Version 4.0 | Renewed January 1st, 2026

Prepared in consultation with the Governing Board and Country Teams

APPROVED — APPLICABLE GLOBALLY |
PUBLIC DISTRIBUTION VERSION

THE DEVELOPMENT CAFÉ (DevCAFE)

Bridging Grassroots with Policy

INSTITUTIONAL POLICY ON

Research Integrity
Data Protection & Privacy
Client Confidentiality & Non-Disclosure

Originally Adopted: 25 June 2017 | Governing Board Resolution GGB-001-2017 | Effective: 1 January 2018

www.devcafe.org | admin@devcafe.org |

GOVERNING BOARD RESOLUTION

Formal Resolution of the Global Governing Board of The Development CAFÉ (DevCAFE)

Resolution Number	GGB-001-2017
Meeting	Inaugural Global Governing Board Meeting
Date of Meeting	25 June 2017
Location	Global (Multi-site Governing Board Convening)
Quorum	Confirmed — Full Board Present or Represented
Vote	Unanimous — Passed Without Objection
Effective Date of Policy	1 January 2018

BE IT RESOLVED by the Global Governing Board of The Development CAFÉ (DevCAFE), duly convened at its Inaugural Global Governing Board Meeting on 25 June 2017, with full quorum confirmed, that:

(a) The Institutional Policy Framework on Research Integrity, Client Confidentiality, Non-Disclosure, and Data Protection and Privacy (hereinafter "the Policy") is hereby formally adopted as official institutional policy of The Development CAFÉ (DevCAFE), effective 1 January 2018.

(b) The Policy shall apply universally and without exception to all DevCAFE staff, consultants, associates, sub-contractors, and partners operating in any jurisdiction, and to all research, evaluation, consultancy, and knowledge production activities conducted under the DevCAFE name, mandate, or funding.

(c) The Policy reflects DevCAFE's foundational commitments as an apolitical, areligious, and majority-self-funded institution, and constitutes the ethical and legal infrastructure governing the protection of research participants, clients, and institutional integrity.

(d) The Policy is to be reviewed no less than every two years from the effective date, or sooner upon material changes in applicable law, regulation, or operational context, with any amendments subject to Governing Board approval.

(e) The Country Director is designated as the accountable officer for policy implementation and enforcement, and is authorised to designate a Data Protection Lead for day-to-day operational compliance.

(f) The Policy is approved for publication on the DevCAFE website and for distribution to all institutional stakeholders as a public declaration of DevCAFE's standards.

Signed and affirmed by the Global Governing Board of The Development CAFÉ (DevCAFE) on 25 June 2017.

✍ FOREWORD

A Message from the Global Governing Board

When the founding members of The Development CAFÉ gathered to establish this institution, they chose a name and a metaphor with deliberate care. The English coffee houses of the sixteenth and seventeenth centuries were not merely places to drink coffee — they were the original open-source platforms, where the merchant sat beside the philosopher, the sea captain beside the poet, the pamphleteer beside the politician, and ideas moved freely across boundaries of class, profession, and geography. They were, in their time, the engines of the Enlightenment.

DevCAFE was founded in that spirit. We are a global institution built on the conviction that the most powerful instrument of human development is not money — though resources matter — but knowledge: rigorous, independent, participatory, and ethically produced knowledge that connects the reality of the grassroots with the decisions made in corridors of policy and power.

On 25 June 2017, the Global Governing Board of DevCAFE convened for the first time and adopted this Policy as the foundational ethical and legal framework of the institution. This was not a bureaucratic exercise. It was a statement of who we are, what we stand for, and how we must conduct ourselves in every country, community, and context in which we operate.

This Policy governs three interconnected domains. Research Integrity ensures that our knowledge production is honest, independent, and accountable — that no funder, no government, and no ideology can determine our findings. Client Confidentiality and Non-Disclosure ensures that those who trust us with their information are protected, and that our institutional credibility rests on the reliability of our discretion. Data Protection and Privacy ensures that the individuals and communities who participate in our research — often among the most vulnerable people on earth — are treated with the dignity, care, and legal protection their participation deserves.

DevCAFE operates across more than 40 countries, with particular depth in Southeast Asia, the ASEAN region, and the Indo-Pacific. We are 70% self-funded. This is not an accident: it is an architectural choice. Our financial independence is the structural guarantee of our intellectual independence.

The communities we work with have entrusted us with their stories, their data, and their aspirations. This Policy is our institutional promise to honour that trust — not only when it is convenient, but especially when it is costly. It is not a compliance document. It is a covenant.

Governing Board

The Development CAFÉ (DevCAFE) | 25 June 2017

TABLE OF CONTENTS

Part A
Foundational Framework

1. Institutional Mission and Identity

The Development CAFÉ (DevCAFE) is a global research, technology, and development think tank established to bridge the gap between grassroots realities and policy decision-making. Conceived in the tradition of the great English coffee houses — democratic spaces of intellectual exchange that helped drive the Enlightenment — DevCAFE operates as an open, rigorous, and independent institution committed to evidence-based transformation.

DEVCAFE AT A GLANCE
Nature: Global think tank — apolitical, areligious, financially independent
Founding: Incorporated and operational; Global Governing Board established 25 June 2017
Reach: 40+ countries across Asia, Pacific, Africa, the Americas, and Europe
Funding Model: 70% self-funded | 30% from commissioned consulting engagements
Mission: Empower countries, regions, and communities by bridging grassroots with policy
Pillars: Research 4 Development | Innovation and ICT | Capacity Development
Core Areas: MEL | Development Finance | Gender | Technology | Climate | Governance

DevCAFE operates at the intersection of evidence, community, and power. Its unique self-funding model ensures that DevCAFE selects and conducts projects on the basis of their alignment with its mission, not on the basis of commercial or political pressure.

2. Scope of Application

This Policy applies without limitation or exception to:

- All DevCAFE staff, regardless of employment status, location, or level of seniority
- All consultants, associates, sub-contractors, field researchers, translators, and enumerators engaged by DevCAFE
- All research projects, evaluations, assessments, reviews, and consultancy engagements conducted under the DevCAFE mandate, name, or branding
- All data — primary and secondary, digital and physical — collected, processed, stored, transmitted, or shared in connection with DevCAFE work
- All clients, institutional partners, funding entities, and collaborating organisations
- All jurisdictions in which DevCAFE operates, with specific reference to ASEAN member states, the Indo-Pacific, Southeast Asia, and all other countries of operation

Where country-specific legal requirements are more protective than the standards set out in this Policy, the more protective standard shall apply. Where this Policy exceeds the requirements of applicable local law, this Policy's standards shall be maintained.

3. Core Governing Principles

Nine core principles govern all DevCAFE research, data management, client engagement, and institutional conduct, adopted by the Global Governing Board on 25 June 2017:

#	Principle	Definition	Application
1	**Integrity**	Intellectual honesty, methodological rigour, and transparent reporting of methods, limitations, and findings.	All research outputs, reports, evaluations
2	**Independence**	Freedom from political, ideological, religious, or funder-driven influence on research design or findings.	Project selection, analysis, dissemination
3	**Confidentiality**	Protection of client information, participant data, and proprietary findings from unauthorised disclosure.	All engagements and data handling
4	**Informed Consent**	Free, prior, informed, specific, and documented consent from all human research participants.	All primary research activities
5	**Data Minimisation**	Collection of only the data strictly necessary for the stated research purpose.	Data collection design and instruments
6	**Purpose Limitation**	Data used only for the purpose for which it was collected; repurposing requires renewed consent.	Data management, storage, and secondary use
7	**Security**	Technical and organisational security measures proportionate to the sensitivity of data held.	Storage, transmission, and access controls
8	**Time-Limitation**	Retention of data only as long as necessary; secure deletion upon expiry of retention period.	Retention schedules and deletion protocols
9	**Accountability**	DevCAFE takes full responsibility for all data under its stewardship and maintains transparent audit trails.	Governance, breach response, and reporting

4. Regulatory Compliance Matrix

DevCAFE's multi-country operations require compliance with a constellation of national and regional data protection frameworks. The most protective applicable standard is adopted as the operational baseline for each project:

Jurisdiction / Body	Framework / Instrument	Key Requirement for DevCAFE
European Union	GDPR (2016/679)	Full compliance when processing EU data subjects; lawful basis; rights; 72hr breach notification
ASEAN	ASEAN Framework on Personal Data Protection (AFPDP) 2016	Regional baseline: consent/notification/purpose; accuracy; security safeguards; access/correction

Jurisdiction / Body	Framework / Instrument	Key Requirement for DevCAFE
ASEAN	ASEAN Model Contractual Clauses (MCCs) 2021	Cross-border transfer mechanism for ASEAN-to-ASEAN and ASEAN-to-EU data flows
ASEAN / EU	Joint Guide to ASEAN MCCs and EU SCCs 2023/2024	Practical interoperability tool for cross-border transfers between ASEAN and EU jurisdictions
APEC	Cross-Border Privacy Rules (CBPR) System	Applicable for Philippines and Singapore certified entities
Indonesia	PDP Law No. 27/2022	14-day breach notification; data subject rights; DPO for large-scale processing
Philippines	Data Privacy Act 2012 (RA 10173); NPC Regulations	72-hour breach notification to NPC; Privacy Impact Assessment; Data Sharing Agreements
Singapore	PDPA 2012 (amended 2020)	Breach notification to PDPC and individuals; data portability; fines up to 10% turnover
Thailand	PDPA B.E. 2562 (2019)	Explicit consent for sensitive data; cross-border safeguards; fines up to 5M baht
Vietnam	Decree 13/2023/ND-CP	Explicit consent; purpose limitation; data minimisation; cross-border conditions
Malaysia	PDPA 2010	Seven data protection principles; cross-border transfer restrictions; DPO required
Australia / Pacific	Privacy Act 1988 / APPs; NZ Privacy Act 2020	APP compliance for Australian/NZ data subjects; Notifiable Data Breach scheme
India	Digital Personal Data Protection Act 2023	Applies to Indian data subjects; consent-based framework; breach notification to DPBI
Global	Declaration of Helsinki (2013)	Research ethics standard for human subjects research
Global	OECD Privacy Guidelines (2013)	International baseline for data governance and cross-border flows
Global	ISO/IEC 27001:2022	Information security management standard for data systems

Part B
Research Integrity

5. Standards of Research Integrity

5.1 Intellectual Honesty

All DevCAFE research outputs must reflect the evidence base accurately, completely, and without distortion, irrespective of whether findings align with or contradict the expectations or preferences of clients, funders, or partners. Researchers are obligated to report inconvenient findings with the same rigour and care as confirmatory ones.

5.2 Methodological Rigour

All primary research must include:

- A documented and approved research design prior to the commencement of data collection
- Clear articulation of data sources, collection instruments, sampling methodology, and analytical frameworks
- Pre-registration of evaluative frameworks or theories of change where applicable
- Explicit acknowledgment of methodological limitations, confidence intervals, and rival explanations
- Peer review of major analytical outputs prior to client delivery or publication
- Transparent documentation of all data transformations, coding decisions, and analytical choices

5.3 Plagiarism and Attribution

DevCAFE maintains a zero-tolerance policy on plagiarism in all its forms. All research outputs must properly attribute all sources, data sets, ideas, and prior work. Where Generative AI or automated analysis tools are used, their use must be disclosed in accordance with DevCAFE's FRAME (Framework for Responsible AI in Monitoring and Evaluation) methodology.

5.4 Conflict of Interest

All staff and consultants must disclose any actual, potential, or perceived conflicts of interest before undertaking research assignments. Declared conflicts are reviewed by the Country Director. Where material conflicts exist, the researcher will be recused from relevant aspects of the assignment. A Conflict of Interest Register is maintained by the Country Director.

6. Apolitical and Areligious Mandate

DevCAFE's identity as an apolitical and areligious institution is both a principled commitment and an operational necessity. This mandate was among the founding resolutions of the Global Governing Board on 25 June 2017.

⚠ APOLITICAL & ARELIGIOUS STANDARDS — NON-NEGOTIABLE
⊘ DevCAFE does not endorse, support, or advocate for any political party, electoral candidate, or partisan cause.
⊘ DevCAFE's research, branding, and institutional voice may not be used in political campaigns, propaganda, or government advocacy materials.
⊘ DevCAFE does not favour, discriminate against, or condition research participation on religious affiliation or the absence thereof.
Research on political or religious topics maintains rigorous analytical distance, presents multiple perspectives, and follows the evidence.

Staff and consultants representing DevCAFE in official capacities must refrain from expressing partisan political or religious views.
DevCAFE will not accept funding from actors whose primary intent is political advocacy, religious proselytism, or partisan influence.
Any perceived breach of this mandate must be reported immediately to the Country Director.

7. Independence, Conflict of Interest & Funding

DevCAFE's 70% self-funding model is the structural guarantee of its independence. The following standards apply:

- Project selection is driven by mission alignment, not financial necessity
- Funders and clients receive the results of independent research — not the ability to alter those results
- All engagement contracts explicitly state the analytical independence of DevCAFE researchers
- DevCAFE retains the right to publish findings irrespective of client preferences, subject to agreed embargoes and the client pre-review process
- Where a client requests modifications to findings in ways that would distort the evidence, the researcher must decline, document the request, and escalate to the Country Director
- Institutional revenue from any single commissioned client may not exceed 20% of annual operating budget without Governing Board approval

8. Publication and Dissemination Standards

All DevCAFE research outputs undergo the following pre-publication process:

- Factual accuracy check against primary data and source documentation
- Confidentiality review ensuring no participant-identifying information is disclosed without consent
- Client pre-review period (10 working days for standard outputs; 20 days for major reports) — clients may flag factual errors but may not require modification of analytical conclusions
- Attribution of all contributing researchers, data sources, methodologies, and analytical tools
- AI disclosure statement where Generative AI tools contributed to analysis, synthesis, or writing
- Archiving of the underlying dataset in accordance with the project's Data Management Plan

9. Use of Artificial Intelligence in Research

DevCAFE recognises the transformative potential of Generative AI and automated analysis tools in research and evaluation practice. All use of AI in DevCAFE research must comply with the FRAME[1] Methodology (Framework for Responsible AI in Monitoring and Evaluation), which governs five core dimensions:

FRAME Dimension	Standard	Requirement
Accountability Architecture	Clear human accountability for all AI-assisted outputs	Named researcher accountable; AI cannot replace human analytical judgement
Stakeholder Engagement	Participants informed of AI use where relevant	Disclosure in consent forms where AI is used to analyse participant-provided data

[1] Adapted from *Bruce, K., Gandhi, V., & Nielsen, S.B. (Eds.)*. Artificial Intelligence and Evaluation: From Algorithms to Evidence – Using GenAI in Evaluation Practice. *Forthcoming, Routledge, 2026.*

FRAME Dimension	Standard	Requirement
Epistemic Integrity	AI outputs treated as provisional; human validation required	All AI-generated analysis reviewed, verified, and approved by credentialled researcher
Transparency	AI use disclosed in all outputs	Disclosure statement in methodology section of all AI-assisted reports
Proportionality	AI use proportionate to task sensitivity and risk	Enhanced scrutiny for AI use in analyses affecting vulnerable populations or policy decisions

Part C
Data Protection & Privacy

10. Multi-Jurisdictional Compliance Framework

DevCAFE operates a principle of maximum protection: where multiple legal frameworks apply to a given dataset or project, the most stringent applicable requirements are adopted as the operational standard. Compliance is assessed on a per-project basis using the Regulatory Compliance Matrix set out in Section 4.

For all ASEAN-based operations, DevCAFE applies the ASEAN Framework on Personal Data Protection (AFPDP) principles as the minimum standard, and escalates to applicable national law where requirements are more demanding. For projects involving data subjects from the European Union, GDPR requirements apply in full.

11. Data Classification and Handling

11.1 Four-Tier Classification System

Tier	Classification & Examples	Handling Requirements
TIER 1 — CRITICAL	Special category / highly sensitive: Biometric, health/medical, ethnic/racial identity, sexual orientation, political opinions, criminal records, GBV survivor data	Explicit consent; AES-256 encryption; named individual access only; mandatory deletion on project close; 24hr internal breach notification
TIER 2 — SENSITIVE	Personally Identifiable Research Data: Names, contacts, income, household composition, employment status, community membership	Informed consent; pseudonymisation as default; restricted access with audit log; 72hr breach notification
TIER 3 — INTERNAL	Confidential Institutional/Client Data: Client strategy, financial data, draft reports, stakeholder mapping, proprietary methodologies	NDA coverage required; internal access controls; written authorisation for external sharing
TIER 4 — PUBLIC	Non-identifiable Research Data: Aggregated statistics, published reports, public policy analyses, fully anonymised datasets	Standard professional handling; may be published subject to quality review and attribution

11.2 Special Category Data — Enhanced Protection

The following data categories attract the highest level of protection under this Policy, irrespective of tier classification:

- Ethnic, racial, or indigenous identity
- Religious or philosophical beliefs
- Political opinions and party or organisational affiliations
- Health, medical, and biometric data
- Sexual orientation and gender identity

- Financial vulnerability indicators (extreme poverty, debt, dependence)
- Immigration, refugee, or stateless status
- Location data of persons in conflict-affected or high-risk security contexts
- Data pertaining to minors (under 18 years in all jurisdictions)
- Data from indigenous communities with collective data rights

12. Data Collection and Informed Consent

12.1 Consent Standards

DEVCAFE CONSENT STANDARD — SEVEN PILLARS
1 FREE: Voluntarily given, without coercion, inducement, or power imbalance
2 INFORMED: Based on clear, accessible explanation in participant's preferred language
3 SPECIFIC: For a defined, stated purpose — not blanket or open-ended consent
4 UNAMBIGUOUS: Expressed through a clear affirmative action — not pre-ticked boxes or silence
5 WITHDRAWABLE: Participant may withdraw at any time without penalty or adverse consequence
6 DOCUMENTED: Evidenced in writing, audio recording, or verified digital trail
7 REVISABLE: Re-consenting required where research purpose changes materially

12.2 Informed Consent Process — Required Elements

The consent process must communicate the following in the participant's preferred language:

- Identity and contact details of DevCAFE and the Principal Researcher
- Research purpose and how findings will be used
- Nature, duration, and scope of the participant's involvement
- Types of data to be collected and how they will be recorded
- How data will be stored, who will have access, and for how long
- How data will appear in reports (anonymised / attributed / quoted)
- The voluntary nature of participation and the unconditional right to withdraw
- Whether withdrawal affects the usability of already-collected data
- Contact details for questions, concerns, and withdrawal requests
- Name and contact of DevCAFE's Data Protection Lead

12.3 Special Consent Situations

- Minors (under 18): Written parental/guardian consent plus child's assent where developmentally appropriate
- Illiterate participants: Oral consent, witnessed by a neutral third party, audio-recorded
- Indigenous communities: Community-level consent from recognised leadership, plus individual consent
- Vulnerable adults with limited capacity: Capacity assessment; proxy consent procedures apply
- Conflict-affected contexts: Heightened risk assessment; security risks to participants explicitly addressed
- Digital/online research: Digital consent mechanism equivalent to physical signature; IP logging alone insufficient

13. Data Storage and Security Standards

13.1 Technical Security Requirements

- All Tier 1 (Critical) data encrypted at rest using AES-256 or equivalent
- All data in transit protected using TLS 1.2 or higher
- Cloud storage providers contractually bound to ISO/IEC 27001 compliance
- Physical research materials stored in locked facilities with restricted key access
- No research data stored on personal devices without full device encryption and mobile device management controls
- Access to identifiable data restricted to named project team members on need-to-know basis
- Access logs maintained for all Tier 1 and Tier 2 data systems, retained for 3 years
- Two-factor authentication required for all systems holding Tier 1 or Tier 2 data

13.2 Cloud and Third-Party Processors

- All third-party data processors must be subject to a Data Processing Agreement (DPA) or equivalent
- Storage locations must be disclosed to data subjects where required by applicable law
- Data stored outside the project's primary operating country must comply with cross-border transfer requirements (see Section 15)
- A Third-Party Processor Register is maintained for each project by the Data Protection Lead

13.3 Pseudonymisation and Anonymisation

- Participant names and direct identifiers replaced with unique codes at point of data entry where feasible
- Code keys stored separately from research data with separate access controls
- Anonymisation (irreversible) applied prior to publication and archival per the project's Data Management Plan
- Coded data is not anonymous — it retains Tier 2 (Sensitive) classification until de-identification is verified

14. Data Retention and Deletion Protocol

14.1 Retention Principles

Data is retained only for as long as necessary for the stated research purpose, or as required by applicable law, contractual obligation, or funder requirement. The most extended applicable requirement governs the retention period.

14.2 Standard Retention Schedule

Data Type	Standard Retention Period
Signed informed consent forms	5 years from project close (or funder requirement — whichever is longer)
Primary research data (identifiable/Tier 1–2)	3 years from project close, unless funder or law specifies longer
Primary research data (anonymised/Tier 4)	Up to 10 years, subject to Data Management Plan
Audio/video recordings	Duration of analysis; deleted within 6 months of project close unless specified in consent form
Interview transcripts (identified)	3 years from project close; then anonymised or deleted
Field notes and research diaries	3 years from project close
Client documents (Tier 3 Confidential)	5 years from project close, or per contractual terms
NDA and confidentiality agreements	10 years from project close or termination
Financial records related to projects	7 years (or as required by applicable tax/audit law)

Data Type	Standard Retention Period
Data breach and incident records	5 years from resolution of incident
Ethics review documentation	10 years from project close
Third-Party Processor Registers	5 years from project close
Access logs (Tier 1 and Tier 2 systems)	3 years

14.3 Secure Deletion Methods

- Electronic data: NIST SP 800-88 compliant deletion (clear, purge, or destroy depending on medium); single-pass overwrite insufficient for Tier 1 data
- Cloud storage: Deletion confirmed via provider certification and audit log entry
- Physical materials: Cross-cut shredding for paper; degaussing or certified physical destruction for portable media
- Backups and archives: All copies and backups included in deletion process; no orphaned copies

⚠ WITHDRAWAL OF CONSENT — DATA DELETION PROTOCOL
When a participant withdraws consent during a study, DevCAFE will:
(a) Immediately cease all further data collection from that individual
(b) Assess whether already-collected data can be removed without prejudicing the scientific validity of prior analysis
(c) Inform the participant in plain language what data (if any) will be retained and why
(d) Document the withdrawal decision and any data retention rationale in the project file
NOTE: Where irreversible destruction of already-collected data is not possible, this must be disclosed in the informed consent form at the outset of the research.

A Data Deletion Certificate (Template T4) must be completed and filed for all Tier 1 and Tier 2 datasets upon deletion.

15. Cross-Border Data Transfers

Cross-border data transfers are a routine feature of DevCAFE's multi-country operations and must comply with the following requirements:

- Applicable law of the jurisdiction where data was collected
- Applicable law of the jurisdiction where data will be processed or stored
- ASEAN Model Contractual Clauses (MCCs) for intra-ASEAN transfers
- EU Standard Contractual Clauses (SCCs) where EU data subjects are involved
- APEC CBPR where applicable to certified entities in the Philippines or Singapore
- Contractual safeguards equivalent to ASEAN MCCs for transfers outside ASEAN and the EU

DevCAFE maintains a Cross-Border Data Transfer Register for all projects involving cross-national data movement. All transfers must be approved in advance by the Data Protection Lead, documented, and communicated to data subjects where required by applicable law.

16. Data Breach Response Procedure

16.1 Definition

A data breach is any incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes both security incidents (cyberattack, device theft) and human error (misdirected email, accidental publication of identifiable data).

16.2 Response Steps

Step	Action
1 CONTAIN	Immediately limit the scope of the breach: isolate affected systems, revoke access credentials, secure physical materials
2 ASSESS	Determine data affected, likely risks to data subjects, and probable cause; record assessment in Breach Register
3 NOTIFY (Internal)	Alert Data Protection Lead and Country Director within 4 hours of discovery
4 NOTIFY (Regulatory)	Report to applicable authorities within mandatory timeframes: 72hr (Philippines DPA / GDPR); 14 days (Indonesia PDP Law); 3 business days (Singapore PDPA)
5 NOTIFY (Participants)	Inform affected data subjects where the breach poses high risk to their rights and freedoms, using clear and accessible language
6 DOCUMENT	Record all breach details, response actions, notifications, and outcomes in the Breach Register
7 REMEDIATE	Conduct root cause analysis; implement prevention measures; report to Governing Board where breach is material

Part D
Confidentiality & Non-Disclosure

17. Client Confidentiality Policy

17.1 Scope of Confidential Information

DevCAFE treats as confidential all non-public information received from clients, including:

- Strategic plans, organisational analyses, and internal assessments
- Financial data, budget allocations, and procurement-related information
- Draft research findings, evaluations, and reports prior to publication
- Proprietary methodologies, theories of change, and programme designs
- Stakeholder lists, political relationships, and negotiation positions
- Human resources information and personnel-related data
- Any information explicitly marked Confidential, or shared in circumstances that reasonably imply confidentiality

17.2 Client Confidentiality Obligations

- Client information used solely for purposes of the contracted engagement
- No disclosure to third parties without prior written consent of the client
- Security measures applied to client information equivalent to those applied to DevCAFE's own confidential information
- Client information returned or securely deleted upon project completion or at client request
- Confidentiality obligations maintained for a minimum of five (5) years post-project completion

17.3 Safety Override — Limits on Confidentiality

SAFETY OVERRIDE PRINCIPLE
Where DevCAFE researchers encounter information indicating a risk of serious or imminent harm to any individual or group — including exploitation, abuse, violence, trafficking, or child harm — confidentiality obligations are superseded by the duty of care. In such cases:
(a) The researcher reports immediately to the DevCAFE Data Protection Lead and Country Director
(b) Appropriate authorities (law enforcement, safeguarding bodies) are notified
(c) Disclosure is documented using only the minimum information necessary
(d) The affected individual is supported with referral to appropriate services where possible
This principle reflects DevCAFE's foundational commitment: participant safety always takes precedence.

Confidentiality obligations also do not apply where disclosure is required by applicable law, a court order, or regulatory requirement; where information was already in the public domain at the time of receipt; or where information was independently developed by DevCAFE.

18. Staff and Consultant Confidentiality Obligations

All individuals working with DevCAFE — regardless of role, engagement type, or location — are subject to the following obligations:

- Confidentiality agreement signed before accessing any project data or client information
- No discussion of project-specific findings, client names, or participant information outside the project team
- No sharing of project data via personal email, social media, or any unsecured channel
- Obligation to report any actual or suspected breach immediately to the Data Protection Lead
- Confidentiality obligations survive termination of the consulting or employment relationship (minimum 5 years)

Breach of confidentiality obligations constitutes grounds for immediate termination of engagement and may expose the individual to legal liability under applicable data protection law. DevCAFE reserves the right to pursue all legal remedies available in the applicable jurisdiction.

19. Non-Disclosure Agreement Policy

DevCAFE operates a mandatory NDA framework for all engagements involving sensitive or confidential data:

Engagement Type	NDA Requirement
All external consultants and sub-contractors	Mandatory bilateral NDA before project commencement
Translators and transcriptionists	Mandatory NDA covering all materials accessed
Data entry and field research staff	Mandatory NDA covering all primary data collected
Technology and software vendors with data access	Mandatory NDA plus Data Processing Agreement (DPA)
Client organisations	Mutual NDA recommended; confidentiality clause in engagement contract minimum
Partner institutions and academic collaborators	NDA or MOU with confidentiality provisions
Interpreters (in-person KII / FGD)	Mandatory NDA before session commencement
Junior researchers and research assistants	Mandatory NDA before data access granted

Modifications to DevCAFE's standard NDA (Template T2) require written approval from the Country Director. NDAs are retained for a minimum of 10 years following project close.

Part E
Participant Rights & Safety

20. Informed Consent Framework

20.1 Language and Accessibility

- All consent forms and participant information sheets must be available in the participant's primary language
- Where participants are not literate, oral consent procedures must be used and documented
- Technical and research jargon must be avoided; plain language standards apply in all communications
- Adequate time must be given for participants to review information and ask questions before consenting
- Consent must not be rushed, incentivised in ways that compromise voluntariness, or obtained under conditions of distress or duress

20.2 Secondary Use of Data

Data collected for one research purpose may not be repurposed for a materially different objective without renewed participant consent. Where DevCAFE intends to archive data for future use, this must be disclosed and specifically consented to at the time of original data collection.

21. Participant Rights

Right	Description	DevCAFE Obligation
Right to be Informed	Full information about who is conducting research, why, and how data will be used.	Participant information sheet in local language before consent
Right to Consent	No participation without free and informed agreement.	Documented consent before any data collection begins
Right to Withdraw	Exit the research at any time without penalty or adverse consequence.	Communicate clearly; cease data collection immediately upon request
Right to Access	Request to see the data held about them.	Respond within 30 days; provide data in accessible format
Right to Correction	Request correction of inaccurate or incomplete data.	Process promptly; update records; notify downstream users of correction
Right to Deletion	Request deletion of personal data where feasible.	Assess; respond; document any limitations on deletion in project file
Right to Confidentiality	Identity not disclosed without explicit consent.	Apply anonymisation/pseudonymisation; review all outputs for identifiability
Right to Safety	Research participation must not expose participant to harm.	Conduct harm assessment prior to data collection; apply Do No Harm protocols

Right	Description	DevCAFE Obligation
Right to Explanation	Understand how any automated decision-making uses their data.	Disclose AI use; explain any automated analysis of participant-provided data

22. Do No Harm and Safety Protocols

22.1 Risk Assessment

Prior to any primary research involving human participants, a Participant Risk Assessment must be completed addressing:

- Physical safety risks — particularly in conflict-affected, politically sensitive, or high-crime contexts
- Psychological and emotional risks — including potential distress from discussing trauma, discrimination, or sensitive personal history
- Social and community risks — including risks of stigma, exclusion, or retaliation
- Economic risks — including potential loss of employment, income, or benefits
- Digital safety risks — including risks from digital data collection, online communication, or traceable participation

22.2 Risk Mitigation

- High-risk contexts: Security protocols; anonymous participation options; secure communication channels; researcher security briefings
- Psychological risk: Trauma-informed interview techniques; referral pathways to psychosocial support services
- Social risk: Community consent; anonymisation by default; no community-identifiable outputs without approval
- Digital risk: Encrypted data capture; offline-capable collection tools; no location tracking without explicit consent

22.3 Referral Protocols

All DevCAFE researchers operating in contexts where participants may disclose harm, distress, or dangerous situations must have pre-established referral pathways to appropriate support services (psychosocial, legal, health, protection). These pathways must be documented in the Research Ethics Declaration (Template T5) prior to data collection.

23. Vulnerable and Marginalised Participants

DevCAFE's work frequently involves communities characterised by vulnerability, marginalisation, or significant power imbalances. Enhanced protections apply to research involving:

- Children and minors (under 18 years)
- Survivors of gender-based violence, sexual violence, trafficking, or abuse
- Persons with physical or intellectual disabilities
- Refugees, asylum seekers, internally displaced persons, and stateless persons
- Indigenous, ethnic minority, and tribal communities
- Persons in institutional settings (prisons, detention centres, hospitals, shelters)
- LGBTQIA+ individuals in contexts where their identity is criminalised or stigmatised
- Persons in extreme poverty or with significant economic dependency on researchers or funders
- Persons living in active conflict zones or under authoritarian governance

Enhanced protections include: additional risk assessment layers; adapted and extended consent procedures; heightened anonymisation standards; additional data security measures; extra caution in all data publication and dissemination; and post-research participant follow-up where appropriate and safe.

Part F
Governance & Accountability

24. Roles and Responsibilities

Role	Responsibilities
Global Governing Board	Ultimate accountability for this Policy; approval of major policy amendments; receive annual compliance report from Country Director; review material data breaches
Country Director	Day-to-day accountability for policy implementation; approve NDAs and non-standard consent processes; resolve conflict of interest cases; escalation point for ethics disputes; annual report to Governing Board
Data Protection Lead	Designated operational contact for all data protection matters; maintains Data Register, Breach Register, Third-Party Processor Register, and Cross-Border Transfer Register; processes withdrawal requests; oversees deletion procedures
Project Team Leader	Ensures policy compliance on assigned projects; completes Risk Assessments and Ethics Declarations; submits and adheres to Data Management Plans; oversees consent processes in the field
All Research Staff & Consultants	Adhere to all provisions of this Policy; complete mandatory training; report breaches and concerns; handle data in accordance with tier classification; sign NDA before project commencement
HR / Admin Lead	Ensures all staff and consultants sign confidentiality agreements; tracks training completion; maintains personnel confidentiality records; manages NDA register

25. Training and Capacity Development

All DevCAFE personnel who collect, process, or access research data must complete:

- Induction training on this Policy before commencing any data-related work
- Annual refresher training covering data protection updates, research ethics, and confidentiality
- Project-specific training where a project involves particularly sensitive data types or vulnerable populations
- FRAME Methodology training for any personnel using automated analysis, AI, or machine learning tools in research

Training completion is documented and maintained by the HR and General Administration Specialist. Non-completion of mandatory training results in restricted access to project data until training is verified. Training records are retained for a minimum of 5 years.

26. Review, Audit and Complaints

26.1 Policy Review

This Policy is reviewed by the Global Governing Board no less than every two years from the effective date of 1 January 2018, or sooner upon: material changes in applicable law in any key operating jurisdiction; significant operational changes; material data breach; or Governing Board resolution. All amendments are subject to Governing Board approval.

26.2 Compliance Audit

DevCAFE conducts annual internal compliance audits covering: data handling practices; consent documentation; NDA compliance; breach and incident records; third-party processor compliance; and retention and deletion procedures. Audit findings are reviewed by the Country Director and reported to the Governing Board. Material gaps result in a documented remediation plan with timelines and accountable officers.

26.3 Complaints and Concerns

Any person — staff, consultant, research participant, client, partner, or member of the public — who has a concern about DevCAFE's data protection or research integrity practices may contact:

CONTACT — DATA PROTECTION & COMPLAINTS
Data Protection Lead: dataprotection@devcafe.org
Country Director: cop@devcafe.org
General Enquiries: info@devcafe.org
Website: www.devcafe.org
DevCAFE is committed to responding to all data protection complaints within 15 working days.
All complaints are handled confidentially and without adverse consequence to the complainant.
Where a complaint is not resolved to the complainant's satisfaction, they are directed to the applicable national data protection authority in their jurisdiction.

Part G
Standard Templates

The following six templates constitute the official DevCAFE standard forms, approved by the Global Governing Board on 25 June 2017. Project Team Leaders are required to use these templates without material modification. Modifications require approval from the Country Director and the Data Protection Lead.

TEMPLATE T1 — INFORMED CONSENT FORM

Approved by Global Governing Board, 25 June 2017 | Applicable Globally

FOR PARTICIPANT INFORMATION — READ CAREFULLY

This research is conducted by The Development CAFÉ (DevCAFE), a global research think tank.

Your participation is entirely voluntary. You may stop at any time without any consequence whatsoever.

Please read this form carefully. Ask any questions you have before signing or agreeing to participate.

Project Name	[INSERT PROJECT NAME]
Country / Location	[INSERT COUNTRY AND SITE]
Principal Researcher	[INSERT NAME AND CONTACT]
Date of Session	[INSERT DATE]
Session Type	[ ] Key Informant Interview [ ] Focus Group Discussion [ ] Survey [ ] Other: _____

1. ABOUT THIS RESEARCH

[Describe the research purpose in plain language — 2–3 sentences. State who commissioned the research and how findings will be used.]

2. YOUR PARTICIPATION

You are being asked to participate in a [INTERVIEW / FOCUS GROUP / SURVEY]. Your participation will take approximately [X] minutes. You will be asked about: [brief description of topics].

3. YOUR DATA

With your consent, we will [record / take notes / collect survey responses]. Your data will be stored securely for [X years] and then [deleted / anonymised per our Data Retention Policy]. Your identity will [be kept fully confidential / appear in the report as: _____].

4. YOUR RIGHTS

- You may refuse to answer any question at any time, for any reason
- You may withdraw from this research at any time without penalty
- You may request to access, correct, or delete your data by contacting: [DATA PROTECTION LEAD CONTACT]
- If you have concerns, you may also contact the national data protection authority: [INSERT COUNTRY-SPECIFIC AUTHORITY AND CONTACT]

5. DECLARATION OF CONSENT

I have read (or had read to me) the information above. I have had the opportunity to ask questions and they have been answered to my satisfaction. I understand that my participation is entirely voluntary and that I may withdraw at any time without consequence.

Participant Name (print)	
Signature / Thumbprint	
Date	

Preferred Language	
Researcher Name	
Researcher Signature	
Date	

Please tick all that apply:

- [ ] I consent to this session being audio-recorded
- [ ] I consent to anonymous quotes from this session being used in published reports
- [ ] I consent to my data being archived for future related DevCAFE research [DELETE IF NOT APPLICABLE]
- [ ] I would like to receive a summary of the final research findings

If ticking the last box, please provide contact: _____

TEMPLATE T2 — NON-DISCLOSURE AGREEMENT (NDA)

Approved by Global Governing Board, 25 June 2017 | Applicable Globally

This Non-Disclosure Agreement (the "Agreement") is entered into as of [DATE] between:

THE DEVELOPMENT CAFÉ (DevCAFE), a global research think tank established and headquartered in the Republic of Indonesia ("Disclosing Party"); and

[FULL LEGAL NAME OF PARTY] of [ADDRESS / ORGANISATION] ("Receiving Party").

1. Purpose

This Agreement is entered into in connection with [PROJECT NAME / ENGAGEMENT DESCRIPTION] ("the Purpose"). The Receiving Party will have access to Confidential Information of the Disclosing Party solely for the Purpose.

2. Definition of Confidential Information

"Confidential Information" means all non-public information disclosed by the Disclosing Party in connection with the Purpose, including but not limited to: research data (primary and secondary), client identities and information, participant data, analytical methodologies, draft findings, financial data, stakeholder information, and any information marked as confidential or disclosed in circumstances implying confidentiality.

3. Obligations of the Receiving Party

The Receiving Party agrees to: (a) hold all Confidential Information in strict confidence; (b) use Confidential Information solely for the Purpose; (c) not disclose Confidential Information to any third party without prior written consent; (d) apply no less protective security measures than those applied to its own confidential information; (e) promptly notify the Disclosing Party of any actual or suspected unauthorised disclosure.

4. Data Protection Compliance

The Receiving Party agrees to handle all personal data in compliance with applicable data protection law and DevCAFE's Data Protection Policy, including: Indonesia PDP Law No. 27/2022; Philippines RA 10173; ASEAN Framework on Personal Data Protection; EU GDPR (where applicable); and all other applicable national requirements.

5. Exclusions

This Agreement does not apply to information that: (a) is or becomes publicly available through no fault of the Receiving Party; (b) was already known to the Receiving Party at the time of disclosure; (c) is independently developed by the Receiving Party; (d) is required to be disclosed by law or court order (with prior written notice to the Disclosing Party where permitted by law).

6. Return and Deletion

Upon completion of the Purpose, or upon request, the Receiving Party shall promptly return or securely delete all Confidential Information and provide written certification of deletion within 10 working days.

7. Term and Survival

This Agreement takes effect from the date of signing and shall remain in force for five (5) years following completion or termination of the Purpose. Obligations relating to Tier 1 (Critical) data survive indefinitely.

8. Governing Law

This Agreement is governed by the laws of [APPLICABLE JURISDICTION — default: Republic of Indonesia]. Disputes shall be resolved through good-faith negotiation, followed by binding arbitration under the rules of [APPLICABLE ARBITRATION BODY].

FOR DevCAFE — Authorised Signatory	Signature: _____ Date: _____
FOR RECEIVING PARTY — Name & Title	Signature: _____ Date: _____
Organisation	_____
Official Stamp / Seal	[ ]

TEMPLATE T3 — DATA MANAGEMENT PLAN (DMP)

Approved by Global Governing Board, 25 June 2017 | Applicable Globally | Complete before data collection

Project Name	
Principal Researcher / TL	
Client / Commissioning Body	
Operating Jurisdiction(s)	
Project Duration	
DMP Version	
Date Prepared / Revised	
Approved by Data Protection Lead	

Section 1: Data Overview

Describe data types (qualitative/quantitative/mixed), formats, estimated volumes, and primary collection methods (KII, FGD, survey, desk review, geospatial, etc.):

[Complete here]

Section 2: Data Classification

Identify applicable tier(s). Justify any Tier 1 (Critical) or Tier 2 (Sensitive) collection. Specify all special category data types:

[Complete here]

Section 3: Consent and Legal Basis

Describe consent process. Identify legal basis in each operating jurisdiction. Attach draft consent form. Address any special consent situations:

[Complete here]

Section 4: Storage and Security

Specify storage platform(s), encryption standards, access controls, and backup procedures. Identify third-party processors and confirm DPAs are in place:

[Complete here]

Section 5: Retention and Deletion

Specify retention period per data type and deletion method. Confirm responsible officer for executing and certifying deletion:

[Complete here]

Section 6: Cross-Border Transfers

Identify all cross-border transfers. Confirm transfer mechanism (ASEAN MCCs / EU SCCs / CBPR / contractual safeguards). Document countries involved:

[Complete here]

Section 7: Risk Summary

Summarise key data risks identified and mitigation measures applied. Reference full Participant Risk Assessment:

[Complete here]

Section 8: Responsibilities

Data Protection Lead (Project Level)	
Data Custodian (Storage Access)	
Deletion Responsible Officer	
Breach Notification Contact	

TEMPLATE T4 — DATA DELETION CERTIFICATE

Approved by Global Governing Board, 25 June 2017 | Complete upon expiry of retention period for Tier 1 and Tier 2 data

OFFICIAL DevCAFE DATA DELETION CERTIFICATE

This certificate provides formal documentation of the secure deletion or destruction of personal and/or confidential research data in accordance with DevCAFE's Data Protection Policy and all applicable legal requirements.

This certificate must be retained for 5 years from date of issuance.

Project Name	
Client / Commissioning Body	
Data Classification Tier(s)	[ ] Tier 1 (Critical) [ ] Tier 2 (Sensitive) [ ] Tier 3 (Internal)
Description of Data Deleted	
Approximate Data Volume	
Storage Platform(s) — Deleted From	
Backup Copies — Deleted From	
Deletion Method Applied	
Standard Complied With	[ ] NIST SP 800-88 [ ] ISO 27001 [ ] Provider Certification [ ] Physical Destruction
Date of Deletion	
Deletion Verified By (Name & Title)	
Signature	
Date of Certificate	

DECLARATION: I confirm that all personal data and confidential information described above has been securely and irreversibly deleted or destroyed in accordance with DevCAFE's Data Protection Policy, the project's Data Management Plan, and all applicable legal requirements. No copies of the deleted data are retained by DevCAFE or any contracted processor in any format, digital or physical.

☑ TEMPLATE T5 — RESEARCH ETHICS DECLARATION

Approved by Global Governing Board, 25 June 2017 | Complete before any primary data collection commences

Project Name	
Principal Researcher	
Operating Countries	
Date of Declaration	

I declare that for this DevCAFE research project, the following standards and requirements have been met:

RESEARCH INTEGRITY

[ ] Research design documented and approved prior to data collection

[ ] Conflict of interest disclosure completed for all team members

[ ] AI/automated tool use is disclosed and FRAME-compliant

[ ] DevCAFE apolitical and areligious mandate respected in design and framing

DATA PROTECTION

[ ] Data Management Plan completed, reviewed, and approved

[ ] Data Classification completed; all tiers identified

[ ] Third-Party Processor Register established; DPAs in place

[ ] Cross-border transfer mechanisms confirmed (where applicable)

[ ] Retention schedule documented; deletion officer designated

CONSENT AND PARTICIPANT RIGHTS

[ ] Informed consent process designed; forms available in participant language(s)

[ ] All special consent situations addressed (minors, illiteracy, indigenous communities, etc.)

[ ] Participant rights communicated clearly in consent documentation

CONFIDENTIALITY

[ ] NDAs signed by all project team members before data access

[ ] Client confidentiality obligations reviewed with team

SAFETY AND DO NO HARM

[ ] Participant Risk Assessment completed

[ ] Risks identified and mitigation measures implemented

[ ] Referral pathways for participant safety concerns documented

[ ] Vulnerable population protocols activated (if applicable)

Additional ethics notes, risks, or concerns:

_____

_____

Researcher Signature	
Date	
Reviewed by (Data Protection Lead)	
Date	
Approved by (Country Director)	
Date	

TEMPLATE T6 — PARTICIPANT SAFETY ASSESSMENT

Approved by Global Governing Board, 25 June 2017 | Complete for ALL primary research with human participants

Project Name	
Country / Context	
Participant Group(s)	
Researcher Name	
Date of Assessment	

Risk Category	Risk Present? (Yes / No / Unknown)	Mitigation Measure
Physical safety — conflict, crime, violence		
Political risk — association with research		
Psychological distress — sensitive topics		
Social stigma — community or family repercussions		
Economic risk — employment or income at risk		
Digital safety — device, location, communication		
Legal risk — criminalisation of identity/activity		
Power imbalance — researcher-participant dynamics		
Minor participation — child safeguarding risk		
Vulnerable adult — capacity / dependency risk		

Referral Pathways Documented:

Psychosocial support: _____

Legal support: _____

Protection / safety: _____

Health services: _____

Overall Risk Level: [ ] Low [ ] Medium [ ] High [ ] Critical (requires Country Director approval)

Researcher Signature	
Reviewed by (Team Lead)	
Date	

Public Policy Statement
For Publication on the DevCAFE Website

The Development CAFÉ (DevCAFE) is a global research, technology, and development think tank operating across 40+ countries. We exist to bridge the distance between the lived realities of communities and the decisions made by policymakers. We do this work with independence, rigour, and deep respect for the people who trust us with their knowledge, their data, and their voices.

This Policy was adopted by our Global Governing Board on 25 June 2017 and applies to every project, every team member, and every partners globally, without exception.

OUR PUBLIC COMMITMENTS

RESEARCH INTEGRITY: All DevCAFE research is conducted with intellectual honesty and methodological rigour. We are apolitical and areligious. Our findings follow the evidence, not the funder.

DATA PROTECTION: We collect only the data we need. We store it securely. We delete it when its purpose is fulfilled. We comply with applicable data protection law in all 40+ countries we operate in, including Indonesia's PDP Law, the Philippines' Data Privacy Act, Singapore's PDPA, Thailand's PDPA, Vietnam's Decree 13/2023, and the ASEAN Framework on Personal Data Protection.

INFORMED CONSENT: No one participates in DevCAFE research without free, informed, and voluntary consent. Every participant may withdraw at any time. Their rights are protected by our Policy.

CONFIDENTIALITY: All client and participant information is treated as confidential and protected by legally binding agreements. We do not disclose confidential information without consent.

PARTICIPANT SAFETY: Do No Harm is a non-negotiable standard in all DevCAFE research. Where participant safety is at risk, safety overrides all other considerations.

ACCOUNTABILITY: DevCAFE takes full responsibility for all data in its care. Breaches are reported, investigated, and remediated. This Policy is reviewed by our Governing Board, and is available publicly as our declaration of standards.

Questions about our data practices or to exercise your rights as a research participant:

admin@devcafe.org | www.devcafe.org

Approved by the Global Governing Board of The Development CAFÉ (DevCAFE) | 25 June 2017

THE DEVELOPMENT CAFÉ (DevCAFE) — Bridging Grassroots with Policy