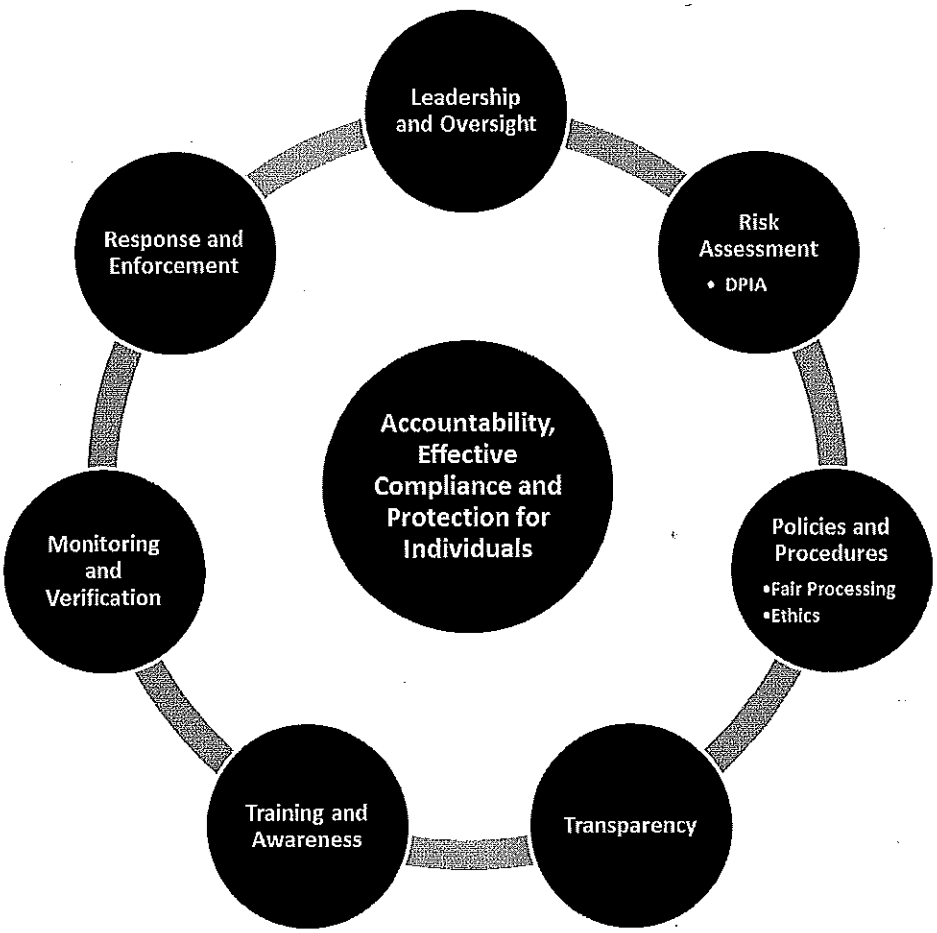

Figure 1 – CIPL "Accountability Wheel" – Universal Elements of Accountability

Accountability Element:	The Accountable Organisation...
Leadership and Oversight	Ensures appropriate data privacy governance, accountability, oversight, reporting, and buy-in from mid-level and top-level management, including appointing appropriate personnel (e.g., DPO or DPO Team, senior level privacy executives and data governance staff) to oversee the organisation's privacy and accountability program and report to senior management and the board.
Risk Assessment	At program level, periodically assesses its privacy program and its relevance in light of changes in business models, risk, law, technology and other external and internal factors. At product, service and project level, implements controls to identify, understand and mitigate risks to individuals and organisations. In case of a data breach incident, assesses the potential risks to the rights and freedoms of individuals to mitigate the risks and perform the relevant notifications to the DPA and the data subjects.

Policies and Procedures	Builds and maintains written data privacy policies and procedures that reflect applicable laws, regulations, industry standards and organisational values and goals and implements mechanisms to operationalise them throughout the organisation. This includes policies and procedures to ensure fair processing and ethical considerations.
Transparency	Communicates to individuals critical information about its data privacy program, procedures and protections, as well as the benefits and/or potential risks of data processing and information about individual rights through easily accessible means (e.g., privacy notices, policies and transparency tools such as dashboards and portals). Communicates and engages with relevant data privacy regulators about its privacy program.
Training and Awareness	Ensures ongoing training and communication to employees, contractors and others who handle data processed by the organisation about the privacy program, its objectives and controls.
Monitoring and Verification	Monitors ongoing internal compliance with the program, policies and procedures and establishes procedures for regular self-assessments, internal audits and in some instances external audit or certifications.
Response and Enforcement	Puts in place appropriate procedures for responding to inquiries, complaints, data protection breaches and internal non-compliance. Enforces against internal non-compliance with the program, rules and controls. Cooperates with third-party certification bodies, Accountability Agents, and data privacy regulators in investigations and enforcement actions.

Table 1 – Organisational measures to implement the elements of accountability