Master Policy Matrix

This Master Policy Matrix serves as the central, authoritative map of the charity's entire governance framework. Its primary function is to visualise the "golden thread" of accountability that runs through the organisation. It achieves this by explicitly connecting the charity's constitutional duties—its internal law—and its external legal obligations to the practical, board-approved policies that function as tangible risk controls. This matrix is not a static list but a dynamic tool for trustees to ensure comprehensive oversight, facilitate the induction of new board members, and demonstrate due diligence to regulators and stakeholders.

The Master Policy Matrix

Policy Reference & Title	Primary Constitutional Driver(s)	Primary External Legal Driver(s)	Core Function / Risk Mitigated
ORG/DP/001 Data Breach Notification Policy	• Duty to manage the affairs and protect the CIO (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR, Articles 33 & 34) • Data Protection Act 2018	Provides a critical framework for a robust and timely response to data breaches. It mitigates the risks of significant harm to beneficiaries, reputational damage, and regulatory fines by ensuring a compliant and structured response.
ORG/DP/002 Subject Access Request (SAR) Handling Policy	• Duty to manage the CIO's affairs lawfully (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR, Article 15) • Data Protection Act 2018	Ensures the charity upholds the fundamental right of access for individuals regarding their personal data. It mitigates the legal and reputational risk of failing to respond to SARs in a lawful, complete, and timely manner.
ORG/DP/003 Lawful Basis Policy (Data Protection)	• Duty to manage the CIO's affairs (Clause 9(1)). • Duty to ensure all activities align with	• UK General Data Protection Regulation (UK GDPR, Articles 6 & 9) • Data Protection Act	Ensures all personal data processing is legally justified from its inception. It mitigates the fundamental risk of

	charitable objects (Clause 3).	2018	unlawful data processing and 'purpose creep' by mandating the documentation of a valid lawful basis for every activity.
ORG/DP/005 Direct Marketing Policy (Soft Opt-in)	• Power to provide a communications network (Clause 3(5)).	• UK General Data Protection Regulation (UK GDPR) • Privacy and Electronic Communications Regulations 2003 (PECR)	Provides a lawful framework for fundraising and informational communications with beneficiaries. It mitigates the legal risk of non-compliant marketing and the reputational risk of contacting individuals against their wishes.
ORG/DP/006 Information Security Policy	• Duty to manage the CIO's affairs and protect its assets (Clause 9(1)). • Duty of care to beneficiaries (Clause 3).	• UK General Data Protection Regulation (UK GDPR, Article 32) • Data Protection Act 2018	Establishes the technical and organisational measures required to protect the charity's information assets. It mitigates the risk of data breaches through preventative controls, safeguarding the confidentiality, integrity, and availability of data.
ORG/DP/007 Privacy Policy	• Duty to manage the CIO's affairs (Clause 9(1)). • Duty to support and communicate with the Beneficiary Community (Clause 3).	• UK General Data Protection Regulation (UK GDPR)• Data Protection Act 2018	Acts as the primary external communication tool for data protection, building trust with beneficiaries and stakeholders. It mitigates the risk of non-transparent data processing and ensures the charity meets its accountability obligations.
ORG/DP/008 Data Retention and Deletion Policy	• Duty to manage the CIO's affairs (Clause 9(1)). • Duty regarding accounting records	• UK General Data Protection Regulation (UK GDPR) • The Charities Act 2011	Manages the information lifecycle to prevent the unnecessary or indefinite retention of

	(Clause 25).		data. It mitigates the risks of non-compliance with the storage limitation principle and reduces the potential scope and impact of a data breach.
ORG/DP/009 Overall Data Protection Policy	• Duty to manage the CIO's affairs (Clause 9(1)). •Duty of care to the Beneficiary Community (Clause 3).	• UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018 • The Equality Act 2010	Establishes the definitive framework for lawful and ethical data processing. It mitigates the risk of non-compliance, reputational damage, and harm to beneficiaries by ensuring adherence to core data protection principles.
ORG/DP/010 Data Subject Rights Policy (Rectification, Erasure, Objection)	• Duty to manage the CIO's affairs lawfully (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR, Chapter 3) • Data Protection Act 2018	Provides a compliant framework for responding to rights beyond access (e.g., rectification, erasure, objection). It mitigates the risk of failing to uphold these statutory rights, which could lead to regulatory action and a loss of trust.
ORG/DP/011 Data Protection Impact Assessment (DPIA) Policy	• Duty to manage the affairs and risks of the CIO (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR, Article 35)	Embeds 'privacy by design' by providing a process to proactively identify and minimise data protection risks associated with new projects. It mitigates the risk of launching high-risk initiatives that could harm individuals or breach data protection law.
ORG/DP/012 Automated Decision-Making Policy	• Duty to manage the CIO's affairs fairly (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR, Article 22) • The Equality Act 2010	Provides essential safeguards for any automated decision-making or profiling activities. It mitigates the risk of

			unfair, biased, or discriminatory outcomes that could harm beneficiaries and create legal liability.
ORG/DP/013 International Data Transfer Policy	• Duty to manage the CIO's affairs and protect its assets (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR, Chapter 5)	Ensures that any transfer of personal data outside the United Kingdom is conducted lawfully and with appropriate safeguards. It mitigates the risk of data being transferred to jurisdictions with inadequate data protection standards, which could harm individuals and breach UK law.
ORG/DP/014 Data Re-use (Further Processing) Policy	• Duty regarding research and heritage objects (Clause 3). • Duty to manage the CIO's affairs (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR) • The Data (Use and Access) Act 2025	Provides a lawful and ethical framework for using existing data for new purposes (e.g., research). It mitigates the risk of unlawful 'purpose creep' and ensures that the reasonable expectations of beneficiaries are respected.
ORG/DP/015 Photography and Images Policy	• Duty of care to beneficiaries (Clause 3). • Duty to manage the CIO's affairs (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018 • General Safeguarding duties	Establishes a lawful and ethical framework for capturing, storing, and using images of individuals. It mitigates critical privacy, data protection, and safeguarding risks, particularly when dealing with vulnerable people.
ORG/DP/017 Complaints Handling Policy (Data Protection)	• Duty to manage the CIO's affairs accountably and lawfully (Clause 9(1)).	• UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018	Provides a specific, compliant procedure for data-related complaints. It mitigates the specific legal risk of failing to handle data protection

			complaints correctly, which can lead to investigation by the Information Commissioner's Office (ICO).
ORG/FIN/001 Trustee Payment Policy	• Power regarding trustee expenses (Clause 5(1)(a)). • Rules regarding benefits and payments to trustees (Clause 6). • Duty to manage conflicts of interest (Clause 7).	• The Charities Act 2011 (sections 185-188) • Charity Commission Guidance (CC11)	Provides a transparent and lawful framework for the rare instances of trustee payment for services or goods. It mitigates the risk of unauthorised financial benefit, conflicts of interest, and breaches of trust.
ORG/FIN/002 Reserves Policy	• Duty to manage the CIO's affairs prudently and ensure its sustainability (Clause 9(1)).	• Charity Commission Guidance (CC19)	Ensures the charity maintains sufficient financial resilience to manage unforeseen events. It mitigates the risk of insolvency or disruption to beneficiary services due to unexpected drops in income or emergency expenditure.
ORG/FIN/003 Investment Policy	• Power to deposit or invest funds (Clause 4(5)). • Duty to manage assets responsibly (Clause 9).	• The Trustee Act 2000 • Charity Commission Guidance (CC14)	Provides a strategic framework for managing the charity's investments. It mitigates the risk of financial loss from inappropriate investments and the reputational risk arising from unethical holdings.
ORG/FIN/004 Internal Financial Controls Policy	• Duty to manage the CIO's affairs (Clause 9(1)). • Duty regarding the application of income and property (Clause 5). • Duty to keep accounting records (Clause 25).	• The Charities Act 2011 • Charity Commission Guidance (CC8)	Establishes a framework of financial discipline, authorisation, and accountability. It mitigates the risk of fraud, error, and misuse of charitable funds, ensuring assets are protected and applied solely for charitable purposes.

ORG/FIN/005 Anti-Fraud Policy	• Duty to manage the CIO's affairs and protect its assets (Clause 9(1)). • Duty regarding the proper application of property (Clause 5).	• The Fraud Act 2006 • The Bribery Act 2010 • Charity Commission Guidance	Establishes a zero-tolerance approach to fraud. It mitigates the risk of financial loss and reputational damage from fraudulent activity by grant applicants, internal actors, or other third parties.
ORG/FIN/006 Support Contribution Grant Policy	• Power to provide financial assistance in deserving cases of need (Clause 3(3)).	• The Charities Act 2011 • Principles of UK Contract Law	Provides a robust framework for assessing and funding ongoing care costs for beneficiaries. It mitigates the risk of creating unmanageable liabilities and ensures funds are directed to those with the greatest demonstrable need.
ORG/FIN/007 General Grant Making Policy	• Power to provide financial assistance by way of grants (Clause 3(3)).	• The Charities Act 2011 • Principles of UK Contract Law	Establishes the formal terms and conditions for grant awards. It mitigates the risk of misapplication of charitable funds and ensures a fair, accountable, and legally sound relationship with beneficiaries.
ORG/GOV/001 Conflicts of Interest Policy	• Duty regarding conflicts of interest (Clause 7). • Rules regarding benefits and payments to trustees (Clause 6).	• The Charities Act 2011 • Charity Commission Guidance (CC29)	Provides the operational framework for identifying, declaring, and managing conflicts. It mitigates the critical risk of decisions being made that are not in the best interests of the charity, thereby protecting institutional integrity.
ORG/GOV/002 Risk Management Policy	• Duty to manage the affairs of the CIO (Clause 9(1)).	• Charity Commission Guidance (CC26)	Establishes a systematic framework for identifying, evaluating, and mitigating strategic and operational risks. It mitigates the risk of

			strategic failure by embedding proactive risk management into the Board's decision-making.
ORG/GOV/003 Campaigning and Political Activity Policy	• Duty to ensure campaigning furthers charitable objects (Clause 3). • Duty to act in the charity's best interests (Clause 9).	• Charity Commission Guidance (CC9)	Provides a framework to ensure any campaigning is legally compliant and mission-focused. It mitigates the significant legal and reputational risk of engaging in prohibited party-political activity.
ORG/GOV/004 Complaints Handling Policy	• Duty to manage the CIO's affairs accountably (Clause 9(1)).	• Charity Commission Guidance • The Equality Act 2010	Provides a fair, clear, and accessible procedure for handling general complaints. It mitigates reputational risk by ensuring dissatisfaction is handled constructively and provides an opportunity for organisational learning.
ORG/GOV/005 Fundraising Policy	• Duty to manage the CIO's affairs (Clause 9(1)). • Powers which allow for fundraising activities (Clause 4).	• The Charities Act 2011 • Charity Commission Guidance (CC20)	Ensures all fundraising is conducted in a legal, open, and honest manner. It mitigates reputational risk from inappropriate fundraising tactics and protects potentially vulnerable donors from undue pressure.
ORG/GOV/006 Insurance Requirement Policy	• Power to purchase Trustee Indemnity Insurance (Clause 5(1)(b)). • Duty to protect the charity and its trustees (Clause 9).	• The Charities Act 2011 (Section 189) • Charity Commission Guidance (CC49)	Ensures that adequate insurance is maintained to cover key risks. It mitigates the financial risk of significant loss from unforeseen events and protects trustees from personal liability where they have acted honestly and reasonably.

ORG/GOV/007 Whistleblowing Policy	• Duty to protect the charity's assets and reputation (Clause 9).	• Public Interest Disclosure Act 1998 • Charity Commission Guidance	Provides a safe and confidential mechanism for individuals to raise serious concerns about wrongdoing. It mitigates the risk of malpractice (e.g., fraud, safeguarding failures) going undetected by fostering a culture of integrity.
ORG/GOV/008 Code of Conduct	• Duty regarding the functions and duties of charity trustees (Clause 9). • Rules regarding retirement and removal of trustees (Clause 12).	• The Charities Act 2011 • Charity Commission Guidance	Establishes unambiguous standards of behaviour for trustees and appointed persons. It mitigates the reputational risk associated with poor conduct by individuals representing the charity.
ORG/GOV/010 Honorific Appointments Policy	• Power to create non-voting associate membership (Clause 17). • Duty to manage conflicts of interest for appointees (Clause 7). • Rule regarding the specific dispute resolution role for the Hon. Life President (Clause 27).	• The Charities Act 2011 • The Equality Act 2010	Provides a transparent framework for non-governance roles. It mitigates the governance risk of blurring the lines between voting trustees and non-voting appointees, ensuring the CIO's legal structure and accountability are protected.
ORG/HR/001 Family Friendly Policy	• Power to employ staff (Clause 4(4)).	• The Employment Rights Act 1996 • The Equality Act 2010	Provides a compliant framework for managing family-related leave (e.g., maternity, paternity, adoption). It mitigates the legal risk of failing to provide statutory leave and pay entitlements to future employees.
ORG/HR/002 Flexible Working Policy	• Power to employ staff (Clause 4(4)).	• The Employment Rights Act 1996• The Equality Act 2010	Provides a fair and consistent framework for managing flexible working requests. It mitigates legal risks related to statutory

			requests and supports staff retention, well-being, and inclusive employment practices.
ORG/HR/003 Health and Safety Policy	• Duty of care to increase wellbeing (Clause 3). • Duty to manage the CIO's affairs (Clause 9(1)).	• Health and Safety at Work etc. Act 1974 • The Equality Act 2010	Provides a framework to protect all people associated with the charity from harm. It mitigates the risk of injury, ill health, and legal liability from unsafe activities, premises, or events.
ORG/HR/004 Workplace Pension Scheme Policy	• Power to employ and remunerate staff (Clause 4(4)).	• The Pensions Act 2008	Ensures compliance with statutory auto-enrolment duties for any future employees. It mitigates the significant legal and financial risks of failing to meet the charity's obligations as an employer.
ORG/HR/005 Written Statement of Principal Terms and Conditions of Employment Policy	• Power to employ and remunerate staff (Clause 4(4)).	• The Employment Rights Act 1996	Ensures the charity is prepared to meet its legal obligations as an employer from day one of employment. It mitigates the legal risk of non-compliance with the statutory requirement to provide a written statement of terms.
ORG/HR/006 Disciplinary and Grievance Policy	• Power to employ and manage staff (Clause 4(4)).	• The Employment Act 2008 • The ACAS Code of Practice	Provides a fair and legally compliant framework for managing staff relations. It mitigates the legal risk of unfair dismissal claims and helps to maintain a positive and productive operational environment.

ORG/HR/007 Sickness Absence Policy	• Power to employ and manage staff (Clause 4(4)).	• Statutory Sick Pay (SSP) regulations • Employment Rights Act 1996 • The Equality Act 2010	Provides a supportive and legally compliant framework for managing sickness absence. It mitigates legal risks related to SSP and disability discrimination while ensuring operational continuity is considered.
ORG/HR/010 Time Off for Dependants Policy	• Power to employ staff (Clause 4(4)).	• The Employment Rights Act 1996	Ensures compliance with the statutory right for employees to take reasonable unpaid time off for unforeseen emergencies involving a dependant. It mitigates the legal risk of unlawfully refusing such requests.
ORG/HR/011 Equal Opportunities and Diversity Policy	• Duty regarding the object to enhance social inclusion (Clause 3(1)). • Rule regarding diversity in trustee recruitment (Clause 10(2)).	• The Equality Act 2010	Provides a framework to ensure fair, accessible, and inclusive operations. It mitigates the legal and reputational risk of discrimination in service delivery, governance, and any future employment practices.
ORG/HR/012 Safeguarding Vulnerable People Policy	• Duty of care to the Beneficiary Community (Clause 3).	• The Care Act 2014 • The Charities Act 2011 • Charity Commission Guidance	Provides the core framework for protecting vulnerable adults from harm, abuse, and neglect. It mitigates the profound legal, reputational, and ethical risks associated with any failure in the charity's duty of care.
ORG/HR/013 Pay and Remuneration Policy	• Power to remunerate staff (Clause 4(4)). • Duty to manage funds prudently (Clause 9).	• National Minimum Wage regulations • The Equality Act 2010	Ensures that any pay decisions for future staff are fair, defensible, and in the charity's best interests. It mitigates the legal risk of unequal

			pay claims and the financial risk of paying excessive or un-benchmarked salaries.
ORG/HR/014 Employee Privacy Notice	• Power to employ staff (Clause 4(4)).	• UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018	Fulfils the legal duty of transparency towards employees regarding their personal data. It mitigates the risk of non-compliant data processing within the employment relationship.
ORG/HR/015 Unpaid Parental Leave Policy	• Power to employ staff (Clause 4(4)).	• The Employment Rights Act 1996	Provides a compliant framework for managing unpaid parental leave. It mitigates the legal risk of failing to provide this statutory entitlement to eligible employees.