IPE GLOBAL CENTRE FOR KNOWLEDGE AND DEVELOPMENT

DATA PROTECTION AND PRIVACY POLICY

A. PURPOSE

This Policy outlines information security, data protection and privacy requirements of the IPE Global Centre for Knowledge and Development (CKD) (hereinafter referred to as "Organisation") in alignment with the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and Sensitive Personal Data or Information, Rules 2011. It is intended to protect both the Organisation and users from possible liability and to safeguard information and data. Users may be employees, clients, contractors, teaming partners, or suppliers of the Organisation.

B. SCOPE

This policy applies to all employees, contractors, vendors, consultants, business partners, interns and any other third-party service providers of CKD ("Users") who collect, access, process, store, transmit or otherwise handle digital personal data on behalf of CKD.

It covers all data processing activities by CKD, including collection, storage, use, disclosure, transfer (domestic or cross-border), disposal and archival of digital personal data (including sensitive personal data or information, as applicable). It applies to all digital personal data, whether collected online or offline and later digitised.

C. LEGAL & REGULATORY OBLIGATIONS

Organisation shall ensure that:

- Personal data is processed lawfully, for specific purposes, with notice and consent where required.
- Reasonable security practices are implemented across systems.
- Privacy notices, contracts and vendor controls meet statutory requirements.
- Data Principals' rights (access, correction, erasure, grievance) are honoured.

D. ROLES & RESPONSIBILITIES

Associated Director – Risk & Compliance: Oversight of compliance, risk management, intellectual property issues, and resource allocation. Responsible for conducting due diligence, which includes checking data protection policies, security infrastructure, compliance history, access control mechanisms of the third party, and their ability to respond to breaches. The person is also responsible for remaining vigilant on local laws and donor guidance, and updating our internal practices as needed.

Project Manager: As custodians of project-specific personal data, Project Managers ensure controlled access, limit data usage to essential purposes, conduct risk assessment, and verify that third-party service providers comply fully with contractual data-protection obligations.

IT Department: Implements cybersecurity controls, access management, backups, monitoring and incident handling.

Individuals (the Data Principals): The individual to whom the Personal Data relates has rights, including the right to access their data, the right to correct/update it, the right to erasure, the right to grievance redressal, and the right to withdraw consent.

E. SECURITY CONTROLS:

Organisation shall maintain Reasonable Security Practices, including:

Access Control: Role-based access, unique IDs, strong passwords, MFA where applicable.

Network Security: Firewalls, antivirus, secure configurations, regular patching and vulnerability management.

Email & Internet Security: Anti-phishing controls, restricted unsafe downloads, and monitoring of malicious

activities.

Endpoint Security: Encryption of laptop management.

Backup & Recovery: Regular backups, offline copies, periodic restoration tests.

Physical Security: Restricted access to server rooms and IT assets.

Data Disposal: Secure wiping/destruction of digital and physical records.

F. TRAINING & AWARENESS:

The organisation shall provide training to all employees through the induction session on data protection, privacy obligations, security best practices, and incident reporting.

All third-party partners are bound by contracts with explicit data protection clauses, including confidentiality, audit rights, and clear restrictions on how the data can be used.

G. POLICY REVISIONS

The policy shall be amended in case of (i) changes in laws/regulations, (ii) significant technology or operational changes, and (iii) notable incident(s) or audit findings.

H. CONSEQUENCES OF VIOLATION

Non-compliance with this policy may result in disciplinary measures, including warnings, suspension, termination of access or employment, and legal action where applicable

DATA PROTECTION & PRIVACY POLICY ACKNOWLEDGMENT

After reading this policy, please sign this acknowledgement form and submit the same to HR Department for filing.

I hereby acknowledge that I have received, read, and understood the Organisation's Data Protection & Privacy Policy, including its requirements under the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and the IT (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011.

I understand that:
I am responsible for protecting personal data and sensitive personal data or information (SPDI) that I may access, handle, or process during the course of my employment.

I must comply with all data protection obligations, confidentiality requirements, security procedures, and acceptable-use standards defined in the policy.

I must immediately report any suspected or actual data breach, loss of data, unauthorised disclosure, or policy violation to the Associate Director – Risk and Compliance.

Failure to comply with the Data Protection Policy may result in disciplinary action, including termination of employment, and may also lead to legal consequences under applicable laws.

By signing below, I confirm my commitment to follow the policy at all times and to safeguard the Organisation's information assets, systems, and data in accordance with my role and responsibilities.

Location: _____

Department: _____

Name: _____

Signature: _____ Date: _____/_____/_____