SHIA ISLAMIC CENTRE
AL-JAAFARIA

Privacy and Confidentiality Policy

Privacy and Confidentiality Policy

Context

We aim to protect the privacy and confidentiality of all information and records about staff and management by ensuring continuous review and improvement on our current systems, storage, and methods of disposal of records. We will ensure that all records and information are held in a secure place and are only retrieved by or released to people who have a legal right to access this information.

Legislative Provisions

Privacy Act 1988
https://www.oaic.gov.au/privacy/the-privacy-act/

Privacy Amendments (Enhancing Privacy Protection) Act 2012
https://www.legislation.gov.au/Details/C2012A00197

Implementation

The Notifiable Data Breaches (NDB) scheme requires organisations to provide notice to the Office of the Australian Information Commissioner (formerly known as the Privacy Commissioner) and affected individuals of any data breaches that are 'likely' to result in 'serious harm'.

If we suspect an eligible data breach may have occurred, the Principal/CEO must undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected. A breach of an Australian Privacy Principle is viewed as an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.

Roles and Responsibilities

The Principal/CEO will:

- Ensure we act in accordance with the requirements of the Australian Privacy Principles and *Privacy Act 1988* by developing, reviewing, and implementing procedures and practices that identify:
    - What information we collect and the source of information;
    - Why the information is collected;
    - Who will have access to information;
    - Collection, storage, use, disclosure, and disposal of personal information collected by us;
    - Any law that requires the particular information to be collected;
    - Adequate and appropriate storage for personal information collected by us;
    - Protection of personal information from unauthorised access.

- Provide staff with relevant information regarding changes to Australian privacy law and policy;
- Ensure all relevant staff understand the requirements under Australia's privacy law and Notifiable Data Breaches (NDB) scheme;
- Maintain currency with the Australian Privacy Principles (this may include delegating a staff member to oversee all privacy-related activities to ensure compliance);
- Ensure personal information is protected in accordance with our obligations under the *Privacy Act 1988* and *Privacy Amendments (Enhancing Privacy Protection) Act 2012;*
- Regularly back-up personal and sensitive data from computers to protect personal information collected;
- Ensure all computers are password protected and install security software-anti virus protection;
- Ensure the appropriate and permitted use of images of children;
- Ensure information relating to staff employment will remain confidential and available only to the people directly involved with making personnel decisions.

Staff will:

- Read and adhere to the Privacy and Confidentiality Policy at all times;
- Ensure documented information and photographs of children are kept secure but may be accessed at any time by the child's parent/guardian;
- Treat private and confidential information with respect in a professional manner;
- Maintain individual and organisational information and store documentation according to this policy at all times;
- Not to share information about the individual or the organisation, management information, or other staff as per legislative authority.

APPENDIX ONE

THE AUSTRALIAN PRIVACY PRINCIPALS (APP)

The APP Outline

- The open and transparent management of personal information, including having a privacy policy
- An individual having the option of transacting anonymously or using a pseudonym where practicable
- The collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection
- How personal information can be used and disclosed (including overseas)
- Maintaining the quality of personal information
- Keeping personal information secure
- Right for individuals to access and correct their personal information

The APPs place more stringent obligations on APP entities when they handle 'sensitive information'. Sensitive information is a type of personal information and includes information about an individual's:

- Health (including predictive genetic information)
- Racial or ethnic origin
- Political opinions
- Membership of a political association, professional or trade association or trade union
- Religious beliefs or affiliations
- Philosophical beliefs
- Sexual orientation or practices
- Criminal record
- Biometric information that is to be used for certain purposes

Australian Privacy Principles (APPs)

APP 1 – Open and transparent management of personal information.
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up-to-date APP privacy policy.

APP 2 – Anonymity and Pseudonymity.
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 – Collection of solicited personal information.
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing with unsolicited personal information.
Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of the collection of personal information.
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use or disclosure of personal information.
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 – Direct marketing.
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-order disclosure of personal information.
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 – Adoption, use or disclosure of government related identifiers.
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information.
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information.
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information.
Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information.
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.