



# Northumberland County Council

## DATA QUALITY POLICY

DOCUMENT REFERENCE	VERSION	DATE OF THIS VERSION	DATE OF ORIGIN
NCC/IG11	2.2	18/05/2018	08/10/2008

	APPROVED BY	APPROVAL DATE
1	Data Protection Officer	24/05/2018

DATE REVIEWED	REVIEWED BY	APPROVAL DATE	NEXT REVIEW DATE
			May 2020



# Northumberland County Council

## Related Policies

POLICY NAME	POLICY REFERENCE NUMBER	VERSION
Records Management Policy	NCC.IG01	1.3
Data Protection and Confidentiality Policy	NCC.IG02	5.3
Freedom of Information Policy	NCC.IG04	2.2
Environmental Information Policy	NCC.IG05	1.0
Information Security and Transportation, Transfer and Sharing of Data Policy	NCC.IG10	
Employee and Elected Members Code of Practice		

## Amendment History

VERSION	DATE	DESCRIPTION
0.1	08/10/2008	Working Draft
1.0	23/03/2009	Changes made after consultation with the Information Governance Group
2.0	30/07/2013	Amendments to contact details
2.1	18/02/2016	Policy put into new format
2.2	18/05/2018	Amendments to reflect the General Data Protection Regulation (GDPR) 2018



# Northumberland County Council

## Table of Contents

1. [Scope](#)
2. [Purpose](#)
3. [Introduction](#)
4. [Responsibilities](#)
5. [Data Management](#)
6. [Legislation](#)
7. [Violations](#)
8. [Training and Awareness](#)
9. [Compliance](#)
10. [Implementation](#)
11. [Monitoring and Review](#)
12. [Useful Contacts](#)



# Northumberland County Council

## 1. Scope

- 1.1 The scope of this Policy applies to all Northumberland County Council employees and members. Agency workers or sub-contractors who are required to use Northumberland County Councils information systems will also be made aware of and be expected to abide by this policy.

## 2. Purpose

- 2.1 The purpose of this Policy is to set out requirements and responsibilities for managing data retained in any and all formats, including electronic records, throughout the data's lifecycle. It applies to all aspects of the Council's work, all data created and received during the conduct of the Council's business and all information systems used to create or otherwise process the data.
- 2.2 This Policy is part of a suite of Information Governance policies.

## 3. Introduction

- 3.1 For the purposes of this Policy, Data Quality is defined as being the creation, processing and management of Council information in such a way as to ensure its authenticity, reliability, integrity and usability. This is explained in more detail below.
- 3.2 Data created, received and used by individuals become and remain the property of the Council. As such, the data must be organised and retained to meet both immediate short-term user needs and the long-term corporate requirements of the Council. This is explained in more detail in the Corporate Records Management Policy.

## 4. Responsibilities

- 4.1 The quality of data is the responsibility of the Council as a corporate body, and consequently is the responsibility of all members of staff.
- 4.2 All staff must ensure the security, integrity, confidentiality and availability of all data that they create, process or use, and must only attempt to access data for which they have access permissions.
- 4.3 Senior managers in groups and departments are responsible for the implementation and policing of this Policy, ensuring that all staff are aware of the need for high quality data and why specific data is produced and retained.



# Northumberland County Council

- 4.4 Senior managers must also ensure that responsibility for data quality is reflected in Job Descriptions, commensurate with the post holder's level of involvement in data quality issues.
- 4.5 All staff are also reminded that there are elements of the Council's Code of conduct which also apply.

## 5. Data Management

- 5.1 The Council's data require proper management throughout their lifecycle from creation to disposal or transfer to permanent archive.
- 5.2 The Council's data must be consistent and comprehensive, produced in a timely manner and be of high quality. In order to achieve this there are four general principles governing the quality of the Council's data:
- Authenticity
  - Reliability
  - Integrity
  - Usability
- 5.3 In order to meet these principles, all staff are responsible for ensuring that any data they create must:
- Be what it purports to be
  - Include the name of its creator
  - Be created by the person purported to have created it
  - Be created at the time purported.
  - Be complete and unaltered
  - Include an indication of types of annotations made to the record
  - Include indication of any technical modifications made to the record
  - Be capable of being trusted as a full and accurate representation of the transactions, activities, facts etc that it refers to
  - Be capable of being depended upon in the course of subsequent transactions or actions
  - Be easily located and distributed to or retrieved by any authorised user
  - Be capable of being interpreted and presented individually or as part of a report, table, chart etc, in a consistent and agreed format
- 5.4 The general principles identified above must be applied to the creation, management, processing and sharing of all Council data. To this end, all staff in all groups of the Council must be aware of the need for high quality data, and for this to be an integral part of all the day-to-day operations of all departments.



# Northumberland County Council

- 5.5 All data must have a named creator and owner with permissions set for those who can access and / or carry out amendments and modifications to that data.
- 5.6 All data should be processed and input at the earliest opportunity, and on an ongoing basis.
- 5.7 Systems used for creating, storing, processing and presenting data must have a named individual responsible for Data Quality with a nominated deputy. S/he will ensure that:
- Users have adequate training
  - Access to and amendment of the data is secure
  - System upgrades are made as and when necessary
  - Actions recommended as a result of audit system reviews are completed
  - A suitably secure user guide exists for the creation / processing of all data
  - A business continuity plan exists to safeguard the data
- 5.8 Access to data must be restricted in accordance with its nature, content and sensitivity, with a retention period identified to ensure that the data is not retained for longer than is necessary.
- 5.9 A computer must not be logged onto a system and left unattended unless a password-protected screensaver has been activated or the computer has been locked. Screensavers with password protection must be those supplied with the machine as password protection of some other screensavers has been found to be ineffective.
- 5.10 Where data needs to be shared between individuals the data must be held in a networked, restricted shared folder or other secure environment. The Information Services Service Desk can advise on this.
- 5.11 The quality of data produced by third parties such as external contractors must be to an agreed standard and where appropriate be included in all contractual arrangements.

## 6. Legislation

- 6.1 The Council and its policies, procedures and practices must comply with all legislation affecting the creation and processing of data. This includes but is not limited to:
- The General Data Protection Regulation 2018
  - The Freedom of Information Act 2000



# Northumberland County Council

- The Human Rights Act 1998
- The Copyright Designs and Patents Act 1988
- The Computer Misuse Act 1990

## 7. Violations

7.1 Violations of this Policy will include:

- The disclosure of confidential information
- Unauthorised use of Council data and / or the sending of defamatory information
- Creation, processing or use of any data known to be inaccurate or invalid
- The accessing, creation, processing or use of any data by unauthorised users
- The use of data for illicit or illegal purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government agency

7.2 Any individual who has knowledge of such a violation must report it to his / her supervisor or to the Data Protection Officer via [informationgovernance@northumberland.gov.uk](mailto:informationgovernance@northumberland.gov.uk)

7.3 Any breach of this Policy may lead to appropriate action being taken against those who commit the breach, including Disciplinary Procedures.

## 8. Training and Awareness

8.1 All staff and Members will need to be aware of the Council's Data Quality Policy to help understand their basic responsibilities. Some members of staff will require further training and guidance. Those members of staff will be identified by their line manager.

8.2 When staff and Members join the Council, it is important that they are introduced to their basic responsibilities in regard to data quality.

## 9. Compliance

9.1 Any violation of this policy will be investigated and if the cause is found to be wilful disregard or negligence, it may be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the HR Department.

## 10. Implementation



# Northumberland County Council

10.1 This procedure is effective immediately.

## **11. Monitoring and Review**

11.1 This policy will be monitored by the Digital Northumberland Board and will be reviewed every two years or where there are changes to Legislation.

## **12. Useful Contacts**

The Data Protection Officer via [informationgovernance@northumberland.gov.uk](mailto:informationgovernance@northumberland.gov.uk)

The Information Commissioner's Office via [www.ico.org.uk](http://www.ico.org.uk)