



GDPR Compliance and Privacy Policy

Indigenous Education Foundation Limited (IEF)

1. INTRODUCTION:

IEF is committed to protecting the rights and freedom of your personal data by safely and securely processing this data in accordance with our moral and legal obligations.

This Privacy Policy is designed to help you understand how we collect, use and protect personal information, and what to do if you have any questions, concerns or complaints.

In addition, this policy is to ensure that IEF personnel understand and comply with the rules governing their use of this data which they have access to via the course of their duties. The information we collect is yours, and you can choose to change or access it at any time.

2. WHAT IS GDPR?

Keeping information about clients and staff confidential makes clear business sense, but it is also required by law. The EU General Data Protection Regulation (GDPR) defines the ethical handling of personal data. Replacing legislation written before the digital age, the regulation became EU law in 2016, enforceable from 25th May, 2018.

3. SCOPE

This policy applies to all IEF personnel. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to privacy and website terms of use. We may supplement or amend this policy by additional policies

and guidelines from time to time. Any new or modified policy will be circulated to members before being adopted.

A. WHO IS RESPONSIBLE FOR THIS POLICY?

As our Data Protection Officer, **Sreehari Nair**, has overall responsibility for the day-to-day implementation of this policy.

4. DATA PROTECTION PRINCIPLES

IEF is committed to Processing data in accordance with its moral and legal responsibilities under guidance of the GDPR.

Article 5 of the GDPR requires that Personal Data shall be:

- a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, or further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) Accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisation measures required by GDPR in order to safeguard the rights and freedoms of individuals; and

- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. WHAT INFORMATION IS BEING COLLECTED?

A. PERSONAL INFORMATION

IEF will at times ask for information from our donors, program participants, volunteers and other members of the public to enable us a means to share our IEF activity updates and stay engaged with our audience. When we ask you for personal information we will at all times provide you a secure transmission method to send or share this data.

Examples of the personal information we collect includes:

- Your primary personal data, such as name and contact details;
- Other personal / profiling data, such as your family details, how you've previously supported or interacted with IEF, your personal comments; and
- Personal identifiers, such as your credit card details, where necessary.

B. SPECIAL CATAGORIES OF PERSONAL DATA

Previously known as *sensitive personal data*, this refers to data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases IEF does not request these special categories of personal data, however in rare cases where we do require this information we will also request the data subject's *explicit* consent. Unless otherwise required by law, any such consent clearly identifies what the relevant data is, why it is being processed and to whom it will be disclosed.

C. PERSONAL FINANCIAL DATA

IEF does not retain any financial data about donors or sponsors other than that required to verify that a relationship and/or transactions exists or has existed, as this information is required for transparency purposes and to demonstrate financial integrity.

IEF does not retain any credit card information or similar personal financial data. All electronic payment transactions operated through the IEF website or social media pages are handled by a secure and authorized third party which is contractually responsible for processing all credit card information and complying with applicable legislation.

6. ACCURACY AND RELEVANCE

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose.

IEF executes its own security policies, rules and technical measures to protect the personal data that we have under our control from:

- Unauthorized access
- Improper use or disclosure
- Unauthorized modification
- Unlawful destruction or accidental loss

A. Your personal data

You must take reasonable steps to ensure that the personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the IEF Data Protection Officer so that

they can update your records.

7. RESPONSIBILITIES

A. IEF responsibilities and objectives are to:

- Keep secure the personal data we hold;
- Check IEF procedures to ensure they cover all the rights of the individual;
- Identify and execute the lawful basis for processing data;
- Ensure consent procedures are lawful;
- Implement and review procedures to detect, report and investigate personal data breaches;
- Store data in safe and secure ways;
- Assess the risk that could be posed to individual rights and freedoms should data be compromised;
- Check that any data processing activities we deal with comply with our policy and are justified;
- Do not use data in any unlawful way;
- Comply with this policy at all times; and
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

B. IEF Data Protection Officer's responsibilities include:

- Keeping the board updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and policies on a regular basis;
- Facilitating data protection training and advice for all staff members and those included in this policy;
- Responding to questions about data protection from IEF staff, board members and other stakeholders; and
- Responding to individuals such as donors, employees and volunteers who wish to know which data is being held on them by IEF.

C. Responsibilities of the IT Systems Administrator include:

- Ensuring that all IEF's information technology systems, services, software and equipment meet acceptable security standards;
- Checking and scanning security hardware and software regularly to ensure it is functioning properly; and

- Researching any third-party services, such as cloud services, that IEF may consider using to store or process data in the future.

D. The processing of all data must be:

- Necessary to deliver our services; and
- In our legitimate interests and not unduly prejudice the individual's privacy.

8. TERMS OF USE

A. Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with this policy.

B. Transferring data internationally

IEF does not transfer any personal data internationally. Should there be a requirement for IEF to do so, it will only be done subject to a lawfully binding agreement between all parties involved.

C. Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. All subject access requests received must be referred immediately to IEF's Data Protection Officer.

D. Processing data in accordance with the individual's rights

IEF personnel must abide by any request from an individual not to use their personal data for direct marketing purposes and notify the data protection officer about any such request.

E. Storing data securely

- In cases when data is stored on printed paper, it is kept in a secure place where unauthorised personnel cannot access it;
- Printed data is securely disposed of when it is no longer needed;

- Data stored on a computer is protected by strong passwords that are changed regularly. We encourage all IEF staff to use complex passwords which are audited regularly;
- The IT Systems Administrator must approve any cloud-based storage system used to store data before executing;
- Servers containing personal data are kept in a secure location, with access significantly limited;
- Data is regularly backed up in line with the company's backup procedures;
- All servers containing sensitive data are approved and protected by security software; and
- All possible technical measures within reasonable practicality are put in place to keep data secure.

F. Rights of individuals

IEF recognise that individuals have rights to their data which must be respected and complied with to the best of our ability. IEF must ensure individuals can exercise their rights in the following ways:

1. Right to be informed:

- Privacy Notices are in place which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children; and
- Records kept of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access:

- Individuals are able to access their personal data and supplementary information; and
- Individuals are made aware of the lawfulness of the processing activities.

3. Right to rectification:

- Personal data of the individual is rectified or amended if requested by the data subject if it is inaccurate or incomplete; and
- Rectification is done without delay, and no later than one month. On rare occasions, this can be extended to two months with permission from the IEF data protection officer and approval of the data subject.

4. Right to erasure:

- IEF will delete or remove an individual's personal data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing:

- IEF will comply with any request to restrict, block, or otherwise suppress the processing of personal data; and
- IEF are permitted to store personal data if it has been restricted, but not process it further. IEF will retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability:

- Upon request, IEF will provide individuals with their data so that they can reuse it for their own purposes or across different services; and
- IEF will provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

G. Right to object

- IEF respects the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task;
- IEF respects the right of an individual to object to direct marketing, including profiling; and
- IEF respects the right of an individual to object to processing their data for scientific and historical research and statistics.

9. DEFINITIONS

A. GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

B. BUSINESS PURPOSES:

The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- *Compliance with our legal, regulatory and corporate governance obligations and good practice;*
- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests;*
- *Ensuring business policies are adhered to (such as policies covering email and internet use);*
- *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking;*
- *Investigating complaints;*
- *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments;*
- *Monitoring staff conduct, disciplinary matters;*
- *Marketing our charities; and*
- *Improving services.*

C. PERSONAL DATA:

Information relating to identifiable individuals, such as job applicants, current and former employees and volunteers, agency, contract and other staff, donors, subscribers, members, suppliers and business operational contacts.

Personal data we gather from IEF personnel may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

D. SENSITIVE PERSONAL DATA:

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data shall be strictly controlled in accordance with this policy.

E. PROCESSING:

Collecting, disclosing, storing, using or any other operation performed upon personal data. If you use personal data in any way you will be “processing” it.

10. CONTACT

To modify or delete your personal data held by IEF, either click the UPDATE YOUR PREFERENCES or UNSUBSCRIBE button links situated at the bottom of IEF e-communications; or, submit request to our Data Protections Officer via email or post. All requests, enquiries, breaches or other to be sent to:

IEF data protection officer email: it@iefprograms.org

IEF’s current Australian office address as listed on our website contact page: <http://www.iefprograms.org/contact>

All data breaches are recorded and actioned with IEF’s **Data Breach Response Plan within 72 hours.*

RELATED DOCUMENTS:

- IEF Data breach response plan
- IEF Data breach report form
- IEF Website content policy
- IEF Website terms of use
- General Data Protection Regulation EU 2016/679 (GDPR)
- Australian data protection act

AUTHORISATION:

Andrew Lunardi
IEF Secretary

| VERSION | LAST REVISED | APPROVED BY | NEXT REVISION |
|---------|--------------|-------------|---------------|
| 1.0 | 15-Oct-2019 | IEF Board | Oct-2020 |
| | | | |