Policy

Data Governance Policy

POLY-101779

1. Purpose

This policy outlines the roles, responsibilities and organizational structures pertaining to the governance of all NSW Health Pathology (NSWHP) Data Assets. Effective data governance builds organisational capital, strengthens governance structures and ensures NSWHP data is managed, used and protected in line with legal and policy requirements, community expectations and the 'Five Safes' risk management model for managing data sharing risks. This policy facilitates the accessibility and availability of data assets, information security, and the standardisation of data governance principals.

2. Scope

This Policy is intended to be consistent with the the NSW Health Data Governance Framework GL2019_002 (**GL2019_002**). As such, terms used in this Policy are adopted from GL2019_002 unless otherwise specified. GL2019_002 governs only statewide data assets (data sets) that are mandated either by law or a policy recognised by NSW Health. This Policy applies to all other NSWHP data assets irrespective of their abstraction, representation, temporality, medium, usage, and intended purpose.

This Policy is subject to compliance with all relevant laws, regulations and policies. A list of the most relevant references is provided in Section 6.

Delegate roles specified in this Policy are also subject to the NSWHP Delegations Manual and NSW Health Combined Delegations Manual.

3. Definitions

- **Data Asset:** Any collection of data or information (medical or otherwise) that is held within NSWHP, that is captured in either paper or electronic format and may comprise one or more Information Assets.
- **Delegate:** A NSWHP staff member with delegated authority and responsibilities as a Data Sponsor, Data Custodian or Data Steward under this Policy.
- **Domain:** A specialized area of practice (department or discipline) that sits within a portfolio and is defined by highly specialised needs and expertise. (e.g. oncology, genomics, microbiology which all sit within the clinical operations portfolio).
- **Information Asset:** A discrete collection of data or information, stored in any manner, which is recognised as having value and is required to be managed by the organisation (refer to Information security policy)
- **ISWG:** Information Security Working Group - manages matters regarding the ISMS and advises the Data and Technology Committee.
- **ISMS**: Information security management system.
- **Dissemination limiting marker:** A protective marker that indicates access to the information should be restricted.

Approver: James Patterson, Version Number: 1.0, Publication Date: 27/02/2026

Policy

Data Governance Policy

POLY-101779

4. Policy Statement

Data are a critical asset to our organisation, customers, and stakeholders. To ensure that the appropriate stakeholders are informed, empowered and accountable for the decisions on the management and use of our data, a data governance framework is required. This Policy clearly identifies the roles and responsibilities associated with information decision management within NSWHP and defines the scope of their decision-making authority. A delegate is assigned to each role by the associated parent role in the Information Governance Hierarchy, beginning with the Chief Executive.

4.1 Principles

The role of a Delegate is to make decisions about information within the scope of their authority. This includes:

- Information classification, appropriate dissemination limiting markers, security classifications and associated considerations.
- Relevant units and terminology standards, their development process and operational tools, registers and capabilities.
- The required review and approval processes for the creation and storage, dissemination and use, retention and disposal of information within the scope of the authority.
- Identification and verification of potential hazards, likelihoods and consequences of managing information.
- Identification, verification, resourcing and implementation of appropriate controls for potential hazards.
- Acceptance, ownership and management of residual risk within the organisation's enterprise risk management framework.
- Assessment of the effectiveness of controls and determination of residual risk.

In addition, as described in GL2019_002 NSW Health Data Governance Framework, it is the responsibility of all data users to:

- Ensure that data is recorded or collected according to data standards
- Report data errors and quality issues in a timely manner
- Ensure data security and privacy are maintained whenever data is accessed
- Ensure login details are kept confidential and are only used by the designated user
- Report any breach or suspected breach of data security or privacy in compliance with NSWHP's Data Breach Response Plan.
- Sign an acknowledgement of their obligations to protect data privacy
- Ensure compliance with all relevant legislation, policies and standards, including
- the NSW Health Code of Conduct
- Obtain approval from Data Sponsor or delegated authority for public release of data

Approver: James Patterson, Version Number: 1.0, Publication Date: 27/02/2026

- Abide by all terms and conditions associated with approval for access to data.

4.2 Governance hierarchy

This Policy specifies the data governance hierarchy and the roles and responsibilities to be delegated. While local, domain and enterprise-level Delegates will be empowered to make data governance decisions within their delegation, their actions will be transparent, and visible to higher-level Delegates.

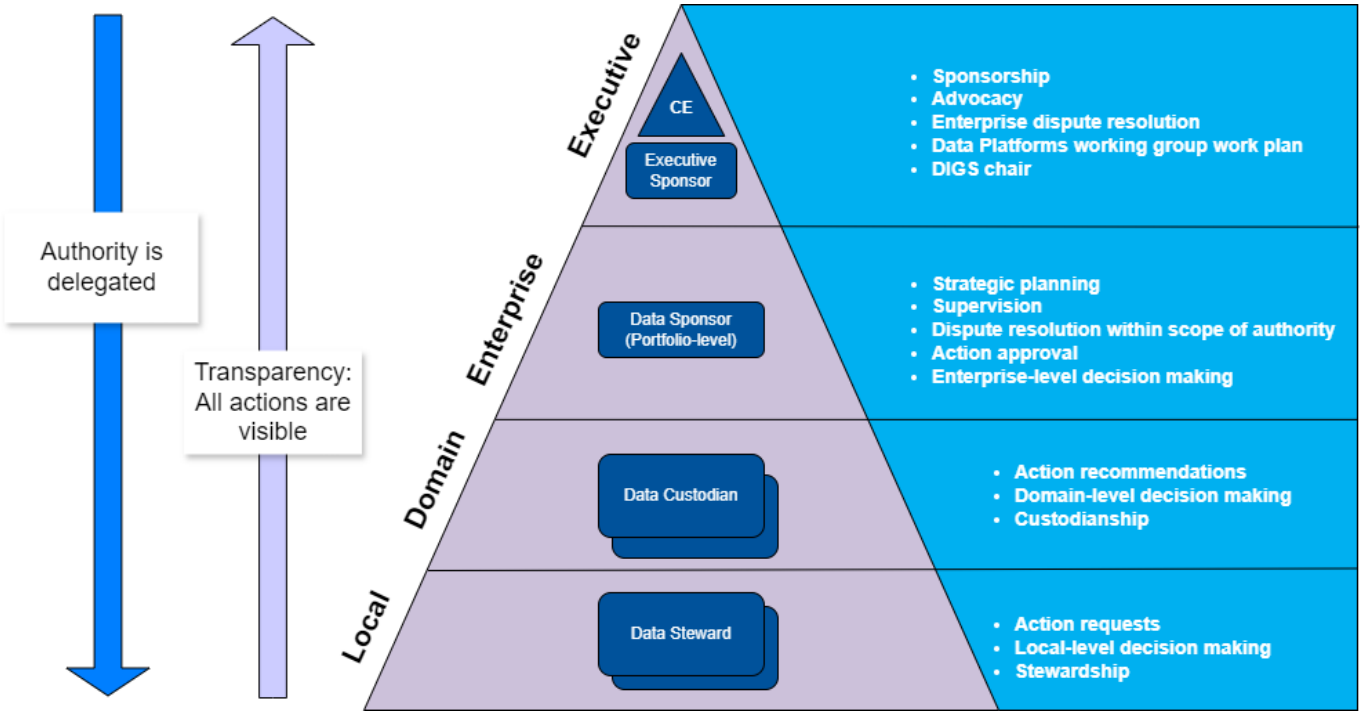


Figure 1. Data governance hierarchy and associated responsibilities.

5. Roles and Responsibilities

We adopt role definitions found in the NSW Health Data Governance Framework. Based on their role, each Delegate will be tagged as either responsible (R), accountable (A), consulted (C) or informed (I) per each activity (RACI matrix) as follows;

Executive Sponsor.

The chief executive, as the level 1 role delegate per the NSW Health Data governance framework, owns ultimate responsibility and decision-making authority over organisational data assets. The chief executive has delegated data governance responsibility to the Chief Medical Information Officer, who is aligned to the Level 2 role specified in the NSW Health Data Governance Framework, and is responsible for:

- Sponsorship:

- Ensuring that appropriate resourcing is available to support the management, use, security of and access to enterprise-wide data assets or risks that are unable to be effectively mitigated at the Sponsor level (A).
- Establishment, mandate, resourcing, and support of a Data Platform Working Group to inform data governance, security and associated best practices (A).

- Advocacy: Providing vocal support of decision-making process / decisions pursuant to the policy to stakeholder groups both inside and outside of the organisation (A).
- Risk Management: managing risks that cannot be mitigated at a lower level of the governance hierarchy (A)
- Incident Management: ensure appropriate procedures and resources are available for incident response (A)
- Audit and Compliance: being aware of any breach associated with audit log review (I)
- Dispute Resolution / Action Approval
  - Where there is more than one Sponsor involved in a decision within their scope of authority and unable to reach consensus, facilitate consensus and determine the matter if consensus cannot be reached (A)
  - Endorsing and resourcing actions / action plans developed by Sponsors within their scope of authority (A)
- Leadership:
  - Driving overall strategy and pathway for the enterprise (A).
  - Remain informed of activities conducted by all delegates under their jurisdiction (I)
  - Appointment of Sponsors (A/R)

This role will be supported by two advisory committees:

a. Data and Technology Committee: established by the Chief Executive of their nominated delegate to provide oversight and strategic direction in relation to data, information and technology infrastructure management in NSWHP.
b. Data Platform Working Group: a technical working group appointed by the Executive Sponsor or their delegate who, at the direction of the Executive Sponsor, will develop enterprise level patterns, practices, platforms and solutions that uplift the enterprise's data governance capabilities and posture. This group will consist of, or have access to subject matter experts on information security, infrastructure, data quality, analytics & legal. They will facilitate enterprise-level decision making to ensure appropriate technical governance (e.g. appropriate standards for encryption and cryptography) focused on the fair, equitable and effective use of data assets. The group deliverables will be submitted to the Information Security Working Group for consultation and endorsement.

Policy

Data Governance Policy

POLY-101779

Data Sponsor:

The Data Sponsor is a senior leader who is responsible for a given portfolio (e.g. clinical operations, finance, workforce etc.). This is aligned to the Data Sponsor in the NSW Health Data Governance Framework. They are responsible for the control of strategic direction and undertaking duties that includes:

- Sponsorship.
    - Ensuring appropriate resourcing is available to support the curation, use and management of data assets falling under their jurisdiction (R).
    - Identify domains within their portfolios and appoint Data Custodians for each (A/R).
    - Providing oversight of relevant work packages and ensuring they receive adequate support to proceed to plan (R).
- Risk management: managing risks that cannot be mitigated at a lower level of the governance hierarchy (R)
- Dispute Resolution / Action Approval:
    - When consensus cannot be reached between Data Custodians within their scope of authority, facilitating consensus and ultimately making the decision if consensus cannot be reached (R).
    - Endorsing and resourcing actions / action plans developed by Data Custodians within their scope of authority (R).
    - Endorsing decisions made by the relevant Data Custodians once they adequately address any relevant concerns within the context of the entire enterprise (A).
- Leadership:
    - Driving overall strategy and pathway for the portfolio (R)
    - Appointment of Data Custodians (A/R)
    - Ensure data and information is correctly categorised and labelled in accordance with information handling guidelines (A)
    - Incident Management: ensure appropriate procedures and resources are available for incident response (C)
    - Audit and compliance: ensuring data access and manipulation auditing requirements and processes within the scope of custodianship are implemented and regularly reviewed (A)

Data Custodian:

This role aligns with the Data Custodian of the NSW Health Data Governance Framework.

Policy

Data Governance Policy

POLY-101779

Certain portfolios may be diverse and consist of multiple domains that require specialised understanding and administration. Data Custodians are responsible for the day-to-day management and oversight of Data Assets within their specialised area (or domain) which is defined as their scope of custodianship, and the overall quality and security of the Data Assets within that scope.

Each domain must be overseen by a Data Custodian which consists of subject matter experts with deep understanding of each domain, as well as experts in data science, analytics, Information and Communications Technology (ICT), legal and security.

A Data Custodian must report up to a single Data Sponsor. A Data Sponsor may be responsible for multiple Data Custodians.

A Data Custodian's accountabilities are:

- Funding. Responsibility for appropriate resourcing to support the curation, use and management of data assets falling under their jurisdiction (R).
- Sponsorship. Providing oversight of deliverables and ensuring that they receive adequate support to proceed to plan (R).
- Risk assessment and management. Reviewing and where necessary assessing and potentially identifying information management risk within their scope of authority (R).
- Ensure data and information is correctly categorised and labelled in accordance with information handling guidelines (R)
- Access control: ensuring appropriate requirements and processes are in place to govern access to data within the scope of custodianship (A)
- Audit and compliance: ensuring data access and manipulation auditing requirements and processes within the scope of custodianship are documented and implemented (R)
- Human resource security: onboarding and offboarding procedures for data access, staff education on security policies and best practices, monitoring and management of insider threats. (R)
- Managing and coordinating execution of strategic planning elements and actions within their scope of authority in conjunction with Data Custodian (R)
- Domain-Level Decision Making:
    - Reviewing content within their scope of authority and approving for Data Sponsor inclusion and endorsement (R).
    - Collaborating with Data Platform Working Group to ensure requirements are understood and where appropriate, adequately addressed (R).
    - Resolves disputes pertaining to access and use of data assets (R).

Approver: James Patterson, Version Number: 1.0, Publication Date: 27/02/2026

  - Determining cradle to grave lifecycle processes and procedures for data within their custodianship (R).
  - Determining appropriate processes for system change management that could impact data management within their scope of custodianship (C)
  - Approves incident response processes and procedures involving data within the scope of custodianship (C)

- Leadership:
  - Driving overall strategy and pathway for their domain (R)
  - Appointment of Data Stewards and vesting responsibility of key activities and assets (R)

Data Steward:

This role aligns with the Data Steward from the NSW Health Data Governance Framework.

Data Stewards are responsible for the day-to-day management and oversight of assets that fall under their purview, as well as their overall completeness and quality. They perform these tasks under the direction of the Executive Sponsor, Data Sponsors and Data Custodians associated with the Data Assets they are providing stewardship of. The Data Steward is responsible for:

- Action Requests: coordinating resources to assess and action requests at a local operational / tactical level (C/I)
- Risk assessment and management. Assessing information management risk within their scope of authority (R).
- Local-Level Decision Making: making day to day decisions on information management (R)
- Ensuring that information management policies, procedures and practices required by the Executive Sponsor, Data Sponsors or Data Custodians, legal or policy requirements or senior authorities (sponsors or custodians) are adhered to on a day-to-day basis within their scope of responsibility (e.g. within a laboratory, a project team, department etc.) (R)
- Ensure up-to-date centralised documentation including a data dictionary, metadata, and management information including the purpose, supply, storage and retention strategy, and quality of data assets in conjunction with the direction set out by the Data Platform Working Group (R).
- Audit and compliance: ensuring data access and manipulation auditing requirements are implemented (R)

Escalations and consultations:

Policy

Data Governance Policy

POLY-101779

In addition, each nominated individual is responsible for the following communications to their respective Custodians / Sponsors / Executive directly above in the governance hierarchy.

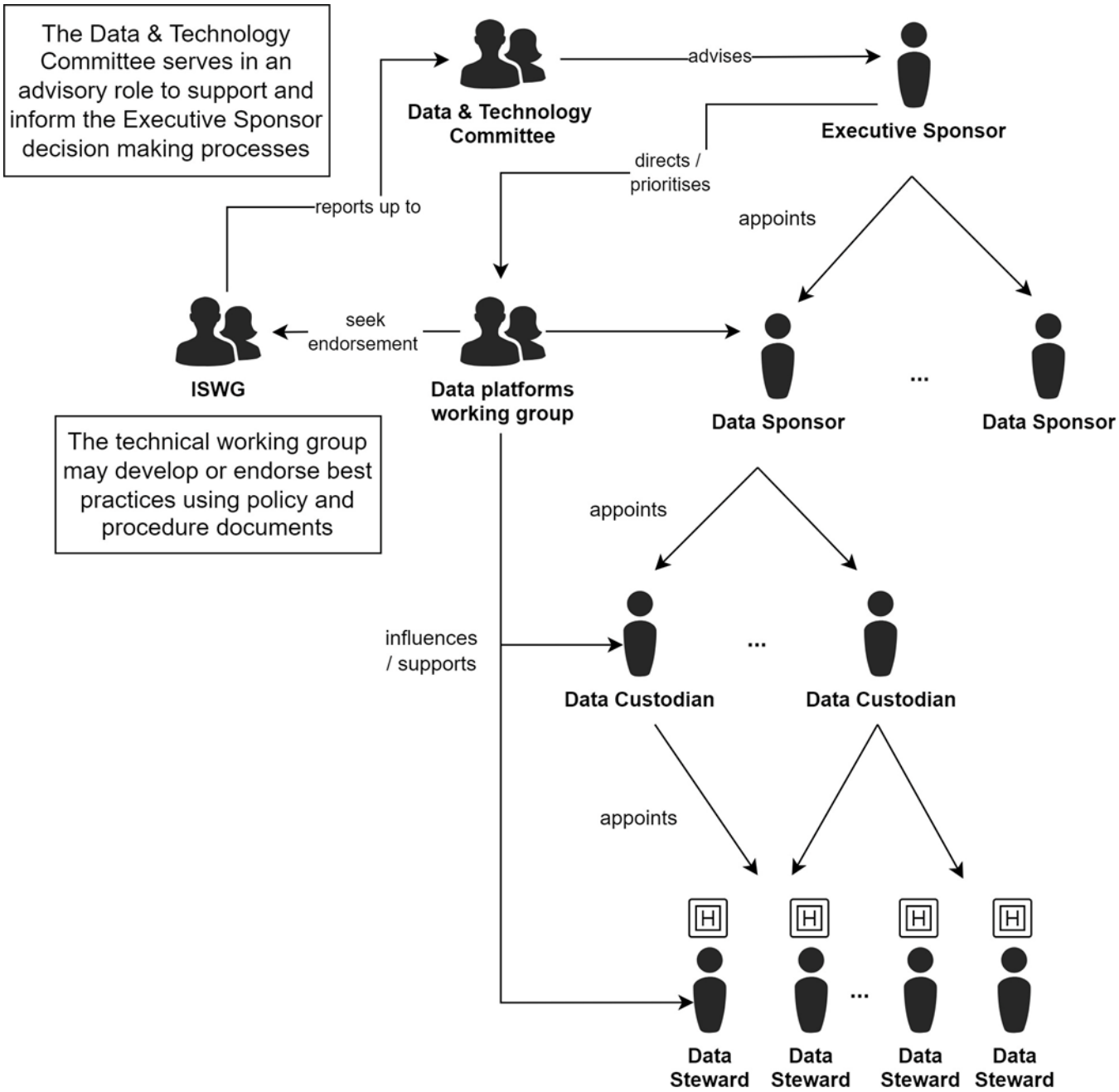
- Escalate risks, issues and conflicts (R)
- Escalate resourcing requests (R)
- Provide advice on the governance, use and future strategy for the data asset (A)

Figure 2 presents an abbreviated view of interactions between the Executive Sponsor, Data Sponsors, Data Custodians, Data Stewards.

Policy

Data Governance Policy

POLY-101779



Approver: James Patterson, Version Number: 1.0, Publication Date: 27/02/2026

5.4 Disclosure

Any disclosure of data must be compliant with the Privacy Principles and Health Privacy Principle outlined in the Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW) and within delegation. NSWHP Delegations Manual and NSW combined delegations provides details of delegations. Further, there must be a legal basis for disclosure of unit record data. If there is uncertainty as to the legal basis, legal advice can be sought from the Corporate Governance team.

5.5 Non-compliance

Breaches of and departures from this Policy will be addressed in accordance with the NSWHP Compliance Management Framework, including but not limited to:

- Reporting and remediation of the breach or departure; and
- Commitment to ensuring that such or similar breaches or departures are not repeated.

6. Related Procedure Document Suite

- NSWHP_PD_033 NSW Health Pathology Information Security Policy
- PD2020_046 NSW Health Electronic Information Security Policy
- GL2019_002 NSW Health Data Governance Framework
- NSWHP CG_011 Information Security Management System
- NSWHP_PD_028 Records Management Policy
- NSWHP_CG_010 Compliance Management Framework
- NSWHP_PR_076 Research Data Management Procedure
- NSWHP_PR_104 NSW Health Pathology Data Breach Response Plan

7. Related Legislation and Supporting Documents

- NSW Government Information Classification, Labelling and Handling Guidelines
- NSW government data strategy
- NSW government data and information custodianship policy
- NSW government information management framework
- Australian National Data Service (ANDS) De-identification Guide
- Commonwealth Scientific and Industrial Research Organisation (CSIRO) The De-identification Decision-Making Framework
- Health Administration Act 1982 No 135 (NSW)
- Health Administration Regulation 2020 (NSW)
- Health Records and Information Act (2002) (HRIP) (NSW)

- Information and Privacy Commission NSW (IPC) Fact Sheet: De-identification of personal information
- Information and Privacy Commission NSW (IPC) Health Records and Information Act (2002) (HRIP) (NSW)
- NHMRC Australian Code for the Responsible Conduct of Research 2018
- NHMRC Management of data and information in research
- NHMRC National Statement on Ethical Conduct of Human Research
- NSW Government Cyber Security Policy Version 4.0 March 2021
- NSW Health Code of Conduct (PD2015_049)
- NSW Health Communications - Use & Management of Misuse of NSW Health Communications Systems (PD2009_076)
- NSW Health Data Collections - Disclosure of Unit Record Data for Research or Management of Health Services (PD2015_037)
- NSW Health Electronic Information Security Policy (PD2020 _046)
- NSW Health Privacy Manual for Health Information
- NSW Health Research - Authorisation to Commence Human Research in NSW Public Health Organisations (PD2010_056)
- NSW Health Research Governance in NSW Public Health Organisations (GL_2011_001)
- Public Health Act 2010 (NSW)
- Privacy and Personal Information Protection Act 1998 (NSW)
- State Records Authority (NSW) Health Services, Public: Patient/Client records (GDA17) Section 8.0.0 'Research Management'
- State Records Act 1998
- Therapeutic Goods Administration Note for Guidance on Good Clinical Practice (CPMP/ICH/135/95)

8. Review

This Policy will be reviewed annually. The next review will be completed by DD/MM/YYYY

9. Risk

Risk Statement	Compliance with this Policy will ensure that NSW Health Pathology administers and utilises its data assets in a safe and secure manner in line with institutional and legislative requirements.
Risk Category	Leadership and Management

Policy

Data Governance Policy

POLY-101779

10. Further Information

For further information, please contact:

Policy Contact Officer	Position: Manager, Data & insights
	Name: Suranga Kasturi
	Email: suranga.kasturi@health.nsw.gov.au

11. Version History

The approval and amendment history for this document must be listed in the following table.

Version No	Effective Date	Approved By	Approval Date	Procedure Author	Risk Rating	Sections Modified
1.0	15/01/2026	SLT	15/01/2026	Manager, Data & insights	High	New Policy

Approver: James Patterson, Version Number: 1.0, Publication Date: 27/02/2026

Policy

Data Governance Policy

POLY-101779

12. Appendix

12.1RACI Matrix

Responsible (R), Accountable (A), Consulted (C), Informed (I)

	CE / Executive Sponsor	Data Sponsor	Data Custodian	Data Steward	Data and Technology Committee	Data Platform Working Group
Sponsorship	A	R	R	I	C	C
Advocacy	A	R	R	R	R	R
Dispute Resolution	A	R	C	I	C	C
Strategy and Direction	A	R	R	I	C	C
Appointment of Sponsors	A/R	I	I	I	I	I
Appointment of Data Custodians	I	A / R	I	I	I	I
Appointment of Data Stewards	I	I	A/R	I	I	C
Appointment of Data platform working group	A / R	C	I	I	C	C
Appointment of Data and Technology Committee	A/R	C	I	I	I	I
Endorsing and Resourcing Action Plans	A	R	C	C/I	C/I	C/I
Resourcing and Support	A	R	I	I	C	C

Approver: James Patterson, Version Number: 1.0, Publication Date: 27/02/2026

Policy

Data Governance Policy

POLY-101779

	CE / Executive Sponsor	Data Sponsor	Data Custodian	Data Steward	Data and Technology Committee	Data Platform Working Group
Human resource security	A	R	R	R	C	C
Access Control Management	I	I	A	R	I	C
Lifecycle Management	I	C	A/R	C	I	C
System Change Management	I	I	C	A/R	I	C
Enterprise-wide decision making	A/R	C	I	I	C	C
Information Classification and Labelling	I	A	R	I	I	I
Risk Management	A	R	R	R	C	C
Incident Management	A	C	C	R	C	R/C
Audit and compliance	I	A	R	R	C	C

Approver: James Patterson, Version Number: 1.0, Publication Date: 27/02/2026