GRIFFITH UNIVERSITY

Local Protocol

Griffith Data Trust – Data Governance and Management Protocol

1.0 Purpose

This Local Protocol sets out the processes applicable to the governance and management of data handled by the Griffith Data Trust, including those applicable to its role as an Accredited Data User and Data Service Provider under the *Data Availability and Transparency Act* (Cth) (DAT Act).

2.0 Scope

This Local Protocol applies to the Griffith Data Trust when handling data obtained from data providers, including data under the DAT Act.

This Local Protocol applies subject to any requirements of a Data Sharing Agreement, which will prevail over this document.

3.0 Local Protocols

3.1 Data governance

3.1.1 Governance Body

The Griffith Data Trust Committee is the governance body responsible for overseeing data governance, data management, and security governance practices and procedures. This oversight encompasses physical, ICT, and data security, alongside monitoring risks linked with research projects, and ensuring non-compliant projects are discontinued.

3.1.2 Data Governance and Security Roles

3.1.2.1 Director of the Griffith Data Trust

- Responsible for data governance and management, as well as security governance.
- Acts as a security risk owner, overseeing the identification and mitigation of security risks.
- Ensures the governance and management of personal information, ensuring compliance with relevant laws and standards.

3.1.2.2 Lab Coordinator of the Griffith Data Trust

- Acts as a security steward, assisting in implementing and maintaining security protocols and practices.

3.1.2.3 Policy and Compliance Coordinator of the Griffith Data Trust

- Responsible for managing security risks, ensuring that security measures are aligned with regulatory requirements and best practices.
- Ensures adherence to relevant laws, regulations, and standards, including the 'DATA Scheme'.
- Develops and updates data governance policies and procedures, and monitors compliance, reporting issues to the Griffith Data Trust Committee.

3.1.3 Subject Matter Expertise

As members of the Griffith Data Trust Committee, the Director of Cybersecurity and the Policy and Compliance Coordinator serve as subject matter experts, providing guidance and recommendations to support data oversight and management. Their contributions may include:

- Risk assessment and management: provide insights into potential threats and vulnerabilities and recommend appropriate measures to mitigate these risks affectively.
- Research project approvals: Assess the data management and security aspects of proposed research projects, ensuring they meet the Griffith Data Trust's standards and comply with regulatory requirements.
- Compliance oversight: providing guidance on complying with relevant laws, regulations and standards governing data management and privacy, including those outlined in the 'DATA Scheme'.

3.1.4 University security oversight

- The University Executive Group, through the Vice President (Industry and External Engagement) oversees Griffith Data Trust's governance, security, and compliance, based on the Annual Report from the Director of the Griffith Data Trust.

3.2 Data Strategy

The data strategy includes:

- Creating a roadmap for data utilisation, defining research objectives, and outlining the data lifecycle.
- Establishing and periodically reviewing data quality standards to ensure the accuracy, completeness, and reliability of research data.
- Aligning data initiatives with the Griffith Data Trust's research priorities, considering ethical implications, and promoting collaboration among researchers and data custodians.
- Promoting a data-driven research culture by providing researchers with diverse datasets, analytical tools, and expertise to address societal challenges and guide evidence-based policy decisions.

The data governance framework for the Griffith Data Trust is comprised of the University's Information Governance and Management Framework and Information Management Policy.

3.3 Data Identification and Management

Griffith Data Trust uses specific processes to identify, manage, and track its data assets. These processes help monitor and report on data governance, data management and usage.

3.3.1 Data inventory

The process for inventory management of datasets are as follows:

- Dataset identification: work with data providers to identify datasets requiring housing within The Facility.
- Centralised data inventory: datasets are catalogued and classified based on their sensitivity and usage requirements. Metadata fields including dataset name, description, source, and security classification level are recorded in a centralised data inventory spreadsheet.
- Regular audits: conduct regular audits of the dataset inventory to ensure compliance with security policies and regulations. This includes verifying access permissions, monitoring usage patterns, and identifying any anomalies or unauthorised access attempts.

3.3.2 Data value

Dataset value is determined by several factors, including but not limited to categorising data based on its alignment with Griffith's strategic goals, sensitivity levels, the reputational, financial, and legal impacts of data breaches, and costs associated with protecting the data.

The Griffith Data Trust will continuously monitor data quality, if a datasets value diminishes or security risks arise, steps are taken to update or enhance its protection.

3.3.3 Data classification

Adhere to Griffith's Information Security Classifications Procedure, to ensure data is assessed, identified, and labelled with an appropriate information security classification corresponding with the data's value and risk.

3.3.3 Data Management Practices

Follow standards of the data providing party and the Australian Government Recordkeeping Metadata Standards (AGRkMS) where possible. Additional standards for managing data may be applied to DATA scheme data as requested by the data custodian or data sharing agreement.

For some datasets that arise from fields with specific standards such as HL7 for health datasets, the metadata standards for these fields will be used.

3.3.4 Monitoring and Reporting

Griffith Data Trust Director will regularly report on data management to the Griffith Data Trust Committee and annually to the University Executive Group.

3.4 Data transfer requirements

Prior to the transfer of data to Griffith University, Griffith Data Trust requires:

- Data sharing agreement(s) to be signed and agreed upon by all parties and a data extraction policy form from the data provider.
- Ethics review on the onboarded data.
- Privacy Impact Assessment (if required) by the data providing agency before data transfer to Griffith University.

3.4.1 Preferred data transfer method

Grifith Data Trust's preferred method is through a securely encrypted USB drive. Other methods require approval from the Director of the Griffith Data Trust. This method will be used for all data obtained under the DAT Act. The method entails:

- A USB drive with a hardware keylock is prepared by cleaning and creating a new keycode (this is kept separate).
- The data provider encrypts one or multiple files containing data and metadata, keeping the key separate. The encrypted files are copied to the secure USB drive and provided to Griffith Data Trust.
- Once the Griffith Data Trust informs the data provider that the data is in the facility, the hardware keycode and software encryption key are provided.
- The data undergoes virus and malware checks. Once the cybersecurity verification is complete, the data and metadata are transferred to the secure data facility.
- The disk is wiped and physically destroyed.
- The data provider is notified that the data was successfully added to the facility and that the disk has been formatted and destroyed.

3.4.2 Secure Cloud Solutions

- Lab Coordinator downloads the data onto a clean machine.
- Using the clean machine, data is downloaded and transferred to a secure USB disk, and the process of the preferred data transfer method is followed as described in section 3.4.1.
- Once the data is in the secure data facility, the clean machine's disk is formatted and physically destroyed.
- Data provider is notified that the data was successfully added to the secure data facility and is instructed to remove data from the secure cloud environment.

3.5 Data linkage methods

Data linkage must be expressly authorised by the governing data sharing agreement. Before starting a research project with the Griffith Data Trust, the data linkage method will be agreed upon. This method will be determined based on the type and sensitivity of the data, and whether the data is classified as DATA scheme data. The preferred data linkage methods are outlined below:

3.5.1 Shared Attributes or Identifiers

- For linkage to occur, there must be common attributes or identifiers between the datasets. These could be direct identifiers like names or identification or indirect identifiers like date of birth or postcode.

3.5.2 Deterministic Linkage

- This involves matching records based on exact matches of identifiers. If two records have the exact same identifier value (e.g. Driver's License Number), they are linked.

3.5.3 Probabilistic Linkage

- This method considers multiple identifiers and assigns weights based on the likelihood of a match. It's useful when identifiers might not be exact due to errors or inconsistencies.

3.5.4 De-identification

- To maintain privacy, personal identifiers are removed or encrypted during the linkage process, unless otherwise not possible. This ensures that the merged dataset doesn't compromise the confidentiality of individuals.

3.5.5 Quality assurance

- Effective data linkage requires high data quality, as errors or mission values can reduce the accuracy of the linkage. Proper preprocessing, cleaning, and validation are essential components of the linkage process.

3.6 Data Extraction and Sanitisation procedure

- The sanitisation/data extraction procedure required to remove data from the facility or from the research zone to a teaching zone within the facility is:
    1. Users ensure data has been appropriately sanitised in accordance with the appropriate data extraction policy.
    2. Users submit ticket, requesting data extraction.
    3. Administrative staff check data to ensure it meets the appropriate data extraction policy.
    4. Administrative staff copy approved data to a removable drive.
    5. Administrative staff archive removed data to secure storage for historical evidence.
    6. Administrative staff close the ticket, logging the actions taken.
- If the data is provided under the DATA Scheme, extraction can only occur if expressly permitted in the Registered Data Sharing Agreement. Data extraction is subject to the Data sharing agreement with the Commonwealth entity allowing it. This ensures personal information is protected against loss and unauthorised access, use, modification, disclosure, and other misuse.
- Refer to the Data Extraction and Sanitisation Protocol for further details.

3.7 Ethical use of data

The Griffith Data Trust will uphold ethical data use by ensuring all datasets and research projects are reviewed and approved, and when required, obtain ethics approval from the Griffith University Human Research Ethics Committee.

3.8 Data Retention and Disposal

- Generally, data retention and disposal decisions will align with the maximum retention period as per specific requirements outlined in data sharing agreements by the data providers. The retention period specified in each data sharing agreement will be reviewed and followed appropriately.
- Data and datasets created as part of research activities will adhere to Griffith University's, 'Schedule of Retention Periods for Research Data and Primary Materials', recommended as the standard practice for data retention. This document aligns with the University Sector Retention and Disposal Schedule approved by Queensland State Archives.

3.9 Management of data risks

Griffith University policies and procedures are implemented to manage data risks. These include:

3.9.1 Risk management

The Griffith Data Trust adheres to Griffith's Risk and Resilience Management Framework, following the risk management process and self-controls assessment implemented across the university.

In aligning with the University, the Griffith Data Trust maintains a threat and risk matrix to ensure data risks are being managed.

3.9.2 Incident management

Griffith Data Trust complies with the University's Crises and Incident Response Plan, Resilience Standard, and Data Breach Response Plan. This includes data breach mitigation, disaster recovery, business continuity plans, crisis management and communication plan, and emergency response plan.

3.10 Management of privacy risks

Where the Griffith Data Trust will handle personal information, it must comply with the University's privacy statement. This includes complying with the following processes and procedures:

3.10.1 Privacy statement

Ensure information handling practices are consistent with the University privacy statement at Privacy Statement (griffith.edu.au).

3.10.2 Privacy impact assessments

Follow the process for determining if a privacy impact assessment (PIA) must be conducted for a particular research project or other new or different use of personal information. If a PIA is required, Griffith Data Trust must conduct a PIA in accordance with the University's procedures and implement any identified privacy controls.

3.10.3 Responding to privacy incidents

Follow the University's incident reporting procedure Reporting-a-Privacy-or-Data-Breach.docx.pdf (griffith.edu.au) and report immediately to privacyalert@griffith.edu.au.

3.11 Administration of this Local Protocol

3.11.1 Communication to staff

- New hires will receive training on Griffith Data Trust policies, including the protocol, during the onboarding process.
- Annual refresher sessions will update staff on any new developments or changes.
- All policies, including the Protocol, will be readily accessible in a centralised location.

3.11.2 Monitoring and enforcement

- Maintain detailed records of staff training sessions, including attendance and distributed materials.
- Signed acknowledgements from staff members confirming their understanding and compliance with the Protocol will be documented.
- Instances of non-compliance will be recorded, and appropriate actions will be taken.

3.11.3 Reporting

- Breaches of this Protocol are to be reported by the Griffith Data Trust Director to the Griffith Data Trust Committee.

4.0 Definitions

For the purposes of this policy and related policy documents, the following definitions apply:

Data quality refers to the overall utility of a dataset and its ability to be easily processed and analysed for other uses.

Data linkage the process of matching records from one dataset with those from another, based on shared attributes or identifiers, without necessarily revealing or compromising the identity or privacy of the entities within those datasets.

Data provider is an organisation that provides internal data assets to external parties.

Data sharing agreement is a contract that documents what data is being shared and how it can be used.

Direct identifiers these are unique to a person, enough to determine someone's identity.

Indirect identifiers indirect identifiers are not unique and include more general information. An indirect identifier allows information to be connected until an individual can be identifiable.

Information Security Classification is a process where the creator of information assesses the sensitivity and importance of the information and assigns a label to the information so that it can be managed or stored with consideration to its sensitivity and importance.

Metadata means data that provides context or additional information about a record or document.

Personal identifiers any information connected to a specific individual that can be used to uncover that individual's identity.

Privacy impact assessment (PIA) is a systematic assessment of a project that identifies potential privacy impact and recommendations to manage, minimise or eliminate them.

Quality assurance is part of quality management focused on providing confidence that quality requirements will be fulfilled.

5.0 Information

Title	Griffith Data Trust – Data governance and management
Document number	Provided by relevant Policy team
Purpose	This Local Protocol sets out the processes applicable to the governance and management of data handled by the Griffith Data Trust, including those applicable to its role as an Accredited Data User and Data Service Provider under the *Data Availability and Transparency Act* (Cth) (DAT Act).
Audience	GDT Staff
Category	Academic
Subcategory	Research
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal/s: 16: Peace, Justice and Strong Institutions
Approval date	October 2024
Effective date	October 2024
Review date	2025
Policy advisor	GDT Policy and Compliance Coordinator
Approving authority	Director, Griffith Data Trust

6.0 Related Policy Documents and Supporting Documents

Legislation	*Data Availability and Transparency Act 2022 (Cth) (DAT Act)* *Privacy Act 1988* *Information Privacy Act 2009 (Qld)*
Policy	Griffith Data Trust Policy Griffith University Privacy Plan Griffith University Information Management Policy
Procedures	Griffith Data Trust Procedure Griffith University Information Security Classification Procedure Griffith University Crises and Incident Response Plan Griffith University Information Governance and Management Framework Griffith University Risk and Resilience Management Framework Griffith University Data Breach Response Plan
Local Protocol	Griffith Data Trust Committee Terms of Reference Griffith Data Trust Security Management Protocol Griffith Data Trust Data Extraction and Sanitation Protocol Griffith Data Trust Human Resource Skills and Capability Management Protocol
Forms	General Staff Agreement form Academic Researcher Agreement form