Assumption Convent School

"It is only through the practice of virtue that respect and honour can be gained"

ESTABLISHED 1946

"Fully Alive" John 10:10

6 weeks to Grade 12

P.O. Box 752127 Garden View, 2047
Cnr Mullins & Pandora Roads, Germiston
Telephone: (011) 616 5053
Fax; (011) 622 6075
admin@assumptionconvent.co.za
www.assumptionconvent.co.za

Protection of Personal Information Policy

Introduction

Assumption Convent collects, processes and use certain information about individuals. These include but are not limited to Students, parents, faculty, and supplier information.

This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards as well as to comply with the data privacy requirements as prescribed by the POPI Act of 2013.

Why this policy exists. This data protection policy ensures Assumption Convent:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, students, parents, and 3rd Parties.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Protection of Personal Information Act

The Protection of Personal Information Act 2013 describes how organisations — including Assumption Convent— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Protection of Personal Information Act is underpinned by eight important conditions. These say that personal information must adhere to:

1. Accountability
2. Processing limitations
3. Purpose specification
4. Further processing limitations

5. Information Quality
6. Openness
7. Security Safeguards
8. Data Subject Participation

People, risks, and responsibilities

Policy scope

This policy applies to:

- Assumption Convent
- All staff and volunteers of Assumption Convent
- All contractors, suppliers and other people working on behalf of Assumption Convent.

It applies to all information that the company holds relating to identifiable individuals, even if that information technically falls outside of the Protection of Personal Information Act of 2013. This can include but not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- any other information relating to Students, employees, parents, and 3rd parties.

Data protection risks

This policy helps to protect Assumption Convent from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Assumption Convent has some responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Information Officer (more than likely the MD of a business) is ultimately responsible for ensuring that Assumption Convent study meets its legal obligations.

- The [Deputy Information Officer], Japie Goosen and Anita Nienaber are responsible for:

1. Keeping the board updated about data protection responsibilities, risks, and issues.

2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
3. Arranging data protection training and advice for the people covered by this policy.
4. Handling data protection questions from staff and anyone else covered by this policy.
5. Dealing with requests from individuals to see the data Assumption Convent holds about them (also called 'subject access requests').
6. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The IT Team are responsible for:

    a. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    b. Performing regular checks and scans to ensure security hardware and software is functioning properly.
    c. Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

- The Marketing Team are responsible for:

    d. Approving any data protection statements attached to communications such as emails and letters.
    e. Addressing any data protection queries from journalists or media outlets like newspapers.
    f. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
    g. Ensuring that all necessary burden of proof and consent are obtained directly from parents when using the school's social media platforms and utilising the student's images.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers or in consultation with the Deputy Information Officers.
- Assumption Convent will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking reasonable precautions and following the guidelines below.
- In particular, strong passwords must be used, and they should never be shared. These passwords should be regularly updated to ensure that the faculty staff data does not get compromised.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be discarded in a manner that is compliant with the school's data retention policies.

- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or in classroom desks.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Assumption Convent unless the school can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the borders of South Africa unless you are contractually obligated to do so.

- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Assumption Convent to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort [Assumption Convent should put into ensuring its accuracy.

It is the responsibility of all school administration who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Assumption Convent will make it easy for data subjects to update the information Assumption Convent holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. Assumption Convent will communicate to both parents of students and faculty to ensure that the information on record is accurate. This includes annual communication to parents and a way parents can periodically update their information beyond the annual updates.

Data Subject access requests

- All individuals who are the subject of personal data held by Assumption Convent are entitled to:
- Ask what information the school holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

Should an individual request such information, this will follow the POPI act, and a nominal fee can be charged at the discretion of the information officer. Notably there are times that this request can be denied upon review of the request and will be assessed on a case-by-case basis and outcomes of these assessments will be communicated to the requestor.

Disclosing data for other reasons

In certain circumstances, the Protection of Personal Information Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Assumption Convent will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Assumption Convent aims to ensure that individuals are aware that their data is being processed through the information Lifecycle, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]