CALLING ACADEMY

INSPIRE · EQUIP · GROW

# PROTECTION OF PERSONAL INFORMATION POLICY

## BACKGROUND

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy, the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. The Protection of Personal Information Act. POPIA is South Africa's data protection law.

## PURPOSE

This Data Protection and Information Sharing Policy describes the process that Calling Education NPC will follow in order to meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013.

## COMPANY CONTACT DETAILS

| | |
|---|---|
| CEO/ Information Officer | Werner Cloete |
| Deputy Information Officers | Raoul Hamman and Kyra Barnard |
| Postal address | 2 Flax Street<br>Welgevonden<br>Stellenbosch<br>Western Cape<br>7600 |
| Physical address | c/o Vlaeberg and Polkadraai Roads<br>Stellenbosch<br>Western Cape |
| Telephone number | 066 023 5525 |
| Email | wcloete@callingeducation.org.za |

## DEFINITIONS

| | |
|---|---|
| Child | means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself |
| Consent | means the voluntary, specific and informed expression of will in terms of which permission is given |
| Data Subject | means the natural or juristic person to whom the Personal Information relates |
| Direct Marketing | means approaching a Data Subject personally for the purpose of selling them a product or service, of requesting a donation |
| Information Officer | The Information Officer is responsible for ensuring the organisation's compliance with POPIA, but it is ultimately the Head of the school who is responsible for ensuring that the Information Officer's duties are performed |
| The school | Means Calling Academy, trading as Calling Education NPC, also referred to as the responsible party |
| POPI | means the Protection of Personal Information Act, No. 4 of 2013 |
| Personal Information | means information relating to an unidentifiable, living, natural person, or an identifiable, existing juristic person, as defined in POPI |
| Processing | means an operation or activity, whether or not by automatic means, concerning Personal Information |

## SCOPE OF POLICY

The Policy applies to all school employees and directors. The provisions of the Policy are applicable to both on and off-site processing of personal information.

## POLICY STATEMENT

The school collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out its business effectively. The school regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between the school and those individuals and entities who deal with it. The school therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPI").

# PROCESSING OF PERSONAL INFORMATION

## Purpose of Processing

The Group uses the Personal Information under its care in the following ways:
- Administration of parent-learner agreements
- Administration of vendor agreements
- Providing educational services to learners
- Funding purposes
- Conducting market research
- In connection with legal or human resources proceedings
- Staff administration
- Keeping of accounts and records
- Complying with legal and regulatory requirements
- Profiling data subjects for the purposes of direct marketing in relation to donations

## Categories of data subjects and their personal information

The school may possess records relating to vendors, learners, parents & accountable persons, individual donors, company donators, staff and learners.

| **Data Subject** | **Personal Information Processed** |
|---|---|
| Parents & Learners | Names, contact details, physical and postal address, ID number, date of birth, nationality, gender, confidential correspondence, psychological test results and profiles, medical history and academic records |
| Donors: Natural Persons | Full name, contact details and postal address of the donor |
| Donators: Juristic Persons/ Entities | Names of contact person, name of legal entity, physical business address of entity and contact details of entity |
| Contracted Service Providers | Names of contact persons, name of legal entity, physical business address of entity, contact details of entity and banking details of the entity |
| Employees & Directors | Full name, contact details, ID number, date of birth, salary details, bank account details, education information, marital status, gender, age, race, language, employment history, SACE registration and criminal record |

## Categories of recipients for processing of personal information

The school may supply the Personal Information to any party to whom the school may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to customers;
- Conducting due diligence checks.

## Retention of personal information records

The school may retain Personal Information records indefinitely, unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information the school shall retain the Personal Information records to the extent permitted or required by law.

## REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURES

To facilitate the processing of a request for access to personal information, the requester must:

- Use the prescribed form, available as attachment to this policy (Annexure A);
- Address your request to the principal;
- Provide sufficient details to enable the school to identify:
  (a) The record(s) requested;
  (b) The details of the requester (and if an agent is lodging the request, proof of capacity);
  (c) The email address of the requester in the Republic.

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

## POPIA COMPLAINTS PROCEDURE

Data subjects have the right to lodge a written complaint with the school in instances where there is any reason to believe that their rights under POPIA have been infringed upon. Calling Education NPC takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

- POPIA complaints must be submitted to the school in writing in a form substantially similar to Annexure B;

- 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 3 working days;
- 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 a friendly 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 school'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 affected data subjects and the Information Regulator will be informed of this breach; and
- the Information Officer will revert to the complainant with a proposed solution;
- in all instances, the school 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; or
    - an apology (if applicable) and any disciplinary action that has been taken against any employees involved; and
- the Information Officer will 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 POPIA related complaints.

Where the data subject is not satisfied with the Information Officer's suggested remedies, the Data Subject has the right to lodge a complaint with the Information Regulator.

## EIGHT PROCESSING CONDITIONS

POPI is implemented by abiding by eight processing conditions. The school shall abide by these principles in all its possessing activities.

### 1. Accountability

The school shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information. The school shall remain liable for compliance with these conditions, even if it has outsourced its processing activities. The assigned Information Officer and Deputy Information Officer will ensure that personal information is collected and processed in accordance with POPIA. These persons will oversee and manage the school's compliance with POPIA and will furthermore handle all requests made by learners, parents, staff and all relevant stakeholders, for access to information. The designated persons will ensure that the school takes 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 responsibilities outlined in this policy.

### 2. Processing Limitation

**Lawful grounds**

The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.
The school will only process Personal Information if one of the following grounds of lawful processing exists:

- The Data Subject consents to the processing;
- Processing is necessary for the conclusion or performance of a contract with the Data Subject;
- Processing complies with a legal responsibility imposed on the school;
- Processing protects a legitimate interest of the Data Subject;
- Processing is necessary for pursuance of a legitimate interest of the responsible party, or a third party to whom the information is supplied;

Special Personal Information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour;
- Information concerning a child.

The school may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons
- If processing of race or ethnic origin is in order to comply with affirmative action laws

**Collection directly from the Data Subject**

Personal Information must be collected directly from the Data Subject, unless:

- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Personal Information is collected from another source with the Data Subject's consent;
- Collection of Personal Information from another source would not prejudice the Data Subject;
- Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the Data Subject would prejudice the lawful purpose of collection;
- Collection from the Data Subject is not reasonably practicable.

## 3. Purpose Specification

The school shall only process Personal Information for the specific purposes as set out and defined above under "purpose of processing".

## 4. Further Processing

New processing activity must be compatible with the original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- Data Subject has consented to the further processing;
- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;

- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party

## 5. Information Quality

The school shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. The Group shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

## 6. Openness/ Transparency

The school shall take reasonable steps to ensure that the Data Subject is made aware of:

- What Personal Information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection;
- Whether the Personal Information shall be shared with any third party.

## 7. Security Safeguards

The school shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks;

**Written records**

- Personal Information records should be kept in locked cabinets, or safes; or behind locked doors in an office;
- When in use Personal Information records should not be left unattended in areas where non-staff members may access them;
- The school shall implement and maintain a "Clean Desk Policy" where support staff shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
- Personal Information which is no longer required (nor likely to be required in the future) should be disposed of by shredding.
- Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

**Electronic Records**

- All electronically held Personal Information must be saved in a secure database;
- As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices (this excludes essential information that staff require to perform their duties);
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently (within reasonable bounds);
- The school shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
- Electronic Personal Information which is no longer required and not likely to be required in the future must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

## 8. Data subject participation

All individuals and entities may request access, amendment or deletion of their own Personal Information held by the school. Any requirements should be directed, on the prescribed form, to the Information Officer. The school shall not disclose any Personal Information to any party unless the identity of the requester has been verified. Fees may be applied to your request, depending on the significance of the cost to the school. See the "request to access personal information procedures" for guidance on how to access your information.

**Rights of the data subject**

In order to ensure that Data Subjects are made aware of the rights conferred upon them by POPIA the school notes for the purposes of this Policy that Data Subjects have, amongst others, the right to:

- be notified that personal information about them is being collected;
- request access to, the correction of, or the deletion of any Personal Information held by the school using the form attached hereto as Annexure A to this Policy;
- withdraw consent to process their personal information in terms of the Form attached hereto as Annexure A;
- lodge a complaint concerning the processing of their personal information in terms of the for attached hereto as Annexure B;
- object, on reasonable grounds, to the processing of their personal information;

- object to the processing of their personal information at any time for purposes of direct marketing;
- be notified that their personal information has been accessed or acquired by an unauthorised person;
- submit a complaint to the Information Regulator regarding the alleged interference with the
  protection of their personal information; and
- institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

**Processes to vindicate the rights of Data Subject**

The school will uphold the rights of the Data Subject by ensuring that it:

- does not collect data unnecessarily;
- implements this Policy in respect of processing personal information;
- does not retain records of personal information longer than it is necessary for achieving the purpose for which the personal information was collected, or as may be prescribed in terms of a law or contract, or with the consent of the data subject;
- trains staff on the obligations imposed by POPIA when they process personal information;
- ensures that personal information is securely stored;
- has complete control over personal information kept at the school;
- keeps a catalogue system to assist the school to address requests for access to personal information by Data Subjects;
- destroys and / or deletes Personal Information this will be conducted in a manner that prevents its reconstruction or reidentification;
- informs Data Subjects about the use of a CCTV on the premises;
- informs the Data Subject if it collects personal information for marketing or advertising purposes and provides an opportunity for them to object;
- In the case of an access breach to the personal information under the control of the school the school will notify the Data Subject and the Information Regulator in writing as soon as reasonably possible after the discovery of the access breach to the personal information via either:
  - mail at the last known physical or postal address;
  - e-mail to the last known e-mail address;
  - publishing a notice on the school website; or
  - publishing a notice in the news media, and
- where applicable, Calling Education NPC will include a link or an option to unsubscribe from any of its electronic newsletters or related marketing activities.

**Rights of the school**

Please note that the school may lawfully process personal information without obtaining consent from a Data Subject if the processing of the personal information:

- is necessary for pursuing the legitimate interest of the school or of a third party to whom the
- information is given;
- protects a legitimate interest of a Data Subject;
- is necessary to conclude or perform a contract to which a Data Subject is a party; or
- complies with an obligation imposed by law.

**Grounds for Refusal**

The school may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which the school may refuse access include:

- Protecting personal information that the school holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that the school holds about a third party or the school (for example information that may harm the commercial or financial interests of the organisation or the third party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- If disclosure of the record would endanger the life or physical safety of an individual;
- If disclosure of the record would prejudice or impair the security of property or means of transport;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record would harm the commercial or financial interests of the school;
- Disclosure of the record would put the school at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer programme; and
- The record contains information about research being carried out or about to be carried out on behalf of a third party or the Group.

**Records that cannot be found or do not exist**

If the school has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit. This will include the steps that were taken to try to locate the record.

## DIRECT MARKETING

All direct marketing communications (newsletters) shall contain contact details and a method for the receiver to opt-out of receiving further communications.

**Existing donors, parents, or prayer partners**

Direct marketing by electronic means to existing donors, parents or prayer partners is only permitted if:

- The donor, parents or prayer partners details were obtained in the context of a donation given, enrolling at the school or interest shown in the school; and
- The marketing is sent out for the same or similar purpose.

The donor, parents or prayer partners must be given the opportunity to opt-out of receiving the direct marketing on each occasion of direct marketing communication sent out.

**Consent**

The school may send electronic direct marketing communication to Data Subject who have consented to receiving it.

**Record keeping**

The school will keep record of:

- Date of consent
- Way of consent (tick-box on application, email, verbal, etc.)
- Wording of the consent
- Who obtained the consent
- Proof of opportunity to opt-out on each marketing contact
- Record of opt-outs

## DESTRUCTION OF DOCUMENTS

Documents may be destroyed after the termination of the retention period specified herein, or as determined by the school from time to time. Each staff member is responsible for attending to the destruction of documents and electronic records, which must be done on a regular basis. Hard copy documents with personal information need to be shredded.

## STATUTORY RETENTION PERIODS

| Legislation | Document Type | Retention Period |
|---|---|---|
| Companies Act | Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act;<br>Copies of annual financial statements required by the Act;<br>Copies of accounting records as required by the Act;<br>Record of directors and past directors, after the director has retired from the company; Minutes and resolutions of directors' meetings, audit committee and directors' committees. | 7 years |
| | Registration certificate;<br>Memorandum of Incorporation and alterations and amendments;<br>Rules and policies;<br>Register of company secretary and auditors | Indefinitely |
| Consumer protection Act | Full names, physical address, postal address and contact details;<br>ID number;<br>Service rendered;<br>Cost to be recovered from the learners' parents;<br>Frequency of accounting to the accountable person;<br>Amounts, sums, values, charges, fees, remuneration specified in monetary terms; | 3 years |
| Basic Conditions of Employment | Section 29(4):<br>-Written particulars of an employee after termination of employment;<br><br>Section 31:<br>-Employee's name and occupation;<br>-Time worked by each employee;<br>-Remuneration paid to each employee; | 3 years |
| Labour Relations Act | Records to be retained by the employer are the collective agreements and arbitration awards. | 3 years |
| | An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; | Indefinite |

| | | |
|---|---|---|
| | Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions. | |
| Unemployment Insurance Act | Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed. | 5 years |
| Tax Administration | Section 29 documents which:<br>-Enable a person to observe the requirements of the Act;<br>-Are specifically required under a Tax Act by the Commissioner by the public notice;<br>-Will enable SARS to be satisfied that the person has observed these requirements | 5 years |
| Income Tax Act | Amount of remuneration paid or due by him to the employee;<br>The amount of employee's tax deducted or withheld from the remuneration paid or due;<br>The income tax reference number of that employee;<br>Any further prescribed information;<br>Employer Reconciliation return. | 5 years |
| National Protocol for Assessment | Learner profiles;<br>Including disciplinary reports, assessment of special needs, medical information, report cards and any personal information. | 3 years |
| Non-profit Organisation Act | Certificate of registration as non-profit organisation | Indefinite |

# IMPLEMENTATION GUIDELINES

## Training & dissemination of information

This Policy has been put in place throughout the school, training on the Policy and POPI will take place with all affected employees. All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPI.
Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff. Responsibilities of employees relating to POPIA are included in the policy below.

## Employee contracts

Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

Each employee currently employed within the school will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

## Specific duties and responsibilities of school's employees

### Information Officer (and/or Deputy Information Officer/s)

The school's Information Officer (or delegated Deputy Information Officer/s) is responsible for:

- keeping the Management Team and/or Board of Governors and/or Board of Trustees of the School updated about the school's responsibilities under POPIA;
- continually analysing POPIA regulations and/or notices issued by the Information Regulator in order to align these with this Policy and procedures thereto;
- ensuring that the school has accessible processes in place that makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the school;

- approving any contracts entered into with operators, employees and other third parties which may have an impact on the Personal Information held by the school;
- oversee the amendment of the school's employment contracts and other service level agreements;
- ensure that employees and other persons acting on behalf of the school are fully aware of the risks associated with the processing of personal information and that they remain informed about the school'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 school;

**Employees and other persons acting on behalf of the school**

Employees and other persons acting on behalf of the school will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain pupils, parents, suppliers and other employees. Employees and other persons acting on behalf of the school are required to treat personal information as a confidential business asset and to respect the privacy of Data Subjects in the following manner:

- employees and other persons acting on behalf of the school may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the school 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 school must request assistance from their 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 school 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 school or of a third party to whom the information is supplied.

**Employees and other persons acting on behalf of the school 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 smartphones (except where it is required to perform their teaching duties). All personal information must be accessed and updated from the school's administrative system or centralised google drive;
- share personal information informally- in particular, personal information should never be sent by email, as this form of communication is not secure; or
- transfer personal information outside of South Africa without the express permission from the Information Officer

**Employees and other persons acting on behalf of the school 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 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 media 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 parent or customer phones or communicates via email;

- 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 Information Officer to delete or dispose of the personal information in the appropriate manner;
- undergoing POPIA Awareness training from time to time; and
- reporting any suspicious activity, security breach, interference, modification, destruction or the unsanctioned disclosure of personal information, immediately to the Information Officer.

## Disciplinary action

Where a POPIA complaint or a POPIA infringement investigation has been finalised, Calling Education NPC 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 school 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 school may enter into a disciplinary process with the employee which may result in dismissal. 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.

| **Annexure A: PERSONAL INFORMATION REQUEST FORM** |
|---|

*Please submit the completed form to the Information Officer below:*

| | |
|---|---|
| Name | |
| Email address | |

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

| **Particulars of Data Subject** | |
|---|---|
| Name and surname | |
| Identity number | |
| Mobile number | |
| Email address | |
| Years associated with Calling Education NPC | |

| **Request** | |
|---|---|
| I request Calling Education NPC to: | |
| | Inform me where the school holds my personal information |
| | Provide me with a record or description of my personal information |
| | Correct or update my personal information |
| | Destroy or delete a record of my personal information |

| | |
|---|---|
| Signature | |
| Date | |

| **Annexure B: POPIA Complaint Form** |
|---|

| We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act. Please submit the completed form to the Information Officer below: | |
|---|---|
| Name | |
| Email address | |

Where we are unable to resolve your complaint to your satisfaction you have the right to complain to the Information Regulator who can be contacted at http://www.justice.gov.za/inforeg/index.html

| **Particulars of Complaint** | |
|---|---|
| Name and surname | |
| Identity number | |
| Mobile number | |
| Email address | |
| Years associated with Calling Education NPC | |

| **Details of complaint:** |
|---|
| |
| |
| |

| **Desired outcome** | |
|---|---|
| | |
| | |
| Signature | Date |