
Plymouth University

EIM-POL-002-Data Quality Policy

Author: Elena Menendez-Alonso (Digital Curator), Peter Anderson (Corporate Information Manager)

Date: 14/10/2016

Security Level: **PUBLIC**

Status: Published

Version: 1.1

Reference: EIM-POL-002

Document Link: www.plymouth.ac.uk/your-university/governance/information-governance

Review Date: 31/12/2018

1. Introduction

1.1 Purpose:

The Data Quality Policy sets the University's position with regards to data quality and enables the creation of standards for the management of University data.

1.2 Audience:

This policy applies to all members of the University and its partner organisations that have responsibility for any aspect of University data collection, maintenance or disposal.

1.3 Scope:

The policy relates to institutional or management data across the following domains:

- Space & Asset data
- Finance data
- Learning resource data
- Research activity data
- Staff data
- Student data

2. Definitions

Data and Information Data are facts and statistics collected together for reference or analysis¹. When data is processed, organised, structured or presented in a way that gives it context and therefore makes it more useful, it is called 'information'.

In the context of this document and the University's Information Governance framework, the terms 'data' and 'information' can be used interchangeably.

Data Owner Individuals or group of people who have been officially designated as accountable for specific data and for ensuring that procedures have been put in place to maintain and improve standards of data quality and to ensure that the data is managed securely and in compliance with University regulations and statutory obligations. The University establishes the roles and responsibilities associated with the governance of the information & data assets in its Information Governance Roles & Responsibilities policy².

Data Quality A perception or an assessment of data's fitness to serve its purpose in a given context. In line with the Audit Commission Data Assurance Framework³, the characteristics of quality data can be defined as: accuracy, validity, reliability, timeliness, relevance, completeness and compliance

¹ Oxford Dictionaries online, 2014. URL: <http://www.oxforddictionaries.com/definition/english/data>. Accessed: 2014-11-20.

² Plymouth University. Information Governance Roles & Responsibilities. URL : <https://www.plymouth.ac.uk/your-university/governance/information-governance>. Accessed: 2016-10-14.

³ Audit Commission, 2007. Improving information to support decision making: standards for better quality data. URL: <http://archive.audit-commission.gov.uk/auditcommission/subwebs/publications/studies/studyPDF/NEW1051.pdf>. Accessed: 2014-11-20. (Archived by WebCite® at <http://www.webcitation.org/6UDxxlls7>)

3. Data quality statement

3.1 High quality data enables accurate reporting and informed decision-making. Plymouth University recognises this key role, as well as the risks associated with poor data quality. Hence, the University is committed to continually improve the quality of its data.

4. Risks associated with poor data quality

4.1 Data owners and staff who have responsibility for data collection and maintenance should be aware of the risks associated with poor data quality. These include:

- Impaired decision-making
- Reputational damage
- Incorrect funding allocations
- Inaccurate reporting to sponsors, resulting in financial penalties
- Mandatory conditions of grant could be breached
- Misleading external and internal impressions of institutional performance in teaching and research
- Inefficient use of resources
- Good performance may go unrecognised and unrewarded
- Poor services may not be improved

4.2 The University includes failure to ensure appropriate data quality on its risk register.

5. Characteristics of quality data

The University defines the characteristics of quality data as follows:

5.1 Accuracy

- Data should be captured once only close to the point of activity
- Data should provide a clear representation of the activity/interaction

5.2 Validity

- Data should be recorded and used in accordance with agreed requirements, rules and definitions to ensure integrity and consistency

5.3 Reliability

- Data collection processes must be clearly defined and stable to ensure consistency over time, so that data accurately and reliably reflects any changes in performance

5.4 Timeliness

- Data should be collected and reported while still current to inform real time management
- Data should remain available for the intended use within a reasonable or agreed time period

5.5 Relevance

- Data should be fit for purpose
- Data requirements should be clearly specified and regularly reviewed to reflect any change in needs
- The amount of data collected should be proportionate to the value gained from it
- Data should be collected at a level of granularity that allows use for all intended and relevant purposes

5.6 Completeness

- Data should be complete

5.7 Compliance

- Data must comply with regulations on data protection and security

6. Data quality objectives

The University aims to set the following objectives with regards to data quality:

6.1 Responsibility, accountability and awareness

- Data Owners are known and aware of their responsibilities.
- All staff are made aware of this data quality policy, data quality impact and risks, and how they can contribute to better data quality.
- Where appropriate, maintaining data quality standards is recognised in job descriptions and forms part of the Performance Development Review (PDR) process.

6.2 Definitions, policies and procedures

- The University defines data requirements and assurance standards.
- Local procedures exist for key activities and major data collection exercises for external returns
- Policies and procedures are reviewed regularly to consider their impact on data quality and to ensure they reflect any change in needs.
- Policies and procedures are embedded within business processes.

6.3 Systems

- Data is collected and recorded once only, and where necessary, shared across other systems.
- Data collection systems contain internal validation to ensure accurate and complete data.

6.4 Security

- Data is protected from unauthorised input, amendment or destruction.

6.5 Staff Development

- Appropriate staff development is provided at induction and periodically to enable staff to

meet the objectives of this policy.

- Changes to policies and procedures are communicated in a timely and effective manner.
- Staff knowledge and capability is reviewed regularly, and PDR plans updated to reflect any change in development needs.

7. Related documents and further information

7.1 [Data Protection Policy](#)

A high level, public facing statement of the University's commitment and approach to data protection.

7.2 [Freedom of Information Policy](#)

Establishes the University's commitment and approach to fulfilling its obligations under the Freedom of Information Act 2000.

7.3 [Information Security Classification Policy](#)

Sets a framework for classifying and handling Plymouth University information based on its level of sensitivity, and its value to the University.

7.4 [Information Governance – Plymouth University website](#)

Central point of access to advice and guidelines for all aspects of information governance, including data protection, freedom of information and information security.

7.5 [Information Governance Roles & Responsibilities](#)

Establishes the roles and responsibilities associated with the governance of the University's information & data assets.

7.6 [Publication Scheme](#)

Lists the information and documents that the University makes public following advice from the Information Commissioner's Office.

7.7 [Business Classification Scheme and Record Retention Schedule](#)

The **Business Classification Scheme (BCS)** is a conceptual representation of the University's business providing a structure for storing and finding organisational documents. Preserving evidence of decisions made and actions taken is essential to support institutional accountability and compliance, and to satisfy the increasing demand for public access to information. Following the BCS helps to create and preserve evidence and audit trails and supports compliance with the Freedom of Information Act 2000.

The **Records Retention Schedule (RRS)** offers guidance on the minimum length of time Plymouth University records should be retained to comply with legal, regulatory and operational requirements. This includes compliance with the Data Protection Act 1998 and the Freedom of Information Act 2000. The schedule also indicates which area of the University is responsible for the storage and disposal of records and recommends a security classification level for each type of record.

7.8 Further information can be obtained by emailing informationgovernance@plymouth.ac.uk

Document Control

Version	Contributors	Details	Date	Approved by	Position	Date
0.1	EMA, PA	Initial draft	26/06/2014	-	-	-
0.2	EMA, PA	Amendments made and Roles and Responsibilities added.	03/07/2014	-	-	-
0.3	EMA, PA	Minor comments and corrections. Changed logo	04/07/2014	-	-	-
0.4	EMA	Content moved to standard document template. Removed Roles and Responsibilities. Revised definitions. Reordered sections. Other minor corrections	25/11/2014	-	-	-
0.5	JW	Amalgamation of Space & Asset data	27/11/2014	-	-	-
1.0	DQC	Updated 5.4 (granularity of data) and 6.4 (protected from amendment). Approved by DQC.	10/12/2014	DQC	-	09/12/2014
1.1	IDMAG	Bi-annual review: added links to related policies	14/10/2016			