

Policy Name	Data Protection Policy			Strategic Strand: Commitment 1: Principled decision-making	
Policy Ref	DIR/POL/018	Owner	Director of Governance and Business Transformation		
Review cycle	Every THREE years	Responsibility	GNRC	Version:	6, Q2 2025
Policy Statement	MAG takes information security very seriously and protecting our information and IT systems is a key component of building and maintaining trust. The consequences of not securing information could expose the organisation and our brand to significant legal and regulatory censure, sanctions and fines. Personal information is legally protected and requires specific attention. Our regulators expect us to comply with best industry practice when securing all types of information.				
Scope and limitation	This Policy applies to all MAG personnel and associates (trustees, international, national and HQ employees and consultants, organisations working in partnership with MAG).				
Implementation	In our role as a charity and an employer, MAG takes data protection very seriously, whether the Personal Data relates to our donors, suppliers, contractors, business associates or current, past, or prospective MAG personnel. MAG personnel and all third parties Processing Personal Data for us or on our behalf to comply with these data protection principles: • Lawfulness, Fairness, and Transparency • Purpose Limitation • Accuracy • Security and Confidentiality • Data Subject Rights				
Reporting concerns	MAG personnel and associates shall report immediately any suspicion of breach of data protection to DataProtectionTeam@maginternational.org				
Data Protection Governance	MAG’s are responsible for implementing and maintaining a data privacy management programme to ensure the Processing of Personal Data meets the requirements outlined in MAG’s Data Protection Procedures.				
Non-Compliance	Failure to comply with this policy will not only put MAG’s data protection compliance at risk, but could have disciplinary consequences for any MAG employees, associates or contractors found to be in breach, including adverse risk metrics and/or investigation and disciplinary action pursuant to the MAG Disciplinary Procedure, up to and including dismissal. In addition, breaches of Data Protection Laws can give rise to criminal and/or civil liability for the individuals concerned.				
Glossary of terms	Personal Data – means any information from which, alone or together with other information, an Individual can be identified. Personal Data can be factual, such as names, identification numbers, location information, and one or more identifiers such as IP addresses or cookies. Personal Data can also be an opinion about an Individual’s actions or behaviour, or related to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of an Individual. Personal Data includes ‘Sensitive Personal Data’. Processing or Process – means any activity, operation or set of operations that is performed on Personal Data, including collecting, holding, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making available, aligning, combining, restricting, erasing or destroying. Sensitive Personal Data – means Personal Data that relates to an Individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation, as well as criminal offences or convictions. Sensitive Personal Data is referred to as Special Categories of Personal Data in the EU General Data Protection Regulation.				
Ethics, Values and Mission	Integrity: MAG takes information security very seriously and protecting our information and IT systems is a key component of building and maintaining trust. The consequences of not securing information could expose the organisation and our brand to significant legal and regulatory censure, sanctions and fines. Personal information is legally protected and requires specific attention. Our regulators expect us to comply with best industry practice when securing all types of information.				
Delegations of Authority	The responsible member of the Leadership Team is the Director of Governance and Business Transformation.				
Mandatory Reporting	All investigations of Data Breaches will be reported to MAG’s Governance Nominations Committee and if contract, regulation or law requires, to donors, the UK Charity Commission, the UK Information Commissioners Office and relevant local authorities.				
Risk management	Risks are managed through the MAG Risk Framework.				
Legislation and codes of conduct	• The EU General Data Protection Regulation 2016/679 (‘GDPR’), the UK Data Protection Act 2018 • All data protection laws relevant to MAG’s donor countries and countries of operation • MAG Code of Conduct / Policy on Personal Conduct • IT policy • MAG Data Protection Procedures and guidance documents				

ENDS