Please use blue or black pen and write in BLOCK LETTERS

The Shard's operators and third-party service providers shall be required to enter into service level agreements with the company where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

Definition of terms

Operators and third-party service providers – shall refer to either contractors or consultants employed by The Shard to render services to the company.

The Company – means The Shard

POPIA – means the Protection of Personal Information Act,2003

Personal Information includes but is not limited to – the names, email addresses, phone numbers, gender, nationality, date of birth, race, home address, identity documentation numbers of The Shard's employees and customers.

sensitive information such as previous criminal convictions or any alleged criminal convictions, mental, physical health status, and identity documentation numbers relating to The Shard's employees and or customers, information relating to jobs of the Shard's employees such as remuneration packages and job titles.

Agreement by the operator/third party

The operator/third party will not make or communicate any statement (whether written or oral) to any representative of the press, television, or other media and will not write any article to the press or otherwise for publication on any matter concerned with or relating to the business of the company, and any information that the company considers confidential without obtaining the prior written approval of the Company.

If the third party/operator is uncertain as to whether any information is confidential or is a trade secret, it will in writing request a ruling from the Company and will abide by any ruling made by the Company.

The third party/operator undertakes that, should they at any stage become aware of any improper disclosure or use of any confidential intimation or trade secret of the Company by themselves or any other person they will immediately bring the matter to the attention of the Company in writing.

Agreement by the operator/third party

I confirm that I have read, understood the above and I agree to comply with the requirements mentioned therein.

Name (IN BLOCK)	**Signature**	**Date**
……	……	……

Annexure F – Information Officer Appointment Letter

Information Officer Appointment Letter

Company Address

Date

Subject: Appointment for the position of Chief Information Officer

Dear [_____]

Following your acceptance of the job offer letter which you signed on [_____], we would like to confirm your appointment with The Shard as a Chief Information Officer. Your employment is be subject to the terms and conditions listed below:

Starting Date
Your starting date is [_____].

Working hours
Your work timings are from 8AM to 5PM, Monday to Friday.

Probation Period
You will be on a probation period for the first [_____] months. Upon successfully completing the probation period, your employment will become of a permanent status.

Salary
Your monthly salary is [_____]

Other Benefits
[List other benefits if applicable]

Annual Leave
You are entitled to [_____] days of paid leave per year.

Further information governing your employment can be found in the signed contract as well as the Employee Policy document.

If you have further questions, please contact me directly.

Congratulations on your appointment and welcome to The Shard. We look forward to years of fruitful cooperation and success. We wish you the best of luck in your new role.

Sincerely,

[_____]