Data Privacy Framework

1 Leadership & Governance

- Establish clear lines of accountability and oversight for data protection compliance at the highest level of leadership.
- Demonstrate evidence-based compliance with data privacy requirements (e.g. policies, contracts, records and other formal documentation).
- Embed data protection awareness and responsibility into the strategic and operational planning of the organisation.
- Balance the organisation's overall strategy and objectives with a risk-based and proportionate approach to compliance.
- Designate a Data Protection Officer (DPO) or equivalent with direct reporting lines to senior management.
- Manage roles and responsibilities as appropriate across the organisation.
- Implement a comprehensive system or software to manage the organisation's compliance programme.
- Maintain proactive oversight of changes to relevant privacy laws, regulator guidance and best practices.

2 Record of Processing & Data Mapping

- Establish and regularly review a record of processing or personal data inventory for the organisation's processing activities.
- Ensure involvement from key individuals across the organisation in establishing and maintaining the record of processing or personal data inventory.
- Identify technical and organisational measures or controls to reduce or mitigate risks associated with processing personal data.
- Identify any international data flows, cross-border transfers and applicable mechanisms between the organisation and other parties.
- Document lawful bases where applicable for processing personal data (e.g. consent, performance of a contract, legitimate interests).
- Maintain a records management schedule with document type and retention periods clearly defined.
- Create and maintain a data flow map of personal information across the organisation's systems and departments.

3 Incident & Breach Management

- Implement a system or software for the management of personal data incidents and breaches.
- Establish procedures to identify, assess and manage personal data incidents and breaches.
- Ensure that incident and breach reporting involves all appropriate stakeholders (e.g. senior management, affected individuals and external parties).
- Perform periodic internal or independent testing of the incident and breach response plan involving key internal stakeholders.
- Maintain template letters to affected individuals and regulators as appropriate in the event of an incident or breach.
- Monitor trends and patterns relating to incident and breach management (e.g. affected systems, root causes, severity or response times).
- Periodically review incident and breach management procedures in light of stakeholder feedback and lessons learned.

4 Information Rights & Data Ethics

- Maintain procedures for dealing with complaints, queries and all applicable data subject rights.
- Maintain template responses to individuals following data subject requests and complaints.
- Provide simple mechanisms enabling individuals to opt-out of processing, withdraw consent or make use of any other information right.
- Maintain a record of consent, including withdrawn consent, from data subjects or, in the case of children, from parents/guardians.
- Integrate data ethics into procedures for managing requests for information, ensuring transparency, accountability and fairness.
- Ensure that ethical considerations are considered throughout the planning, development and management of processes involving personal data.
- Maintain metrics for handling data subject requests (e.g. number, location, response times).

5 Training & Awareness

- Conduct appropriate data protection training for all staff, including refresher training.
- Ensure that key individuals with data protection responsibility (e.g. DPO or data owners) receive training appropriate for their roles.
- Report to senior management on the efficacy of privacy training by tracking delivery, participation, comprehension and action items.
- Maintain accessible data protection awareness content (e.g. handbooks, newsletters, videos, posters).
- Ensure that staff are aware of whom to contact for questions and queries concerning data privacy.
- Review and revise training content in accordance with new compliance requirements, laws, regulations and best practices.
- Periodically review lessons learned from the organisation's operations to inform and adapt the training curriculum.

6 Data Sharing & Contracts

- Maintain a directory of relevant data controllers, data processors, or third parties with whom data is shared or transferred.
- Maintain data sharing agreements, data processor agreements and contracts, as appropriate.
- Provide clear data protection guidance and expectations for data processors and third parties.
- Ensure that procurement and vendor engagement processes integrate data protection considerations.
- Ensure that disclosures and data sharing decisions for audit, monitoring and investigations are documented and periodically reviewed.
- Perform due diligence or data processor assessments of vendors or other parties as required.
- Utilise appropriate mechanisms for international transfers of personal data (e.g. Standard Contractual Clauses).

7 Information Security & Operations

- Ensure that IT audits, penetration tests or organisation-wide vulnerability assessments include data protection considerations.
- Implement data protection by design and by default into IT system design and operations.
- Maintain appropriate security measures (e.g. encryption) to protect data controlled by the organisation including transit to data subjects, data processors or other parties.
- Create, test and periodically review business continuity, disaster recovery and backup plans that include data protection considerations.
- Ensure that data protection concerns are integrated with information security risk assessments and controls.
- Develop cross-functional relationships between individuals working in information technology and data protection.
- Ensure that IT software and hardware asset inventories are linked and consistent with the organisation's record of processing and data flow map.

8 Risk Management & Controls

- Ensure that management of risks and controls follow an approach consistent with the organisation's risk appetite and tolerance while ensuring compliance.
- Conduct periodic self-assessments of the compliance programme to ensure that legal obligations and the organisation's stated objectives are met.
- Establish a schedule of independent audits, health checks, or assessments of the organisation's compliance programme.
- Implement and monitor the effectiveness of technical and organisational measures or controls that reduce or mitigate risks to data subjects.
- Conduct Data Protection Impact Assessments (DPIA) where appropriate to assess risks associated with processing activities.
- Ensure that processes and procedures reflect safeguarding and welfare considerations for children and vulnerable data subjects.
- Conduct Legitimate Interests Assessments (LIA) where appropriate to balance processing against individuals' rights.

9 Policies & Notices

- Ensure that senior management is involved in periodic review and approval of new and existing privacy policies and notices.
- Implement and regularly review an overarching data protection policy that describes the organisation's approach to compliance.
- Maintain specific policy provisions to address high risk, large scale or sensitive aspects of processing (e.g. marketing, digital media, safeguarding and welfare).
- Inform data subjects wherever processing takes place with appropriate privacy notices or signage (e.g. website, CCTV).
- Ensure that privacy notices are accessible, easy to understand and written in clear and plain language.
- Maintain a schedule for review, update and approval of all privacy policies and notices.
- Record staff acknowledgement and agreement to applicable privacy policies as part of induction and onboarding.