hyperSHIFT Ethical Technology & Data Use Policy

Applies to: hyperSHIFT (Pty) Ltd and subsidiaries: hyperLOOP, MINDSHIFTERS, Mindshifters Ministries, Mindshifters Academy
Effective date: [insert date] • Review cycle: annually • Policy owner: Group Data Protection & Ethics Lead (G-DPEL)

---

1) Purpose

Set clear, practical standards for building and using technology—especially AI and data systems—in ways that are lawful, secure, fair, transparent, and aligned with our values and South African regulations (POPIA), plus other applicable laws where we operate.

2) Scope

Covers all people acting for hyperSHIFT (employees, contractors, volunteers), all systems (internal and third-party), and all processing of personal information (including special/sensitive categories) across web, apps, analytics, marketing, counselling/ministry contexts, training, research, and media/storytelling.

3) Foundations & Commitments

- **Human dignity first:** Technology must serve people, not the other way around.
- **Lawful, fair, transparent:** POPIA-aligned processing with clear purposes and notices.
- **Security by design:** Reasonable technical and organisational measures throughout the lifecycle.
- **Explainable & accountable AI:** Appropriate human oversight, documentation, and appeal paths.
- **Minimise and de-identify:** Collect only what's necessary; anonymise/pseudonymise wherever possible.
- **No dark patterns:** Interfaces must not mislead or coerce.
- **No surveillance-style practices:** Avoid intrusive tracking; use proportionate, consent-based analytics.
- **Do no harm:** Assess risk to vulnerable people; take additional protections for children and clients in counselling/ministry settings.
- **Stewardship:** Treat data as entrusted, not owned.

---

4) Legal & Standards Alignment

- **South Africa:** POPIA (Act 4 of 2013), PAIA, ECTA, Cybercrimes Act.
- **Where relevant:** GDPR (EU/UK), CPA (Consumer Protection Act), industry codes (ASA, IAB), and professional ethics for counselling/mediation.
- **Standards:** NIST Cybersecurity Framework, ISO/IEC 27001/27701 (as guidance), OWASP ASVS.

If standards conflict, the **stricter** or more protective requirement applies.

---

5) Roles & Accountability

- **Board / ExCo:** Approves policy, receives annual data ethics & security report.
- **G-DPEL:** Owns policy, DPIAs, incident coordination, and vendor risk.
- **Data Stewards (per brand):** Ensure compliance in their domain (e.g., MINDSHIFTERS clinical records, Academy learner data).
- **System Owners:** Keep accurate data maps, access lists, and retention schedules.
- **All Personnel:** Complete training, follow this policy, report incidents or concerns.
- **Vendors/Partners:** Contractually bound to equivalent or stronger controls.

---

6) Lawful Basis & Special Categories

- **Lawful bases (POPIA):** consent, contract, legal obligation, legitimate interests (balanced), vital interests, public task (if applicable).
- **Special/sensitive data:** health, religious/faith data (Ministries), counselling notes, minor’s data—**strict necessity only**, with explicit consent where required, role-based access, encryption, and enhanced retention controls.

---

7) Data Lifecycle Controls

7.1 Collection & Notices

- Clear privacy notices (purpose, lawful basis, retention, rights, contacts).
- Separate, granular consent for optional uses (e.g., marketing, analytics, media).

- Children: obtain verifiable guardian consent; age-appropriate notices.

7.2 Minimisation & Quality

- Only necessary fields; regular accuracy checks; discourage free-text where sensitive content isn't needed.

7.3 Storage & Security

- Encrypt at rest and in transit; MFA for admin access; least-privilege access; segregate production and test data; no live PII in test without masking/anonymisation.

7.4 Use & Sharing

- Use data only for stated purposes; new purpose requires compatibility assessment or new consent.
- Data Processing Agreements (DPAs) with vendors; records of processing maintained.

7.5 Retention & Deletion

- Retention schedules per category (e.g., marketing contacts: 24 months inactivity; counselling records: per clinical guidance and legal minimums).
- Documented deletion/archival; secure wipe from backups per schedule where feasible.

7.6 Cross-Border Transfers

- Transfer only to jurisdictions with adequate protection or with safeguards (SCCs/Binding rules), plus risk assessment and user notice where required.

---

8) Security Baseline (Technical & Organisational)

- MFA for all privileged accounts; SSO where possible.
- Regular patching, vulnerability scans, and penetration tests on Internet-facing assets.
- Network segmentation; secret management (vaulted); audit logs with tamper protection.
- Device controls: full-disk encryption, EDR/anti-malware, screen locks, no unmanaged BYOD for sensitive workloads.
- Backups: encrypted, tested restores, 3-2-1 principle.

- Incident Response Plan (IRP) with 24/72-hour internal timelines; regulator/data-subject notifications per law.

---

9) Cookies, Tracking & Marketing Tech

- Consent banner for non-essential cookies; honour choices.
- Use privacy-respecting analytics by default; if using third-party pixels, apply server-side tagging, IP masking, and strict data filters.
- No collection of precise geolocation or sensitive inferences for marketing without explicit consent.
- Email/SMS/WhatsApp: opt-in required; one-click unsubscribe/STOP commands honoured promptly.

---

10) Automated Decision-Making & Profiling

- **High-risk decisions** (credit, employment, access to services) may **not** be fully automated; require human-in-the-loop review and an appeal path.
- Provide meaningful information about the logic involved, significance, and envisaged consequences, proportional to the risk.
- Keep model cards or equivalent documentation for significant models.

---

11) AI Use & Governance

11.1 Acceptable Use

- Productivity assistants (e.g., drafting, summarisation) with **no** input of special/sensitive PII unless the tool is approved for such data and bound by DPA.
- Analytics & forecasting using de-identified or aggregated data where possible.

11.2 Prohibited

- Facial recognition for identification; emotion recognition; surreptitious surveillance; scraping protected sources in breach of terms; training on confidential/PII without legal basis and DPA.

11.3 Risk Tiers

- **Low** (content ideation), **Medium** (lead scoring), **High** (clinical triage, learner placement). High-risk requires DPIA, senior sign-off, human oversight, and pilot with guardrails.

11.4 Fairness & Bias

- Assess training data for representativeness; monitor outcomes by relevant segments; document mitigations; allow human override.
- No discriminatory outputs; set thresholds with fairness metrics where used.

11.5 Explainability & Records

- Keep **Model Cards**: purpose, data sources, training method, performance, limitations, monitoring plan.
- Log prompts/decisions (without storing PII unnecessarily) to enable audits.

12) Clinical, Counselling & Ministry Data

- Separate, access-controlled system for clinical notes; audit trails; no marketing use.
- Informed consent forms specify limits of confidentiality and emergency escalation.
- Mandatory escalation for risk of harm; minimum necessary sharing with authorities/guardians.
- Ministry prayer/care lists require consent; default to anonymised sharing in groups.

13) Media, Storytelling & Research

- Written, informed consent for testimonials, photos, video, and **Voices of Hope/Light in the Marketplace** features.
- Dignity-first guidelines: avoid sensationalism, unnecessary identifiers, or sensitive location details.
- De-identify where risk exists; allow withdrawal where feasible (subject to legal/reporting constraints).
- Research uses ethics review (internal or partner); anonymise datasets; register protocols where appropriate.

14) Vendor & Tooling Governance

- Pre-procurement assessment: security, data location, sub-processors, breach history, AI use, compliance posture.
- DPA + SCCs (if cross-border).
- Access reviews quarterly; offboarding checklist to revoke access and ensure data return/destruction.

---

15) Data Subject Rights (POPIA/GDPR-like)

- Right to access, rectify, delete, object, restrict processing, and withdraw consent.
- Requests via info@hypershift.co.za → acknowledge in 48 hours; fulfil within legal timelines.
- Identity verification before action; keep minimal audit record of the request.

---

16) Children & Young People

- Collect the least data necessary; guardian consent verified; higher bar for profiling and tracking—generally avoided.
- No direct marketing to minors.
- Education contexts (Academy): transparent grading/placement criteria; appeals process.

---

17) Data Protection Impact Assessments (DPIAs)

Mandatory for:

- New systems processing special categories;
- Significant profiling/automated decisions;
- Large-scale tracking or cross-border transfers;
- Clinical/ministry data tooling;
- Biometrics or CCTV beyond basic safety.

DPIA Contents: purpose, lawful basis, data flows, risks to individuals, mitigations, residual risk, sign-offs, review cadence.

18) Training & Awareness

- Induction plus **annual refreshers** for everyone; deeper modules for engineers, analysts, counsellors, and ministry/academy staff.
- Phishing simulations and secure-coding clinics for technical teams.

19) Incidents & Breaches

- Report immediately to info@hypershift.co.za.
- IRP steps: contain → assess impact → notify leadership → legal/regulatory assessment → communications → corrective actions → post-mortem.
- Notify Information Regulator and affected data subjects when legally required and risk is non-trivial.

20) Monitoring, Audits & Metrics

- Quarterly privacy & AI ethics dashboard to ExCo (incidents, DSARs, DPIAs, vendor reviews, training completion).
- Annual internal audit; external assurance as needed for major programmes.
- Continuous improvement tickets tracked to closure.

21) Enforcement

Breaches of this policy may lead to disciplinary action up to termination and termination of vendor contracts. Unlawful processing may be reported to authorities.