

# Data Quality Policy

---

**From:** Chief Information Officer

**Date:** May 2018

---

## 1 Relevant Law

---

- 1.1 The General Data Protection Regulation (GDPR) will be incorporated into UK law via the Data Protection Act 2018. These are referred to in this policy as the Data Protection Legislation as defined in the [Glossary of Terms](#).
- 1.2 This policy forms part of the University's Information Governance Framework and demonstrates compliance with its obligations under the [Data Protection Legislation](#).

## 2 Introduction

---

- 2.1 The University needs timely, accurate and reliable data in order to manage activities and meet internal and external requirements to demonstrate accountability through accurate reporting.
- 2.2 Specifically the University needs to ensure its data quality so that it can:
  - 2.2.1 Comply with its obligations under the Data Protection Legislation to ensure that the Personal Data it processes are accurate and, where necessary, kept up to date and that reasonable steps are taken to ensure that any Personal Data that are inaccurate, having regard to the purposes for which it is processed, are erased or rectified without delay.
  - 2.2.2 Provide effective and efficient services to Users.
  - 2.2.3 Produce accurate and comprehensive management information on which timely, informed decisions can be made to inform the future of the University.
  - 2.2.4 Monitor and review activities and operations.
  - 2.2.5 Produce accurate external returns to ensure accurate funding allocations, and to demonstrate accountability to public and private funders.

- 2.2.6 Meet the 'Terms and Conditions of Funding for Higher Education Institutions' between the Office for Students and the University; and the 'Terms and Conditions of Research England Grant' between Research England and the University.

### 3 Scope

---

- 3.1 To ensure the security of the University's information assets by:
- 3.1.1 Providing effective and efficient services to Users.
  - 3.1.2 Ensuring availability of assets to users.
  - 3.1.3 Preserving integrity by protecting assets against unauthorised or accidental disclosure.
  - 3.1.4 Preserving confidentiality by protecting assets against unauthorised disclosure.

### 4 Roles and Responsibilities

---

#### 4.1 The Audit Committee

- 4.1.1 Is responsible for reviewing and monitoring the effectiveness of the arrangements for the management and quality assurance of data submitted to the Higher Education Statistics Agency (HESA), Office for Students, Research England, and other funding bodies. The Memorandum of assurance and accountability between the Office for Students and Higher Education institutions ("HEI") sets out the terms and conditions for payment of teaching grants to HEI's and provides that each Institution must have an audit committee which follows best practice in Higher Education corporate governance A link to the memorandum can be found under clause 10 (Further Information).
- 4.1.2 Is responsible for preparing a report to Council as Governing Body and the Vice Chancellor as the Accountable Officer assuring them about the adequacy and effectiveness of:
  - (a) Risk management, control and governance
  - (b) Value for money (VFM)
  - (c) The management and quality assurance of data.
- 4.1.3 Is responsible for sharing the final annual Audit report to Council (as Governing Body and the President & Vice Chancellor as the Accountable Officer) with the Office for Students each year. This report must include the Committee's opinion on the adequacy and effectiveness of the HEI's arrangements for:
  - (a) Risk management, control and governance

- (b) Economy, efficiency and effectiveness (VFM)
  - (c) Management and quality assurance of data submitted to the Higher Education Statistics Agency, the Student Loans Company, Office for Students, Research England, and other bodies.
- 4.2 The Chief Information Officer has overall accountability for University information governance/assurance, and for establishing and maintaining an effective document management system.
- 4.3 The Head of Information Security is responsible for ensuring that appropriate security measures are in place to protect data from unauthorised access from outside the University.
- 4.4 The Data Quality Group (DQG) has responsibility for the oversight of processes, systems and review to ensure accurate and valid data, concerning external statutory returns. The DQG reports to the Information Governance Group. A copy of the terms of reference can be requested via email: [planning@soton.ac.uk](mailto:planning@soton.ac.uk).
- 4.5 For all Users employed by the University an integral part of their role is to ensure that they follow the principles of this policy in order to maximise the accuracy, timeliness and quality of data collected and recorded, analysed and reported.

## 5 Risk

---

- 5.1 Key risks relating to data are as follows:
- 5.1.1 Processing of inaccurate data breaches the principles of the Data Protection Legislation,
  - 5.1.2 Mandatory conditions of grant could be breached.
  - 5.1.3 Data could give misleading external and internal impressions of the University's performance in teaching and research.
  - 5.1.4 Poor data could result in inappropriate decision-making across the University.
  - 5.1.5 Poor data could result in reputational damage in areas such as student recruitment and access, and student records.
  - 5.1.6 Poor data could lead to inadequate reporting to sponsors of research, resulting in financial penalties from funders or, depending upon the extent of the problem, reputational damage and diminished funding for research.
  - 5.1.7 Inaccurate data could lead to under-funding.
  - 5.1.8 Inaccurate data could lead to over-funding with subsequent claw-back of overpaid funds which, if significant, could impact adversely on the University's financial health.

5.1.9 Inaccurate data could lead to reduced future funding (holdback) thereby undermining the cash flow forecasts and adversely affecting financial health.

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

## 6 Characteristics of Good Data

---

6.1 In March 2007, the Audit Commission published a Framework to support improvement in data quality in the public sector. A link to the Framework can be found in Clause 10 (Further Information). The Framework sets out six key characteristics of good quality data, which are summarised in [Schedule 1](#).

## 7 Data Quality Objectives

---

7.1 The characteristics of good quality in the points above provide the criteria against which the significance and purpose of the data must be balanced. The objectives of data quality are set out in [Schedule 2](#).

## 8 Monitoring compliance and review

---

8.1 All information governance and security policies and procedures will be subject to periodic audit and review to ensure that they remain fit for purpose and the University remain compliant.

## 9 Further information

---

9.1 Memorandum of assurance and accountability between Office for Students and institutions in force from 1st April 2018, and superseded the HEFCE 'Financial Memorandum and Accountability and Audit Code of Practice', at:

<http://www.hefce.ac.uk/pubs/year/2014/201412/>

9.2 Audit Commission Framework at: <http://archive.audit-commission.gov.uk/auditcommission/subwebs/publications/studies/studyPDF/NEW1051>

9.3 We also have additional policies and guidelines concerning particular activities. Please see our [Publication Scheme](#).

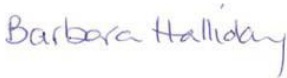

## Document Control

File Name	Data Quality Policy
Original Author(s)	Paula Codd
Current Revision Author(s)	FTVB
Owner	Chief Information Officer
Publication Date	
Target Audience	

## Version History

Version	Date	Author(s)	Notes on Revisions
0.00		Paula Codd	Initial Draft
0.01	05 Mar 15	Paula Codd	Amended draft
0.02	08 Mar 15	Paula Codd	Incorp. ref to Data Protection Policy
0.03	21 May 15	Paula Codd	Updates following comments from Legal services
0.04	15 Sept 15	Paula Codd	Updates following DQG 04.06.15

## Document Sign Off

Name	Role	Doc version	Signoff date	Signature*
Barbara Halliday	Director of Legal Services	1	24-05-2018	
Professor Simon Cox	Chief Information Officer	1	24-05-2018	

\*If signoffs are received by email, print names here and archive the sign off emails.  
Add location of signoff emails here:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Intranet is the controlled document copy. Any printed copies of this document are not controlled.



## Schedule 1 Characteristics of Good Data

### 1 The Six Characteristics of Good Data

---

#### 1.1 Accuracy

- 1.1.1 Data should provide a clear representation of the activity/interaction.
- 1.1.2 Data should be in sufficient detail.
- 1.1.3 Data should be captured once only as close to the point of activity as possible.

#### 1.2 Validity

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

#### 1.3 Reliability

- 1.3.1 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.

#### 1.4 Timeliness

- 1.4.1 Data should be collected and recorded as quickly as possible after the event or activity.
- 1.4.2 Data should remain available for the intended use within a reasonable or agreed time period.

#### 1.5 Relevance

- 1.5.1 Data should be relevant for the purposes for which it is used.
- 1.5.2 Data requirements should be clearly specified and regularly reviewed to reflect any change in needs.
- 1.5.3 The amount of data collected should be proportionate to the value gained from it.

#### 1.6 Completeness

- 1.6.1 Data should be complete.
- 1.6.2 Data should not contain redundant records.

## Schedule 2 Data Quality Objectives

### 2 The Objectives of Data Quality

---

2.1 Appropriate Responsibility, Accountability and Awareness. Where appropriate, users should:

- 2.1.1 Recognise the need for good quality data and how they can contribute to it.
- 2.1.2 Be aware of their individual responsibilities with regard to data collection, storage, analysis and reporting.
- 2.1.3 Be aware of the implications of poor data quality in their area in terms of internal and external accountability including those affecting other departments and the University as a whole.
- 2.1.4 Report any systematic data quality issues immediately to their manager who should ensure remedial action is taken.
- 2.1.5 When handling and sending data for the purpose of producing external returns adhere to the data protection principles and University policies.
- 2.1.6 All users should be aware of and familiar with the principles of the Data Protection Act 1998, the General Data Protection Regulations and the University's policies relating to data protection, confidentiality and the security of personal information. For more information please see the University's Data Protection Policy, A link to the policy can be found under "Further Information".

### 2.2 Appropriate Policies and Procedures

- 2.2.1 The University should define clearly its key data requirements and assurance arrangements.
- 2.2.2 Local procedures must exist for all key activities such as major data collection exercises and external returns.
- 2.2.3 Departmental managers should ensure that all such policies and procedures are adopted and embedded within working processes and that compliance is achieved.
- 2.2.4 Policies and procedures relating to data quality of external returns are overseen by the Data Quality Group and the Student External Returns Sub-Group, with specific external returns (procedures and processes) being subject to review by PwC. All such policies and procedures should be reviewed regularly to consider their impact on data quality and to ensure they reflect any change in need.



## **2.3 Appropriate Systems and Processes**

- 2.3.1 Clear systems and business processes should exist in which data collection and reporting are an integral part.
- 2.3.2 Guidelines for all processes supporting key data requirements as defined by the University should exist and be followed consistently across the University.
- 2.3.3 Data should be collected and recorded once only wherever possible without the need for multiple systems.
- 2.3.4 Data collection systems should contain internal validation to ensure accurate and complete data.
- 2.3.5 Corporate systems should have internal validation checking facilities to ensure data is complete, consistent and internally validated.
- 2.3.6 All systems should be electronic wherever possible to reduce the risk of manual error, except where there is a need to collect, process and store original documents.
- 2.3.7 There should be clear strategies for data storage and archiving from systems, with retrieval and security appropriate to an evaluation of present value and future use.

## **2.4 Appropriate Security**

- 2.4.1 The University should have in place appropriate security arrangements to ensure that data is protected from unauthorised access from outside the University.
- 2.4.2 All corporate systems should have security arrangements in place to ensure appropriate levels of access to data by individual Users.
- 2.4.3 Further details on 'Information Security, policies and regulations' can be found via the [iSolutions](#) website.