Alliance Française
Port Elizabeth

DATA PROTECTION POLICY

In compliance with the Protection of Personal Information Act ("POPIA") of 26 November 2013

+27 (0) 41 585 7889 - admin@pe.alliance.org.za
17 Mackay Street, Port Elizabeth, 6006
https://pe.alliance.org.za

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Alliance Française de Port Elizabeth. This includes obligations in dealing with personal data, inorder to ensure that the organisation complies with the requirements of the POPIA.

RATIONALE

Alliance Française de Port Elizabeth must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by Alliance Française de Port Elizabeth in relation to its staff, service providers and clients in the course of its activities. Alliance Française de Port Elizabeth makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

SCOPE

The policy covers both personal and sensitive personal data held in relation to data subjects by Alliance Française de Port Elizabeth. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by Alliance Française de Port Elizabeth. Both categories will be equally referred-to as Personal Data in this policy, unless specificallystated otherwise.

DEFINITIONS

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller.
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Information Manager	A person appointed by Alliance Française de Port Elizabeth to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients.
Information and Data Protection Officer	The Director of the Alliance Française de Port Elizabeth is the Information and Data Protection Officer, fully responsible for the compliance to thePOPIA.
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.
Consent	Freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.

ALLIANCE FRANÇAISE DE PORT ELIZABETH AS A DATA CONTROLLER

In the course of its daily organisational activities, Alliance Française de Pretoria acquires, processes and stores personal data in relation to:

- Employees of Alliance Française de Port Elizabeth (HR Data)
- Customers of Alliance Française de Port Elizabeth, including within the Language Centre, ExamCenter, Cultural Centre, Library and Translation Service

In accordance with the POPIA, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, Alliance Française de Port Elizabeth is committed to ensuring that its staff has sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Information manager is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by Alliance Française de Port Elizabeth, there is regular and active exchange of personal data between Alliance Française de Port Elizabeth and its Data Subjects. However, Alliance Française de Port Elizabeth exchanges no personal data with Data Processors on the Data Subjects'behalf, as all exchange of data is within Alliance Française de Port Elizabeth only.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that an Alliance Française de Port Elizabeth staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Information manager to seek clarification.

SUBJECT ACCESS REQUESTS

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Information manager, and will be processed as soon as possible, but must be concluded within one month, with no undue delay.

It is intended that by complying with these guidelines, Alliance Française de Port Elizabeth will adhere to best practice regarding the applicable Data Protection legislation.

THIRD-PARTY PROCESSORS

In the course of its role as Data Controller, Alliance Française de Port Elizabeth engages with no Data Processors to process Personal Data on its behalf. All data processing is internal to Alliance Française de Port Elizabeth, and no exchange of information with external Data Controllers or other Third-Party processors occurs, save for its Translation Service, where customers consent to their documents, for which they want translated, to be sent to external approved translators working on a case-by-case contractual basis.

THE DATA PROTECTION PRINCIPLES

The following key principles are fundamental to Alliance Française de Port Elizabeth's Data Protection policy. In its capacity as Data Controller, Alliance Française de Port Elizabeth ensures that all data shall:

1. BE OBTAINED AND PROCESSED FAIRLY AND LAWFULLY.

For data to be obtained fairly, the Data Subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller (Alliance Française de Port Elizabeth);
- The purpose(s) for which the data is being collected;
- The person(s) to whom the data may be disclosed by the Data Controller;
- The legal basis for processing the data;
- The retention periods of the data;
- The right of complaint where Data Subjects are dissatisfied with the implementation of the above criteria;
- Their individual rights under the General Data Protection Regulation.

Alliance Française de Port Elizabeth will meet this obligation in the following way.

- The informed consent of the Data Subject will always be sought before their data is processed, which must be specific, unambiguous and freely given to the Data Controller, by way of a positive indication of agreement, and thus cannot be inferred from silence, pre-ticked boxes or inactivity;
- Where Alliance Française de Port Elizabeth intends to record activity on CCTV or video, a Fair processing Notice will be posted in full view.

- Processing of the personal data will be carried out only as part of Alliance Française de Port Elizabeth's lawful activities, and Alliance Française de Port Elizabeth will safeguard the rights and freedoms of the Data Subject;
- In compliance with the POPIA, data will only be processed if the individual has given clear consent for Alliance Française de Port Elizabeth to process their Personal Data for a specific purpose, which will be disclosed to the Data Subject before processing of their data, and listed in ;
- The retention periods of the data, which differ depending on the specific data category, will be conveyed clearly to the Data Subject before their data is processed, and will be relevant to the individual Data Subject;
- The individual rights of the Data Subject, including their right to complaint, will be posted in full view, both online and in the premises of Alliance Française de Port Elizabeth, and adequate training will be given to relevant staff members to whom the Data Subjects can request a moredetailed explanation;
- The data of the Data Subject will not be shared with a third party, with the exception of customers of the Translation Service, where documents to be translated are submitted to external approved translators.

2. BE OBTAINED ONLY FOR ONE OR MORE SPECIFIED, LEGITIMATE PURPOSES.

Alliance Française de Port Elizabeth will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which Alliance Française de Port Elizabeth holds their data, and Alliance Française de Port Elizabeth will be able to clearly state that purpose or purposes, and will, at least every year, verify its accountability for said purposes. These purposes are listed, too, in the attached Data Purpose and Accountability List.

3. ..... NOT BE FURTHER PROCESSED IN A MANNER INCOMPATIBLE WITH THE SPECIFIED PURPOSE(S).

Any use of the data by Alliance Française de Port Elizabeth will be compatible with the purposes for which the data was acquired, as outlined in the Data Purpose and Accountability List.

4. BE KEPT SAFE AND SECURE.

Alliance Française de Port Elizabeth will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Alliance Française de Port Elizabeth in its capacity as Data Controller. In such a case that data has been breached in any way, the appropriate measures will be taken, in accordance with the attached Data Breach Procedure.

Access to and management of staff and customer records is limited to those staff members who have appropriate authorisation and password access, in its automated format. Data held in manual format are locked and secured in filing cabinets, which are in a secure location, beyond which only appropriate staff can access with a door password and authorisation.

5. BE KEPT ACCURATE, COMPLETE AND UP-TO-DATE WHERE NECESSARY

Alliance Française of Port Elizabeth will :

+27 (0) 41 585 7889 - admin@pe.alliance.org.za
17 Mackay Street, Port Elizabeth, 6006
https://pe.alliance.org.za

+27 (0) 41 585 7889 - admin@pe.alliance.org.za
17 Mackay Street, Port Elizabeth, 6006
https://pe.alliance.org.za

ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;

- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. Alliance Française de Port Elizabeth conducts a review of sample data every year to ensure accuracy; staff contact details are reviewed and updated every year, and when a new staff member joins Alliance Française de Port Elizabeth;
- conduct regular assessments in order to establish the need to keep certain Personal Data, an account of which is found in the attached Data Purpose and Accountability List;
- ensure that any data which may be inaccurate or incomplete, and which has been highlighted by the Data Subject as such, will be updated and reviewed when given notification within the time-limits specified in the attached Subject Access Request document.

6. ... BE ADEQUATE, RELEVANT AND NOT EXCESSIVE IN RELATION TO THE PURPOSE(S) FOR WHICH THE DATA WERE COLLECTED AND PROCESSED.

Alliance Française de Port Elizabeth will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained, as outlined in the attached Data Purpose and Accountability List.

7. NOT BE KEPT FOR LONGER THAN IS NECESSARY TO SATISFY THE SPECIFIED PURPOSE(S).

Alliance Française de Port Elizabeth has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manualand automated format.

Once the respective retention period has elapsed, Alliance Française de Port Elizabeth undertakes to destroy, erase or otherwise put this data beyond use.

8. ... BE MANAGED AND STORED IN SUCH A MANNER THAT, IN THE EVENT A DATA SUBJECT SUBMITS A VALID SUBJECT ACCESS REQUEST SEEKING A COPY OF THEIR PERSONAL DATA, THIS DATA CAN BE READILY RETRIEVED AND PROVIDED TO THEM.

Alliance Française de Port Elizabeth has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

DATA SUBJECT ACCESS REQUESTS

As part of the day-to-day operation of the organisation, Alliance Française de Port Elizabeth's staff engages in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by Alliance Française de Port Elizabeth, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which Alliance Française de Port Elizabeth must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached SubjectAccess Request process document.

Alliance Française de Port Elizabeth's staff will ensure that, where necessary, such requests are forwarded to the Information manager in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than one month from receipt of the request.

IMPLEMENTATION

As a Data Controller, Alliance Française de Port Elizabeth ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation. Alliance Française de Port Elizabeth does not exchange data, or have it processed thereof, by a Data Processor. In the circumstance that this should change, Data Subjects will be made aware, and the relevant documentation shall be updated.

In such a circumstance, failure of a Data Processor to manage Alliance Française de Port Elizabeth's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of Alliance Française de Port Elizabeth s staff to process Personal Data in compliance with this policymay result in disciplinary proceedings.

DATA MAPPING

The Alliance Française de Port Elizabeth has the following data:

Department	Type of Data	Where is the Data	Data protection

Language Centre	• Name
	• Mobile Phone Number
	• Email Address
	• Home Address
	• Gender
	• Nationality
	• Date of Birth
	• Reason for Registration
	• Class History
	• Accounting History
	  ○ Type (Bill/Payment/Credit/Refund)
	  ○ Mode (Cash/Card)
	  ○ Date of Payment
	  ○ Payment Amount
		Program
		ARC EN CIEL
		Jotform
		Xero
			Encrypted and password protected

Exam Center	• Name • Mobile Phone Number • Email Address • Home Address • Gender • Nationality • Date of Birth	Program DELF PROG (FEI)	Encrypted and password protected

	• Mother Tongue • Place of Birth	Program PARAGRAPHE (CCIP PARIS)	Encrypted and password protected

Translation Service	• Name
	• Mobile Phone Number
	• Email Address
	• Home Address
	• Gender
	• Nationality
	• Date of Birth
	• Reason for Registration
	• Accounting History
	  ○ Type (Bill/Payment/Credit/Refund)
	  ○ Mode (Cash/Card)
	  ○ Date of Payment
	  ○ Payment Amount
	• Document for Translation
		Excel sheets on the AF's Google drive	Encrypted and password protected

Department	Details of Personal Data	Where is the data	Data Protection

Cultural Centre	Mandatory Data:
	• Name
	• Email
	
	Optional Data that we may have:
	• Pictures of events
	• Accounting History (if for a paid event)
	  ○ Type (Bill/Payment/Credit/Refund)
	  ○ Mode (Cash/Card)
	  ○ Date of Payment
	  ○ Payment Amount
		Mailchimp
		Program Xero
		
		Documents on the AF's Google drive
			Encrypted and password protected
			
			Restricted access to the service and

			password protected
Library	Mandatory Data: • Name • Date of Birth • Mobile Phone Number • Email Address • Home Address	Program PMB	Encrypted and password protected

Finances and Administration	• Emails
	• Accounting History (if for a paid event)
	  ○ Type (Bill/Payment/Credit/Refund)
	  ○ Mode (Cash/Card)
	  ○ Date of Payment
	  ○ Payment Amount
		Outlook
		Program
		Xero
			Encrypted and password protected

	• Covid screening forms	Stored at the Director's office	Destroyed every six month
	• CCTV recordings	Program Tactical Edge	Destroyed every two weeks
	• Name of the staff and Members • Date of Birth of the staff and Members • Mobile Phone Number of the staff and Members • Email Address of the staff and Members • Home Address of the staff and Members • Visa status of the staff	Documents on the AF's Google drive	Encrypted and password protected

DATA BREACH PROCEDURE

1. Introduction

1.1 This policy sets out the policy and procedure of Alliance Française de Port Elizabeth in relation to detection and response to personal data breaches, and notification of the breach to the datacontrollers, the relevant authorities, and the subjects.

1.2 When dealing with a breach, Alliance Française de Port Elizabeth must focus primarily on the protection of individuals, as well as protecting the interests of the institution.

2. Definitions

2.1 the following phrases are defined;

a) 'Appointed Person' – this is the person who has been appointed to deal with data protection and data breach procedure within Alliance Française de Port Elizabeth, i.e. the Information Manager;
b) 'Data Breach' - a data breach occurs when personal information is lost or subjected to unauthorised access, modification, use, disclosure or other misuse;
c) 'Data Controller' – an entity that possesses and controls data;
d) 'Data Processor' – an entity that is in the possession of data controlled by another entity;
e) 'Data Subject' – an identifiable/identified natural person. They can be identifiable using a personal identifier such as their name, identification number, phone number, etc.;
f) 'Personal Data' – personal data is any data which relates to a Data Subject;
g) 'Supervisory Authority' – the supervisory authority is the Information and Data Protection Officer;
h) 'Manual Data' – data kept in hard copy format;
i) 'Automated Data' – data kept in a digital format.

3. Detecting personal data breaches

3.1 Technological Measures

The kinds of data held by Alliance Française de Port Elizabeth are sensitive and as such, technological measures have been put in place to detect any interference with data or any incidents which may result in personal data breaches. As of the publication of this policy, these include:

a) The placing of all manual data (including but not limited to: application forms, examination certificates, documents for translation, printed materials etc.) in secured filing cabinets;
b) The placing of all automated data on computers within the organisation, which are only accessible by a passcode, in encrypted folders which are only accessible by an additional passcode;
c) Arc-en-Ciel, the learning centre management software used by Alliance Française de Port Elizabeth's Language Centre and Examination Centre, as well as administration, is encrypted, and access to the data on it (which includes but is not limited to the name, contact details, date of birth, billing address and accounting history of clients of Alliance Française de Port Elizabeth) is restricted only to those within Alliance Française de Port Elizabeth, and is accessible only by a passcode;

d) PMB, the library management software used by Alliance Française de Port Elizabeth s Library (known as the *"Médiathèque"*), is encrypted, and access to the data on it (which includes only the name, contact details, date of birth and home address of the clients of the Library), is restricted only to those within the Alliance Française de Port Elizabeth;
e) Mailchimp, the mailing lists management and automation platform, is encrypted, and access to the data on it (which includes only your email address) is restricted only to those within Alliance Française de Port Elizabeth, and is accessible only by a passcode;
f) All data, including miscellaneous data not mentioned above, in both manual and automated form, is protected and/or encrypted on our servers, and no dissemination or distribution of this data occurs outside of Alliance Française de Port Elizabeth, and is internal to our own operations, which keeps the data safe and secure within AllianceFrançaise de Port Elizabeth.

3.2 Organisational Measures

Organisational measures have been put in place to detect any interference with data or any incidents which may result in personal data breaches. As of the publication of this policy, these include:

a) Alliance Française de Port Elizabeth has trained each of its staff and will continue to informthem on matters regarding data protection and data breach;
b) Personnel in administration and those who receive and input information from clients (specifically at Reception and in the Library) have been further trained in how best to approach incidents resulting in personal data breaches, including but not limited to: information regarding data, data protection, data breach procedure, personal data that we may have on a client, Subject Access Request forms, appropriate procedure should they receive a notification of data breach, etc.;
c) Alliance Française de Port Elizabeth will ensure to regularly assess the encryption of data, and the filing thereof, and ensure that data is fully protected and secured at all times;
d) Alliance Française de Port Elizabeth will regularly update staff on any changes or data breaches;
e) Alliance Française de Port Elizabeth will have a stable and efficient system for reporting databreaches (section 4 and 5);

3.3 Alliance Française de Port Elizabeth will regularly review the above measures. Such measures will be reviewed annually, or after the instance of a data breach.

4. Responding to personal data breaches

4.1 Any of the personnel must notify the appointed person immediately if they become aware of any data breach, whether actual or possible. All staff will be notified of this.

4.2 The appointed person is responsible for investigation of possible and actual data breaches and determining whether there is an obligation to notify. Where it is determined that there is an obligation to do so, the appointed person must notify the relevant parties in accordance with the notification policy (Section 7 of this document).

4.3 All personnel must cooperate with the appointed person in the investigation and detection of personal data breaches. All staff will be notified of this.

4.4 It is the duty of the appointed person to determine the role of Alliance Française de Port Elizabeth where there is a personal data breach. They must, therefore, determine whether Alliance Française de Port Elizabeth is acting as a data controller or a data processor in this particular instance.

Alliance Française de Port Elizabeth has acted as a *data controller* in relation to the following categories (this list is non-exhaustive); the names, addresses, ages, phone numbers, and accounting history of people. Keeping or processing data concerning living people constitutes controlling data.

Alliance Française de Port Elizabeth has not acted as a *data processor* in relation to data which is being held or processed by Alliance Française de Port Elizabeth on behalf of someone else. All data within Alliance Française de Pretoria has been collected and distributed solely within Alliance Française de Port Elizabeth, for use within Alliance Française de Port Elizabeth only.

4.5 The steps taken by the appointed person should include (in no particular order):

a) Assessing the risk of the subjects of the data;
b) Ensuring the containment of the breach insofar as possible and as soon as possible;
c) Gathering and collating data from all relevant sources in a way that does not compromise the data;
d) Considering the relevant impact assessments;
e) Informing the relevant parties within Alliance Française de Port Elizabeth, and those that aresubjects of the data of the breach and investigation;
f) Assessing the level of risk to Alliance Française de Port Elizabeth;
g) Notifying the supervisory authorities, data controllers, subjects and others in accordance to policy set out in this document.

4.6 Alliance Française de Port Elizabeth has a duty to keep a record of the response to personal data breach. The appointed person has a responsibility for this. This includes the facts of the breach itself, the effects (if any) of the breach and actions that were taken in relation to the breach. This record will be kept with any others in an official register of Alliance Française de Port Elizabeth concerning data breaches.

5. Notification to supervisory authority

5.1 This section applies to personal data breaches in which Alliance Française de Port Elizabeth is actingas a data controller (outlined in section 4.4).

5.2 Alliance Française de Port Elizabeth must notify the supervisory authority (the Office of the Data Protection Commissioner) of any personal data breach to data covered by this section without undue delay where feasible, within 72 hours. Exceptions are detailed in subsection 5.4.

5.3 Notifications to the supervisory authority will be made by the appointed person using the appropriate form. This will be sent to the Office of the Data Protection Commissioner securely

and confidentially, for example by email or post if practicable. A record of these notifications will be kept by the appointed person and all responses pertaining to it from the supervisory authority in the same register mentioned in subsection 4.6.

5.4 Alliance Française de Port Elizabeth will not notify the supervisory authority if it is unlikely that the personal data breach will result in a risk to the personal rights and freedoms of natural persons. The appointed person is responsible for determining if this applies. A record must be made of the decision not to notify. It must be stored in the same register mentioned in subsection 4.6.

5.5 Any additional information must be sent to the supervisory authority by secure and confidential means, as well as any changes in facts affecting notification under this section.

6. Notification to data controller:

6.1 This section applies to personal data breaches in which Alliance Française de Port Elizabeth is actingas a data processor (outlined in section 4.4).

6.2 Alliance Française de Pretoria does not act as a data processor, and has no contracts wherein it is the data processor for any entity outside of Alliance Française de Port Elizabeth and thereforea data processing notification procedure does not apply.

6.3 This section of the policy will be updated and amended should Alliance Française de Port Elizabeth act as a data processor for any reason.

7. Notification to data subjects:

7.1 This section applies to personal data breaches in which Alliance Française de Port Elizabeth is actingas a data controller (outlined in section 4.4).

7.2 Data subject notifications are made in consultation with supervisory authority, the breach has been confirmed or it is deemed necessary to do so.

7.3 There is an obligation on Alliance Française de Port Elizabeth to notify all subjects of a data breach as soon as is possible, and by secure and confidential means. The appointed person will keepa record of this. It must be stored in the same register mentioned in subsection 4.6.

7.4 Notifications to the data subjects will be made by the appointed person. This will be sent to the data subjects securely and confidentially, for example by post if practicable. A record of these notifications will be kept by the appointed person and all responses pertaining to it from the supervisory authority in the same register mentioned in subsection 4.6.

7.5 Alliance Française de Port Elizabeth will not notify the data subjects if it is unlikely that the personal data breach will result in a risk to the personal rights and freedoms of natural persons. The appointed person is responsible for determining if this applies. A record must be made of the decision not to notify. It must be stored in the same register mentioned in subsection 4.6.

7.6 Other notifications may be required due to contract. The appointed person should consider whether it is appropriate to notify other parties of the breach.

8. Reviewing and updating this policy

8.1 The persons responsible for reviewing and updating the policy are the Director of Alliance Française de Port Elizabeth and the committee of the Alliance Française de Port Elizabeth.

8.2 The policy will be reviewed annually, by the director of the Alliance Française de Port Elizabeth.

8.3 The policy may be reviewed ad hoc after a breach or possible breach that highlights issues that should be addressed or changed in this policy.

8.4 The matters to be considered upon review include changes in technology, breaches that have occurred since the last review, if any, and the types of data that are being collected at present.

DATA RETENTION AND DESTRUCTION POLICY

1. INTRODUCTION

1.1. Introduction

1.1.1. This Data Retention and Destruction Policy (the "DRDP") has been adopted by Alliance Française de Port Elizabeth in order to set out the principles for retaining, reviewing and destroying data. The DRDP covers all employees of Alliance Française de Port Elizabeth.

1.1.2. The DRDP covers all data retained by Alliance Française de Port Elizabeth in whatever medium such data is contained in. The DRDP is not therefore restricted to information contained in paper documents ("manual form") but includes data contained in an electronically readable format ("automated form"). For the purposes of convenience, in this DRDP, the medium which holds data is called "a Document".

1.1.3. This DRDP should be read in conjunction with other policies that have as their objectives the protection and security of data, such as the Data Protection Policy and the Data Breach Procedure.

1.1.4. Alliance Française de Port Elizabeth has five distinct departments ("Centre") which include the Language Centre, the Translation Service, the Library (*'Médiathèque'*), the Examination Centre and the Cultural Centre.

1.2. Objectives

1.2.1. Alliance Française de Port Elizabeth is bound by various obligations with regard to the data that it retains. These obligations include how long data is retained and when and how it can be destroyed.

1.2.2. Further, Alliance Française de Port Elizabeth may be involved in unpredicted events such as litigation or business disaster recoveries that require to have access to the original Documents in order to protect Alliance Française de Port Elizabeth's interests or those of ouremployees or customers.

1.2.3. As a result, Documents may need to be archived and stored for longer than the data may be needed for day-to-day operations and business processes. A student may, for example, have not been a client since two years prior to their subscription, and thus shall expire after said two years, but other Documents may, by law, need to be retained for a longer period.

1.2.4. Broadly, when the Document Retention Period is over, it ought to be destroyed in the proper manner.

2. RETENTION POLICY

2.1. Retention is defined as the maintenance of documents in a production or live environment which can be accessed by an authorised user in the ordinary course of business. For the avoidance of doubt, Documents used or draft versions of Documents shall not be retained beyond their active use period nor copied into production or live environments.

2.2. The retention period of a Document shall be an active use period of two years unless an exception has been obtained permitting a longer or shorter active use period by a specific unit ("Centre") responsible for creating, using, processing, disclosing, storing and destroying the Document.

2.3. After active use has expired and according to appropriate exceptions, Documents shall be archived in accordance with section 3 until the Documents are destroyed in accordance with section 4.

2.4. For the purposes of enforcing retention in accordance with this policy, each Centre is responsible for the Documents it creates, uses, stores, processes and destroys. A sample list of document types across Alliance Française de Port Elizabeth by Centre is in the adjoined Data Retention Periods list. The list shall be maintained by each Centre.

2.5. Each employee in charge of each Centre shall be responsible for enforcing the retention, archiving and destruction of Documents, and communicating these periods to the relevant employees.

2.6. Each employee in charge of each Centre shall be responsible for submitting exception requests to the process, including consulting and receiving legal advice if necessary to justify making an exception request under section 5.

2.7. Each employee shall be responsible for returning Documents in their possession or control to Alliance Française de Port Elizabeth upon separation or retirement. Final disposition of such Documents shall be determined by the immediate supervisor in accordance with this policy.

3. ARCHIVING POLICY

3.1. Archiving is defined as secured storage of Documents such that Documents are rendered inaccessible by authorised users in the ordinary course of business but which can be retrieved by an administrator designated by the employee in charge of each Centre for the Documents in question.

3.1.1. Paper records shall be archived in secured storage onsite, clearly labelled in archive boxes naming the employee in charge of the Centre and date to be destroyed.

3.1.2. Electronic records shall be archived in accordance with Alliance Française de Port Elizabeth's secured, encrypted folder on the computer of the Information manager, with access to said encrypted folder only accessible by a variety of security measures, including a passcode and decryption code, which is secured furthermore in hard copy in a securedfiling cabinet.

3.2. The archiving period of a document shall be seven (7) years unless an exception has been obtained permitting a longer or shorter active use period by the employee in charge of the Centre responsible for creating, using, processing, disclosing, storing and destroying the Document.

3.2.1. An archiving period of more than seven (7) years may be granted by exception for Documents with a vital historical purpose such as corporate records, client history, contracts and technical knowhow, for example. The employee in charge of each Centre will request an exception in accordance with section 5 to archive Documents. Such exception request shall specify the administrative, organisational and technical measures to be undertaken to ensure the confidentiality, integrity and availability of such Documents.

3.2.2. An archiving period of less than seven (7) years may be granted by exception for documents with a limited business purpose such as emails.

3.3. After the archival period has expired, Documents shall be destroyed in accordance with section 4.

3.4. For the purposes of enforcing archiving in accordance with this policy each Centre is responsible for the Documents it creates, uses, stores, processes and destroys. A sample list

of Document types across Alliance Française de Port Elizabeth is found in the adjoined Data Retention Periods list. The list shall be maintained by each employee in charge of a Centre.

3.5. The employee in charge of each Centre shall be responsible for enforcing the retention, archiving and destruction of Documents, and communicating these periods to the relevant employees.

4. DESTRUCTION POLICY

4.1. Destruction is defined as physical or technical destruction sufficient to render the information contained in the Document irretrievable by ordinary commercially available means.

4.2. Alliance Française de Port Elizabeth shall maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived whether in physical storage media such as USB keys, hard drives, mobile devices, portable devices or in database records or backup files. Paper Documents shall be shredded using secure, locked consoles designated which waste shall be periodically picked up by security screened personnel for disposal.

5. EXCEPTIONS TO THE RETENTION PERIOD

5.1. Exceptions may be requested under the following circumstances:

5.1.1. The employee in charge of each Centre shall review and submit to Alliance Française de Port Elizabeth an exception request to archive data for a different period as prescribed in the Data Retention Periods list. The reasons may be a client requirement, business requirement, legal requirement or vital historical purpose.

5.1.2. The Exception Request Form shall be reviewed and approved by Alliance Française de Port Elizabeth's Information manager.

6. RESPONSIBILITIES

6.1. The employee in charge of each Centre shall be responsible for implementing this DRDP and ensuring that employees understand this DRDP and that they perform the processes and procedures to execute this DRDP.

6.2. The Information manager shall be responsible for auditing compliance with this DRDP and providing an audit report with recommendations to be reviewed by Alliance Française de Port Elizabeth's Director.

7. ENFORCEMENT AND REPORTING BREACHES

7.1. Breaches of this DRDP may have serious legal and reputation repercussions, and could cause material damage to Alliance Française de Port Elizabeth. Consequently, breaches can potentially lead to disciplinary action that could include dismissal and legal sanctions, including criminalpenalties.

7.2. All employees are expected to promptly and fully report any breaches of the DRDP, as outlined in the attached Data Breach Procedure. Reports made in good faith by someone who has not breached this DRDP will not reflect badly on that person or their career at Alliance Française de Pretoria. Reports may be made using the following email address: admin@pe.alliance.org.za