INTERNATIONAL EDUCATION BOARD

Data Protection and Privacy Policy

Index

1. Preamble
2. Purpose
3. Scope
4. Definitions
5. Guiding Principles
6. Types of Personal Data Collected
7. Legal Basis for Processing
8. Data Collection Methods
9. Consent
10. Data Subject Rights
11. Data Sharing and Disclosure
12. International Data Transfers
13. Data Security Measures
14. Data Retention
15. Data Breach Management
16. Third-Party Data Processors
17. Website, Cookies, and Online Tracking
18. Children's Data and Vulnerable Persons
19. Automated Decision-Making and Profiling
20. Training and Awareness
21. Roles and Responsibilities
22. Policy Review
23. Disclaimer and Legal Position
24. Conclusion
25. Annexures
26. Document Control
27. Approval

---

1. Preamble

1.1. The International Education Board (IEB) is an independent, private, non-governmental, and non-statutory international education authority.

1.2. IEB operates as a voluntary quality assurance and accreditation body for educational institutions worldwide.

1.3. IEB is committed to protecting the privacy and personal data of all individuals who interact with the organization.

1.4. This policy establishes the framework for the collection, processing, storage, and protection of personal data by IEB.

1.5. IEB recognizes that personal data protection is a fundamental aspect of ethical organizational practice.

1.6. This policy reflects IEB's commitment to transparency, accountability, and respect for individual privacy rights.

1.7. IEB acknowledges the diverse legal frameworks governing data protection across jurisdictions.

1.8. This policy is designed to meet or exceed the standards of major international data protection frameworks.

1.9. IEB is not a government agency, statutory body, or regulatory authority in any jurisdiction.

1.10. IEB accreditation does not constitute government approval, statutory recognition, or professional licensure.

1.11. This policy applies to all personal data processing activities undertaken by IEB in the course of its operations.

---

2. Purpose

2.1. The purpose of this policy is to establish IEB's commitment to protecting personal data and privacy.

2.2. This policy defines the principles governing the collection and processing of personal data.

2.3. This policy specifies the rights of individuals regarding their personal data held by IEB.

2.4. This policy establishes procedures for secure handling, storage, and transfer of personal data.

2.5. This policy defines roles and responsibilities for data protection within IEB.

2.6. This policy ensures compliance with applicable data protection laws and best practices.

2.7. This policy provides guidance to IEB staff on their obligations regarding personal data.

2.8. This policy establishes procedures for responding to data breaches and security incidents.

2.9. This policy builds trust with stakeholders by demonstrating IEB's commitment to privacy.

2.10. This policy supports IEB's broader governance and ethical standards framework.

---

3. Scope

3.1. **Organizational Scope**

3.1.1. This policy applies to all IEB operations, activities, and functions.

3.1.2. This policy applies to all IEB staff, including employees, contractors, and consultants.

3.1.3. This policy applies to all IEB committees, panels, and governing bodies.

3.1.4. This policy applies to assessors, reviewers, and experts engaged by IEB.

3.1.5. This policy applies to third parties processing personal data on behalf of IEB.

3.2. **Data Scope**

3.2.1. This policy covers all personal data processed by IEB, regardless of format.

3.2.2. This policy applies to personal data in electronic and paper-based formats.

3.2.3. This policy covers personal data stored in databases, files, emails, and other systems.

3.2.4. This policy applies to personal data collected directly from individuals.

3.2.5. This policy applies to personal data obtained from institutions or third parties.

3.3. **Individual Scope**

3.3.1. This policy protects personal data of individuals associated with applicant institutions.

3.3.2. This policy protects personal data of individuals at accredited institutions.

3.3.3. This policy protects personal data of learners at IEB-accredited institutions.

3.3.4. This policy protects personal data of complainants, appellants, and grievants.

3.3.5. This policy protects personal data of IEB staff and governance members.

3.3.6. This policy protects personal data of website visitors and subscribers.

3.3.7. This policy protects personal data of event participants and attendees.

3.4. **Exclusions**

3.4.1. This policy does not apply to anonymized data that cannot identify individuals.

3.4.2. This policy does not apply to aggregated statistical data.

3.4.3. This policy does not govern data processing by accredited institutions themselves.

3.4.4. Accredited institutions are responsible for their own data protection compliance.

4. Definitions

4.1. **Personal Data** refers to any information relating to an identified or identifiable natural person.

4.2. **Data Subject** refers to an identified or identifiable natural person whose personal data is processed.

4.3. **Processing** refers to any operation performed on personal data, including collection, recording, storage, retrieval, use, disclosure, and destruction.

4.4. **Data Controller** refers to the entity that determines the purposes and means of processing personal data.

4.5. **Data Processor** refers to an entity that processes personal data on behalf of the data controller.

4.6. **Special Category Data** refers to sensitive personal data including racial or ethnic origin, political opinions, religious beliefs, health data, biometric data, and data concerning sexual orientation.

4.7. **Consent** refers to freely given, specific, informed, and unambiguous indication of agreement to the processing of personal data.

4.8. **Data Breach** refers to a security incident resulting in unauthorized access, disclosure, alteration, or destruction of personal data.

4.9. **Pseudonymization** refers to processing personal data so that it can no longer be attributed to a specific individual without additional information.

4.10. **Anonymization** refers to processing personal data so that it can no longer be attributed to any individual.

4.11. **Third Party** refers to any entity other than IEB, the data subject, and authorized data processors.

4.12. **Cross-Border Transfer** refers to the transfer of personal data to a country or organization outside the originating jurisdiction.

4.13. **Data Protection Officer (DPO)** refers to the individual responsible for overseeing IEB's data protection compliance.

4.14. **Privacy Notice** refers to information provided to data subjects about the processing of their personal data.

4.15. **Lawful Basis** refers to the legal grounds justifying the processing of personal data.

4.16. **Data Minimization** refers to limiting personal data collection to what is necessary for the specified purpose.

4.17. **Retention Period** refers to the duration for which personal data is stored before deletion or anonymization.

---

5. Guiding Principles

5.1. **Lawfulness, Fairness, and Transparency**

5.1.1. Personal data will be processed lawfully, fairly, and in a transparent manner.

5.1.2. IEB will only process personal data where a valid legal basis exists.

5.1.3. Individuals will be informed about how their personal data is used.

5.1.4. Privacy notices will be clear, accessible, and provided at the point of collection.

5.1.5. IEB will not process personal data in ways that are detrimental to individuals.

5.2. **Purpose Limitation**

5.2.1. Personal data will be collected for specified, explicit, and legitimate purposes.

5.2.2. Personal data will not be processed in a manner incompatible with those purposes.

5.2.3. Any change in purpose will be communicated to data subjects.

5.2.4. Further processing for archiving, research, or statistical purposes is permitted with safeguards.

5.3. **Data Minimization**

5.3.1. Personal data collected will be adequate, relevant, and limited to what is necessary.

5.3.2. IEB will not collect excessive personal data beyond stated purposes.

5.3.3. Data collection forms and processes will be designed to minimize data capture.

5.3.4. Regular reviews will identify and eliminate unnecessary data collection.

5.4. **Accuracy**

5.4.1. Personal data will be accurate and kept up to date where necessary.

5.4.2. Reasonable steps will be taken to ensure accuracy.

5.4.3. Inaccurate data will be corrected or deleted without delay.

5.4.4. Individuals are encouraged to inform IEB of changes to their personal data.

5.5. **Storage Limitation**

5.5.1. Personal data will be kept for no longer than necessary for the stated purposes.

5.5.2. Retention periods will be defined for different categories of personal data.

5.5.3. Personal data will be securely deleted or anonymized when no longer required.

5.5.4. Longer retention may be justified for legal, regulatory, or archival purposes.

5.6. **Integrity and Confidentiality**

5.6.1. Personal data will be processed securely to protect against unauthorized access.

5.6.2. Appropriate technical measures will be implemented to ensure security.

5.6.3. Appropriate organizational measures will be implemented to ensure security.

5.6.4. Personal data will be protected against accidental loss, destruction, or damage.

5.7. **Accountability**

5.7.1. IEB is responsible for demonstrating compliance with data protection principles.

5.7.2. Records of processing activities will be maintained.

5.7.3. Data protection impact assessments will be conducted where required.

5.7.4. Staff will be trained on data protection responsibilities.

5.7.5. Policies and procedures will be documented and regularly reviewed.

5.8. **Respect for Individual Rights**

5.8.1. IEB will respect and facilitate the exercise of data subject rights.

5.8.2. Requests from data subjects will be handled promptly and courteously.

5.8.3. IEB will not impede individuals from exercising their rights.

5.8.4. Information about rights will be communicated clearly to data subjects.

---

6. Types of Personal Data Collected

6.1. **Categories of Data Subjects**

6.1.1. Institutional representatives and contacts.

6.1.2. Academic and administrative staff at institutions.

6.1.3. Governance members and board directors of institutions.

6.1.4. Learners and students at accredited institutions.

6.1.5. Complainants, appellants, and grievants.

6.1.6. IEB staff, committee members, and assessors.

6.1.7. Website visitors and subscribers.

6.1.8. Event participants and attendees.

6.1.9. Suppliers, contractors, and service providers.

6.2. **Types of Personal Data**

6.2.1. **Identity Data:** Name, title, date of birth, gender, photograph.

6.2.2. **Contact Data:** Address, email address, telephone numbers.

6.2.3. **Professional Data:** Job title, employer, qualifications, professional experience.

6.2.4. **Educational Data:** Academic qualifications, transcripts, enrollment status.

6.2.5. **Financial Data:** Bank details, payment information, fee records.

6.2.6. **Communication Data:** Correspondence, emails, meeting records.

6.2.7. **Technical Data:** IP address, browser type, device information, login data.

6.2.8. **Usage Data:** Website interactions, preferences, feedback.

6.2.9. **Assessment Data:** Evaluation reports, reviewer comments, accreditation outcomes.

6.3. **Special Category Data**

6.3.1. IEB generally does not collect special category data.

6.3.2. Where special category data is collected, explicit consent or another valid basis is required.

6.3.3. Special category data may be collected in the context of complaints involving discrimination.

6.3.4. Health data may be collected for accessibility accommodations.

6.3.5. Special category data is subject to enhanced protection measures.

6.4. **Learner Data**

6.4.1. IEB may receive limited learner data from accredited institutions.

6.4.2. Learner data is used for verification and quality assurance purposes.

6.4.3. Learner data typically includes enrollment and completion information.

6.4.4. Detailed academic records are not routinely collected by IEB.

6.4.5. Learner data is processed in accordance with the principles in this policy.

---

7. Legal Basis for Processing

7.1. **Overview of Legal Bases**

7.1.1. IEB processes personal data only where a valid legal basis exists.

7.1.2. The legal basis depends on the purpose and context of processing.

7.1.3. IEB documents the legal basis for each processing activity.

7.1.4. Where multiple bases may apply, IEB identifies the primary basis.

7.2. **Consent**

7.2.1. Consent is obtained where processing is based on the individual's agreement.

7.2.2. Consent requests are clear, specific, and separate from other terms.

7.2.3. Consent is freely given without coercion or detriment for refusal.

7.2.4. Individuals may withdraw consent at any time.

7.2.5. Withdrawal of consent does not affect the lawfulness of prior processing.

7.2.6. Records of consent are maintained.

7.3. **Contractual Necessity**

7.3.1. Processing may be necessary for the performance of a contract with the individual.

7.3.2. This applies to processing required to provide services requested by the individual.

7.3.3. This applies to processing required to take steps at the individual's request before entering a contract.

7.3.4. Examples include processing institutional contact data to manage accreditation agreements.

7.4. **Legitimate Interests**

7.4.1. Processing may be necessary for IEB's legitimate interests.

7.4.2. Legitimate interests must not override the rights and freedoms of the individual.

7.4.3. A balancing test is conducted to assess the impact on individuals.

7.4.4. IEB's legitimate interests include quality assurance, organizational administration, and stakeholder communication.

7.4.5. Records of legitimate interest assessments are maintained.

7.5. **Legal Obligation**

7.5.1. Processing may be necessary to comply with legal obligations.

7.5.2. This includes obligations under employment law, tax law, and regulatory requirements.

7.5.3. The specific legal obligation is documented.

7.6. **Vital Interests**

7.6.1. Processing may be necessary to protect vital interests of an individual.

7.6.2. This basis applies in emergency situations involving life or health.

7.6.3. This basis is rarely relied upon in IEB's normal operations.

7.7. **Public Interest**

7.7.1. Processing may be necessary for tasks carried out in the public interest.

7.7.2. This may apply to certain quality assurance activities.

7.7.3. The public interest basis is documented where relied upon.

7.8. **Special Category Data**

7.8.1. Processing special category data requires an additional condition.

7.8.2. Explicit consent is the primary basis for special category data.

7.8.3. Processing may also be permitted for legal claims or substantial public interest.

7.8.4. Enhanced safeguards apply to all special category data processing.

---

8. Data Collection Methods

8.1. **Direct Collection**

8.1.1. Personal data is collected directly from individuals through application forms.

8.1.2. Personal data is collected through correspondence and communications.

8.1.3. Personal data is collected through website registration and subscriptions.

8.1.4. Personal data is collected through event registration.

8.1.5. Personal data is collected through complaints, appeals, and grievance submissions.

8.1.6. Personal data is collected through surveys and feedback forms.

8.2. **Indirect Collection**

8.2.1. Personal data may be obtained from institutions seeking or holding accreditation.

8.2.2. Personal data may be obtained from publicly available sources.

8.2.3. Personal data may be obtained from referees or references.

8.2.4. Personal data may be obtained from other quality assurance bodies.

8.2.5. Where data is obtained indirectly, individuals are informed at the earliest opportunity.

8.3. **Automated Collection**

8.3.1. Technical data is collected automatically through website cookies and similar technologies.

8.3.2. Automated collection includes IP addresses, browser information, and usage patterns.

8.3.3. Details of automated collection are provided in the IEB Cookie Policy.

8.3.4. Individuals can control automated collection through browser settings.

8.4. **Privacy Notices**

8.4.1. Privacy notices are provided at the point of data collection.

8.4.2. Privacy notices explain the purposes of processing.

8.4.3. Privacy notices explain the legal basis for processing.

8.4.4. Privacy notices inform individuals of their rights.

8.4.5. Privacy notices identify how to contact IEB about data protection matters.

8.4.6. Privacy notices are reviewed and updated regularly.

---

9. Consent

9.1. **When Consent is Used**

9.1.1. Consent is used where other legal bases are not applicable or appropriate.

9.1.2. Consent is used for marketing communications and newsletters.

9.1.3. Consent is used for processing special category data where required.

9.1.4. Consent is used for optional data collection beyond essential requirements.

9.1.5. Consent is used for cookies and tracking technologies where required.

9.2. **Standards for Valid Consent**

9.2.1. Consent must be freely given without pressure or coercion.

9.2.2. Consent must be specific to particular processing purposes.

9.2.3. Consent must be informed based on clear explanation of processing.

9.2.4. Consent must be unambiguous through a clear affirmative action.

9.2.5. Silence, pre-ticked boxes, or inactivity do not constitute valid consent.

9.3. **Obtaining Consent**

9.3.1. Consent requests are presented clearly and separately from other matters.

9.3.2. Consent requests explain the specific processing covered.

9.3.3. Consent requests identify IEB as the data controller.

9.3.4. Consent requests inform individuals of their right to withdraw.

9.3.5. Consent is documented with records of what was consented to and when.

9.4. **Withdrawing Consent**

9.4.1. Individuals may withdraw consent at any time.

9.4.2. Withdrawal is made easy, using the same method as giving consent where possible.

9.4.3. Information about withdrawal is provided when consent is obtained.

9.4.4. Withdrawal is actioned promptly upon receipt.

9.4.5. Withdrawal does not affect the lawfulness of processing before withdrawal.

9.5. **Consent for Children and Vulnerable Persons**

9.5.1. Special care is taken when obtaining consent from children.

9.5.2. Parental or guardian consent may be required depending on jurisdiction and context.

9.5.3. Age verification measures are implemented where appropriate.

9.5.4. Consent mechanisms are designed to be understandable by the target audience.

---

10. Data Subject Rights

10.1. **Overview of Rights**

10.1.1. IEB respects and facilitates the data protection rights of individuals.

10.1.2. Rights may be subject to limitations and exemptions under applicable law.

10.1.3. IEB will respond to rights requests without undue delay.

10.1.4. Responses will be provided within thirty (30) days of receiving a valid request.

10.1.5. Complex requests may require an extension of up to sixty (60) additional days.

10.1.6. Individuals will be informed of any extension and the reasons.

10.2. **Right to Information**

10.2.1. Individuals have the right to be informed about the processing of their personal data.

10.2.2. Information is provided through privacy notices at the point of collection.

10.2.3. Information includes the purposes, legal basis, recipients, and retention periods.

10.2.4. Information includes details of individual rights and how to exercise them.

10.3. **Right of Access**

10.3.1. Individuals have the right to obtain confirmation of whether their data is processed.

10.3.2. Individuals have the right to access their personal data held by IEB.

10.3.3. Individuals have the right to receive a copy of their personal data.

10.3.4. Access requests should be submitted in writing to the Data Protection Officer.

10.3.5. Identity verification may be required before providing access.

10.3.6. Access may be restricted where it would adversely affect the rights of others.

10.4. **Right to Rectification**

10.4.1. Individuals have the right to have inaccurate personal data corrected.

10.4.2. Individuals have the right to have incomplete personal data completed.

10.4.3. Rectification requests should specify the data to be corrected and the correction required.

10.4.4. IEB will verify corrections before implementation where appropriate.

10.4.5. Third parties who received the data will be notified of corrections where feasible.

10.5. **Right to Erasure**

10.5.1. Individuals have the right to request deletion of their personal data.

10.5.2. The right applies where data is no longer necessary for the original purpose.

10.5.3. The right applies where consent is withdrawn and no other basis exists.

10.5.4. The right applies where processing is unlawful.

10.5.5. The right does not apply where retention is required for legal obligations.

10.5.6. The right does not apply where retention is necessary for legal claims.

10.5.7. IEB will inform the individual of the outcome of the erasure request.

10.6. **Right to Restriction**

10.6.1. Individuals have the right to request restriction of processing in certain circumstances.

10.6.2. Restriction applies while accuracy of data is being verified.

10.6.3. Restriction applies where processing is unlawful but erasure is not requested.

10.6.4. Restriction applies where data is needed for legal claims after IEB no longer needs it.

10.6.5. Restricted data may only be processed with consent or for legal claims.

10.7. **Right to Data Portability**

10.7.1. Individuals have the right to receive their data in a portable format.

10.7.2. The right applies to data provided by the individual.

10.7.3. The right applies where processing is based on consent or contract.

10.7.4. The right applies where processing is automated.

10.7.5. Data will be provided in a commonly used, machine-readable format.

10.7.6. Where technically feasible, data may be transmitted directly to another organization.

10.8. **Right to Object**

10.8.1. Individuals have the right to object to processing based on legitimate interests.

10.8.2. Individuals have the right to object to processing for direct marketing.

10.8.3. Where objection is received, IEB will cease processing unless compelling grounds exist.

10.8.4. Objections to direct marketing will always be honored.

10.8.5. The right to object will be brought to attention at the point of first communication.

10.9. **Rights Related to Automated Decision-Making**

10.9.1. Individuals have rights related to automated decision-making and profiling.

10.9.2. These rights are detailed in Section 19 of this policy.

10.10. **Exercising Rights**

10.10.1. Requests to exercise rights should be submitted in writing.

10.10.2. Requests should be addressed to the Data Protection Officer.

10.10.3. Contact details are provided in Section 21 of this policy.

10.10.4. IEB may request additional information to verify identity.

10.10.5. Requests are handled free of charge unless manifestly unfounded or excessive.

10.10.6. IEB may charge a reasonable fee or refuse manifestly unfounded or excessive requests.

---

11. Data Sharing and Disclosure

11.1. **General Principles**

11.1.1. IEB does not sell personal data to third parties.

11.1.2. Personal data is only shared where necessary and with appropriate safeguards.

11.1.3. Data sharing is documented and subject to agreements where required.

11.1.4. Individuals are informed of data sharing in privacy notices.

11.2. **Internal Sharing**

11.2.1. Personal data may be shared within IEB on a need-to-know basis.

11.2.2. Access is restricted to staff who require data for their role.

11.2.3. Internal sharing is subject to confidentiality obligations.

11.2.4. Access controls are implemented in IEB systems.

11.3. **Sharing with Institutions**

11.3.1. Personal data may be shared with applicant or accredited institutions as necessary.

11.3.2. Sharing is limited to data necessary for accreditation purposes.

11.3.3. Institutions receiving data are responsible for their own data protection compliance.

11.3.4. Data sharing agreements may be established where appropriate.

11.4. **Sharing with Assessors and Reviewers**

11.4.1. Personal data may be shared with assessors and reviewers for evaluation purposes.

11.4.2. Assessors and reviewers are bound by confidentiality agreements.

11.4.3. Assessors and reviewers receive only data necessary for their role.

11.4.4. Data protection responsibilities are included in assessor training.

11.5. **Sharing with Third-Party Service Providers**

11.5.1. Personal data may be shared with service providers who process data on IEB's behalf.

11.5.2. Service providers are selected based on their ability to provide adequate safeguards.

11.5.3. Data processing agreements are established with all service providers.

11.5.4. Service providers may only process data in accordance with IEB's instructions.

11.5.5. Service providers include IT service providers, payment processors, and event organizers.

11.6. **Sharing with Other Quality Assurance Bodies**

11.6.1. Personal data may be shared with other quality assurance or accreditation bodies.

11.6.2. Sharing is limited to data necessary for quality assurance purposes.

11.6.3. Appropriate safeguards are implemented for such sharing.

11.6.4. Individuals are informed of such sharing in privacy notices.

11.7. **Sharing with Regulatory and Government Authorities**

11.7.1. Personal data may be disclosed to regulatory authorities where legally required.

11.7.2. Personal data may be disclosed in response to valid legal process.

11.7.3. Personal data may be disclosed to law enforcement where legally required.

11.7.4. IEB will inform individuals of such disclosure unless prohibited by law.

11.8. **Public Disclosure**

11.8.1. Limited personal data may be publicly disclosed in the context of accreditation.

11.8.2. Public disclosure includes names of institutional contacts in public registers.

11.8.3. Public disclosure is limited to information necessary for stakeholder awareness.

11.8.4. Individuals are informed of potential public disclosure.

---

12. International Data Transfers

12.1. **Scope of International Transfers**

12.1.1. IEB operates internationally and may transfer personal data across borders.

12.1.2. Transfers may occur to countries where institutions, assessors, or service providers are located.

12.1.3. IEB ensures appropriate safeguards for all international transfers.

12.2. **Transfer Mechanisms**

12.2.1. Transfers to countries with adequate protection laws may occur without additional safeguards.

12.2.2. Transfers to other countries require appropriate safeguards.

12.2.3. Standard contractual clauses may be used for transfers.

12.2.4. Binding corporate rules may be relied upon where applicable.

12.2.5. Consent may be obtained for specific transfers where appropriate.

12.2.6. Transfers may be made where necessary for contracts or legal claims.

12.3. **Safeguards**

12.3.1. IEB assesses the data protection framework in recipient countries.

12.3.2. Additional technical and organizational measures are implemented where necessary.

12.3.3. Data processing agreements include transfer provisions.

12.3.4. Records of international transfers are maintained.

12.4. **Information for Data Subjects**

12.4.1. Privacy notices inform individuals of potential international transfers.

12.4.2. Information about safeguards is available upon request.

12.4.3. Individuals may contact the Data Protection Officer for more information.

---

13. Data Security Measures

13.1. **Security Objectives**

13.1.1. IEB implements appropriate security measures to protect personal data.

13.1.2. Security measures protect against unauthorized access, disclosure, alteration, and destruction.

13.1.3. Security measures are appropriate to the level of risk.

13.1.4. Security measures are regularly reviewed and updated.

13.2. **Technical Measures**

13.2.1. Encryption is used for sensitive data in transit and at rest where appropriate.

13.2.2. Access controls restrict system access to authorized personnel.

13.2.3. Multi-factor authentication is implemented for critical systems.

13.2.4. Firewalls and intrusion detection systems protect network security.

13.2.5. Anti-malware software is deployed and maintained.

13.2.6. Regular security patches and updates are applied.

13.2.7. Secure configurations are implemented for systems and applications.

13.2.8. Regular backups are performed and tested.

13.3. **Organizational Measures**

13.3.1. Staff receive training on data security responsibilities.

13.3.2. Confidentiality agreements are in place for staff and contractors.

13.3.3. Access to personal data is restricted on a need-to-know basis.

13.3.4. Clear desk and clear screen policies are implemented.

13.3.5. Security incident response procedures are documented.

13.3.6. Regular security assessments and audits are conducted.

13.3.7. Third-party security is assessed before engagement.

13.4. **Physical Security**

13.4.1. Physical access to premises is controlled.

13.4.2. Paper records containing personal data are stored securely.

13.4.3. Secure disposal of paper records is implemented.

13.4.4. Physical security measures are appropriate to the environment.

13.5. **Continuous Improvement**

13.5.1. Security measures are reviewed regularly.

13.5.2. Security incidents inform improvements.

13.5.3. Emerging threats and best practices are monitored.

13.5.4. Security testing is conducted periodically.

---

14. Data Retention

14.1. **Retention Principles**

14.1.1. Personal data is retained only for as long as necessary for the stated purposes.

14.1.2. Retention periods are defined based on legal, operational, and archival requirements.

14.1.3. Personal data is securely deleted or anonymized when no longer required.

14.1.4. Retention periods are documented and reviewed regularly.

14.2. **Retention Schedule**

14.2.1. **Accreditation Records:** Core accreditation records are retained for the duration of accreditation plus ten (10) years.

14.2.2. **Application Records:** Records of unsuccessful applications are retained for five (5) years.

14.2.3. **Assessment Reports:** Assessment and evaluation reports are retained for ten (10) years.

14.2.4. **Complaints and Appeals:** Complaints and appeals records are retained for seven (7) years after closure.

14.2.5. **Financial Records:** Financial records are retained as required by applicable law, typically seven (7) years.

14.2.6. **Staff Records:** Staff records are retained for the duration of employment plus seven (7) years.

14.2.7. **Communication Records:** General correspondence is retained for three (3) years.

14.2.8. **Website Data:** Website analytics data is retained for two (2) years.

14.2.9. **Marketing Consents:** Records of consent are retained for the duration of processing plus three (3) years.

14.3. **Retention Review**

14.3.1. Retention periods are reviewed annually.

14.3.2. Data reaching the end of its retention period is identified.

14.3.3. Data is securely deleted or anonymized as appropriate.

14.3.4. Records of deletion are maintained.

14.4. **Extended Retention**

14.4.1. Retention may be extended where required for ongoing legal matters.

14.4.2. Retention may be extended for regulatory investigations.

14.4.3. Retention may be extended for historical or archival purposes with appropriate safeguards.

14.4.4. Extended retention is documented with justification.

14.5. **Secure Deletion**

14.5.1. Electronic data is deleted using secure methods appropriate to the sensitivity.

14.5.2. Paper records are shredded or securely destroyed.

14.5.3. Third-party service providers are required to securely delete data.

14.5.4. Certificates of destruction are obtained where appropriate.

---

15. Data Breach Management

15.1. **Definition of Data Breach**

15.1.1. A data breach is a security incident affecting personal data.

15.1.2. Breaches include unauthorized access to personal data.

15.1.3. Breaches include unauthorized disclosure of personal data.

15.1.4. Breaches include loss or theft of personal data.

15.1.5. Breaches include unauthorized alteration of personal data.

15.1.6. Breaches include accidental destruction of personal data.

15.2. **Breach Detection and Reporting**

15.2.1. All staff must report suspected breaches immediately.

15.2.2. Reports should be made to the Data Protection Officer.

15.2.3. Reports should include all known details of the incident.

15.2.4. Timely reporting is essential for effective response.

15.3. **Breach Assessment**

15.3.1. The Data Protection Officer will assess reported incidents.

15.3.2. Assessment determines whether a breach has occurred.

15.3.3. Assessment determines the nature and scope of the breach.

15.3.4. Assessment evaluates the risk to affected individuals.

15.3.5. Assessment considers the number of individuals affected.

15.3.6. Assessment considers the sensitivity of the data involved.

15.4. **Breach Response**

15.4.1. Immediate steps will be taken to contain the breach.

15.4.2. Steps will be taken to recover lost or compromised data where possible.

15.4.3. The root cause will be investigated.

15.4.4. Measures will be implemented to prevent recurrence.

15.4.5. A breach response team may be convened for serious breaches.

15.5. **Notification to Authorities**

15.5.1. Breaches posing a risk to individuals may be reported to supervisory authorities.

15.5.2. Notification will be made within seventy-two (72) hours where required.

15.5.3. Notification will include details of the breach and response measures.

15.5.4. The decision to notify is made by the Data Protection Officer.

15.6. **Notification to Individuals**

15.6.1. Individuals will be notified where a breach poses a high risk to their rights and freedoms.

15.6.2. Notification will be made without undue delay.

15.6.3. Notification will describe the nature of the breach.

15.6.4. Notification will include the likely consequences.

15.6.5. Notification will include measures taken or proposed.

15.6.6. Notification will include advice on protective steps individuals can take.

15.7. **Breach Records**

15.7.1. All breaches are documented regardless of severity.

15.7.2. Records include the facts, effects, and remedial actions.

15.7.3. Records are reviewed to identify patterns and improvement opportunities.

15.7.4. Records are retained for a minimum of five (5) years.

15.8. **Post-Breach Review**

15.8.1. A post-incident review is conducted for all significant breaches.

15.8.2. The review assesses the effectiveness of the response.

15.8.3. The review identifies lessons learned.

15.8.4. Improvements are implemented to prevent recurrence.

---

16. Third-Party Data Processors

16.1. **Selection of Processors**

16.1.1. IEB selects data processors that provide sufficient guarantees of compliance.

16.1.2. Selection considers the processor's technical and organizational measures.

16.1.3. Selection considers the processor's track record and reputation.

16.1.4. Due diligence is conducted before engaging processors.

16.2. **Data Processing Agreements**

16.2.1. Written agreements are established with all data processors.

16.2.2. Agreements specify the subject matter and duration of processing.

16.2.3. Agreements specify the nature and purpose of processing.

16.2.4. Agreements specify the types of personal data and categories of data subjects.

16.2.5. Agreements include IEB's obligations and rights as controller.

16.3. **Processor Obligations**

16.3.1. Processors must only process data on IEB's documented instructions.

16.3.2. Processors must ensure staff confidentiality.

16.3.3. Processors must implement appropriate security measures.

16.3.4. Processors must obtain IEB's authorization before engaging sub-processors.

16.3.5. Processors must assist IEB in responding to data subject requests.

16.3.6. Processors must assist IEB in meeting compliance obligations.

16.3.7. Processors must delete or return data at the end of the engagement.

16.3.8. Processors must allow for and contribute to audits.

16.4. **Sub-Processors**

16.4.1. Processors must obtain prior written authorization for sub-processors.

16.4.2. IEB maintains a list of approved sub-processors.

16.4.3. Processors must impose equivalent obligations on sub-processors.

16.4.4. Processors remain liable for sub-processor compliance.

16.5. **Monitoring and Audit**

16.5.1. IEB monitors processor compliance with agreements.

16.5.2. IEB may request information about processing activities.

16.5.3. IEB may conduct audits or inspections of processors.

16.5.4. Audit rights are included in data processing agreements.

---

17. Website, Cookies, and Online Tracking

17.1. **Website Data Collection**

17.1.1. IEB collects personal data through its website.

17.1.2. Data collection includes information submitted through forms.

17.1.3. Data collection includes technical data collected automatically.

17.1.4. Privacy notices on the website explain data collection practices.

17.2. **Cookies**

17.2.1. IEB uses cookies and similar technologies on its website.

17.2.2. Cookies are small files placed on user devices.

17.2.3. Cookies enable website functionality and analytics.

17.2.4. IEB uses essential cookies necessary for website operation.

17.2.5. IEB may use analytics cookies to understand website usage.

17.2.6. IEB may use preference cookies to remember user settings.

17.3. **Cookie Consent**

17.3.1. Consent is obtained for non-essential cookies where required.

17.3.2. A cookie banner or notice is displayed to website visitors.

17.3.3. Users can manage cookie preferences through the website.

17.3.4. Users can control cookies through browser settings.

17.3.5. Essential cookies do not require consent.

17.4. **Third-Party Cookies**

17.4.1. IEB may use third-party services that set their own cookies.

17.4.2. Third-party cookies are subject to the third party's privacy policy.

17.4.3. Information about third-party cookies is provided in the Cookie Policy.

17.4.4. IEB is not responsible for third-party cookie practices.

17.5. **Analytics**

17.5.1. IEB uses website analytics to understand user behavior.

17.5.2. Analytics may include page views, session duration, and navigation paths.

17.5.3. Analytics data is used to improve website design and content.

17.5.4. IP addresses may be anonymized in analytics data.

17.6. **Do Not Track**

17.6.1. IEB respects browser Do Not Track signals where feasible.

17.6.2. Users can indicate tracking preferences through browser settings.

17.6.3. Not all services may respond to Do Not Track signals.

---

18. Children's Data and Vulnerable Persons

18.1. **Children's Data**

18.1.1. IEB does not knowingly collect personal data from children under the age of sixteen (16) without appropriate consent.

18.1.2. Where children's data is collected, parental or guardian consent is obtained.

18.1.3. Age verification measures are implemented where appropriate.

18.1.4. Children's data is subject to enhanced protection.

18.2. **Definition of Child**

18.2.1. The definition of a child varies by jurisdiction.

18.2.2. IEB applies the age of sixteen (16) as a general threshold.

18.2.3. Local legal requirements may require a different threshold.

18.2.4. IEB will comply with applicable local requirements.

18.3. **Learner Data**

18.3.1. Learner data received from institutions may include data of minors.

18.3.2. Institutions are responsible for obtaining appropriate consents.

18.3.3. IEB processes learner data only for legitimate quality assurance purposes.

18.3.4. Enhanced safeguards apply to data of minor learners.

18.4. **Vulnerable Persons**

18.4.1. IEB is mindful of the needs of vulnerable persons.

18.4.2. Reasonable accommodations are made for individuals with disabilities.

18.4.3. Additional care is taken in communications with vulnerable persons.

18.4.4. Support is available to assist vulnerable persons in exercising their rights.

---

19. Automated Decision-Making and Profiling

19.1. **IEB's Use of Automated Decision-Making**

19.1.1. IEB generally does not make decisions based solely on automated processing.

19.1.2. Accreditation decisions involve human judgment and review.

19.1.3. Automated systems may support decision-making but do not replace human oversight.

19.2. **Profiling**

19.2.1. IEB does not engage in profiling that produces legal or similarly significant effects.

19.2.2. Basic categorization for administrative purposes does not constitute harmful profiling.

19.2.3. Any future profiling activities will be assessed for compliance.

19.3. **Rights Related to Automated Decisions**

19.3.1. Individuals have the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects.

19.3.2. Where automated decisions are made, individuals may request human intervention.

19.3.3. Individuals may express their point of view and contest automated decisions.

19.3.4. Information about automated decision-making logic is available upon request.

19.4. **Safeguards**

19.4.1. Where automated decision-making is used, appropriate safeguards are implemented.

19.4.2. Safeguards include the right to human review.

19.4.3. Safeguards include clear information about the logic involved.

19.4.4. Regular reviews assess the fairness and accuracy of automated systems.

---

20. Training and Awareness

20.1. **Staff Training**

20.1.1. All IEB staff receive data protection training upon induction.

20.1.2. Training covers the principles and requirements of this policy.

20.1.3. Training covers staff responsibilities for data protection.

20.1.4. Training covers recognition and reporting of data breaches.

20.1.5. Refresher training is provided annually.

20.2. **Role-Specific Training**

20.2.1. Staff with specific data protection responsibilities receive enhanced training.

20.2.2. Training is tailored to the risks and responsibilities of different roles.

20.2.3. Training for assessors includes data protection obligations.

20.2.4. Committee members receive training on their data protection duties.

20.3. **Awareness Activities**

20.3.1. Data protection awareness is promoted throughout IEB.

20.3.2. Regular communications reinforce data protection messages.

20.3.3. Updates on policy changes are communicated to all staff.

20.3.4. Data protection is included in organizational culture.

20.4. **Training Records**

20.4.1. Records of training completion are maintained.

20.4.2. Training attendance is monitored.

20.4.3. Non-completion is followed up and addressed.

20.4.4. Training effectiveness is evaluated.

---

21. Roles and Responsibilities

21.1. **IEB Governing Council**

21.1.1. Provides strategic oversight of data protection.

21.1.2. Approves this policy and significant amendments.

21.1.3. Receives reports on data protection compliance.

21.1.4. Ensures adequate resources for data protection.

21.2. **Director, IEB Secretariat**

21.2.1. Has overall accountability for data protection compliance.

21.2.2. Ensures implementation of this policy.

21.2.3. Reports to the Governing Council on data protection matters.

21.2.4. Ensures adequate resources are allocated.

21.3. **Data Protection Officer (DPO)**

21.3.1. Oversees day-to-day data protection compliance.

21.3.2. Advises on data protection matters.

21.3.3. Monitors compliance with this policy and applicable laws.

21.3.4. Handles data subject rights requests.

21.3.5. Manages data breach response.

21.3.6. Conducts data protection impact assessments.

21.3.7. Serves as the contact point for data protection inquiries.

21.3.8. Liaises with supervisory authorities where necessary.

21.3.9. Contact: dataprotection@ieb-education.org (or designated contact).

21.4. **All Staff**

21.4.1. Comply with this policy and data protection procedures.

21.4.2. Only access personal data necessary for their role.

21.4.3. Keep personal data confidential and secure.

21.4.4. Report suspected data breaches immediately.

21.4.5. Complete required data protection training.

21.4.6. Refer data protection queries to the DPO.

21.5. **Assessors and Committee Members**

21.5.1. Comply with confidentiality obligations.

21.5.2. Only use personal data for authorized purposes.

21.5.3. Protect personal data in their possession.

21.5.4. Return or delete personal data when no longer required.

21.5.5. Report any data protection concerns to IEB.

21.6. **Third-Party Processors**

21.6.1. Process data only in accordance with agreements.

21.6.2. Implement appropriate security measures.

21.6.3. Report data breaches to IEB promptly.

21.6.4. Cooperate with audits and monitoring.

---

22. Policy Review

22.1. This policy will be reviewed every two (2) years.

22.2. Reviews will assess compliance with applicable laws and best practices.

22.3. Reviews will consider feedback from stakeholders.

22.4. Reviews will incorporate lessons learned from incidents.

22.5. Reviews will consider developments in data protection law and practice.

22.6. Amendments will be approved by the IEB Governing Council.

22.7. Stakeholders will be notified of significant amendments.

22.8. The current version of this policy will be published on the IEB website.

22.9. Minor updates may be made without full review where necessary for compliance.

---

23. Disclaimer and Legal Position

23.1. IEB is an independent, private, non-governmental, and non-statutory international education authority.

23.2. This policy does not create any legal rights or obligations enforceable in any jurisdiction beyond applicable data protection law.

23.3. IEB accreditation does not constitute government approval, statutory recognition, or professional licensure.

23.4. This policy is designed to meet international best practices in data protection.

23.5. Where local law imposes stricter requirements, IEB will comply with those requirements.

23.6. IEB reserves the right to amend this policy at anytime without prior notice.

23.7. Decisions made under this policy are internal to IEB operations.

23.8. Individuals seeking legal remedies should consult appropriate legal counsel.

23.9. This policy does not limit any rights individuals may have under applicable data protection law.

23.10. IEB is not responsible for the data protection practices of accredited institutions.

23.11. Accredited institutions are independent data controllers responsible for their own compliance.

---

24. Conclusion

24.1. This policy establishes IEB's commitment to protecting personal data and privacy.

24.2. IEB recognizes that data protection is fundamental to trust and ethical practice.

24.3. IEB is committed to processing personal data lawfully, fairly, and transparently.

24.4. IEB respects the rights of individuals regarding their personal data.

24.5. IEB implements appropriate measures to protect personal data from unauthorized access and misuse.

24.6. This policy reflects international best practices in data protection.

24.7. IEB encourages individuals to contact the Data Protection Officer with any questions or concerns.

24.8. IEB is committed to continuous improvement in data protection practices.

---

25. Annexures

25.1. **Annexure A: Privacy Notice Template**

25.1.1. Annexure A provides the template for privacy notices used by IEB.

25.1.2. The template includes required information elements.

25.1.3. The annexure is available as a separate document from IEB Secretariat.

25.2. **Annexure B: Data Subject Access Request Form**

25.2.1. Annexure B provides the form for submitting data subject access requests.

25.2.2. The form includes identity verification requirements.

25.2.3. The annexure is available as a separate document from IEB Secretariat.

25.3. **Annexure C: Data Breach Reporting Form**

25.3.1. Annexure C provides the internal form for reporting data breaches.

25.3.2. The form includes required information for breach assessment.

25.3.3. The annexure is available as a separate document from IEB Secretariat.

25.4. **Annexure D: Data Processing Agreement Template**

25.4.1. Annexure D provides the template for data processing agreements with third parties.

25.4.2. The template includes required contractual clauses.

25.4.3. The annexure is available as a separate document from IEB Secretariat.

25.5. **Annexure E: Data Retention Schedule**

25.5.1. Annexure E provides the detailed data retention schedule.

25.5.2. The schedule specifies retention periods for all data categories.

25.5.3. The annexure is available as a separate document from IEB Secretariat.

25.6. **Annexure F: Cookie Policy**

25.6.1. Annexure F provides the detailed Cookie Policy for the IEB website.

25.6.2. The policy includes information about specific cookies used.

25.6.3. The annexure is available as a separate document from IEB Secretariat.

25.7. **Annexure G: Data Protection Impact Assessment Template**

25.7.1. Annexure G provides the template for conducting data protection impact assessments.

25.7.2. The template guides assessment of high-risk processing activities.

25.7.3. The annexure is available as a separate document from IEB Secretariat.

25.8. **Annexure H: Consent Form Templates**

25.8.1. Annexure H provides templates for obtaining consent.

25.8.2. Templates are provided for different processing purposes.

25.8.3. The annexure is available as a separate document from IEB Secretariat.

25.9. **Annexure I: Glossary of Data Protection Terms**

25.9.1. Annexure I provides extended definitions of data protection terms.

25.9.2. The glossary supplements the definitions provided in Section 4.

25.9.3. The annexure is available as a separate document from IEB Secretariat.

---

26. Document Control

26.1. **Document Information**

26.1.1. Document Title: Data Protection and Privacy Policy

26.1.2. Document Code: IEB-POL-007

26.1.3. Version: 1.0

26.1.4. Effective Date: January 2026

26.1.5. Next Review Date: January 2028

26.1.6. Prepared by: International Education Board Quality Assurance Division

26.1.7. Approved By: IEB Governing Council

26.1.8. Classification: Public

26.2. **Version History**

26.2.1. Version 1.0 represents the initial release of this policy.

26.2.2. Future versions will be documented with version number, date, and summary of changes.

26.2.3. All previous versions are archived and available upon request.

26.3. **Related Documents**

26.3.1. IEB Accreditation Framework and Standards Policy (IEB-POL-001)

26.3.2. IEB Accreditation Process Policy (IEB-POL-002)

26.3.3. IEB Eligibility Criteria Policy (IEB-POL-003)

26.3.4. IEB Accreditation Levels and Status Policy (IEB-POL-004)

26.3.5. IEB Accreditation Validity, Monitoring, and Review Policy (IEB-POL-005)

26.3.6. IEB Complaints, Appeals, and Grievance Policy (IEB-POL-006)

26.3.7. IEB Recognition and Representation Policy (IEB-POL-008)

26.3.8. IEB Logo Use and Intellectual Property Policy (IEB-POL-009)

26.3.9. IEB Accreditation Decision-Making and Oversight Policy (IEB-POL-010)

26.3.10. IEB Information Security Policy (IEB-POL-011)

26.3.11. IEB Records Management Policy (IEB-POL-012)

---

27. Approval

27.1. This policy has been reviewed and approved by the IEB Governing Council.

27.2. This policy is effective from the date specified in Document Control.

27.3. All stakeholders are expected to comply with this policy.

27.4. Queries regarding this policy should be directed to the Data Protection Officer.

End of Document
