Northumberland County Council

NCC Data Protection Policy

Issue No:	V4.1
Reference:	NCC/IG1
Date of Origin:	28/07/2008
Date of this Issue:	16/05/2014

DOCUMENT TITLE	**NCC Data Protection Policy**	
DOCUMENT REFERENCE	ISSUE	DATE
NCC/IG1	V4.1	16/05/2014

Related Policies:	Incident Management and Reporting Policy
Subject Access Policy	Employee and Elected Members Code of Conduct
Information Security Policy	

Date Reviewed	Reviewed By	Date Approved	Policy Review Date
16 May 2014	Data Protection and Information Governance Officer	October 2014	October 2015

NCC Reviewers

	APPOINTMENT	DATE
AUTHOR	Data Protection and Information Governance Officer	N/A
REVIEWERS:		
1	Information Governance Manager	Jan 2012
2	Head of Information Services	Jan 2012
3	Deputy Chief Executive (SIRO)	Jan 2012

Table 1: NCC Reviewers

NCC Approvals

	NAME	APPROVAL DATE
1	Information Governance Working Group	
2	Information Governance Board	24 May 2013

Table 2: NCC Approvals

Amendment History

VERSION	DATE	DESCRIPTION
0.1	28/07/2008	Working Draft
0.2	21/10/2008	Final Draft
1.0	23/03/2009	Final Version
1.1	20/12/2011	Updated
2.0	02/02/2012	Updated
3.0	28/03/2012	Updated
4.0	09/05/2013	Updated
4.1	**16/05/2014**	**New format, minor amendments**

Table 3: Amendment History

Any queries arising from this Policy or its implementation can be taken up directly with the Data Protection and Information Governance Officer who is the Owner of this document and has approved management responsibility for its development, review and evaluation.

Table of Contents

1. Scope

1.1 This policy applies to all elected members, employees, contractors, agents, consultants, partners or other servants of the Council who manage and handle personal information held by, or on behalf of Northumberland County Council (NCC).

1.2 This policy covers all personal data, however they are held, on paper or in electronic format. It also covers the rights of individuals (data subjects) who wish to see information the Council holds about them (by submitting a Subject Access Request).

1.3 This policy does not intend to replace the Data Protection Act 1998, it merely aims to simplify the Acts content – referral to the act may be necessary in order to ensure compliance with requirements and any advice pertaining to this should be sought initially from the Data Protection and Information Governance Officer or from the Legal Services Unit within NCC.

2. Introduction

2.1 Northumberland County Council is fully committed to compliance with the requirements of the Data Protection Act 1998 (the Act), which came into force on the 1st March 2000. It is a legal requirement that the Council complies with the Act, and all elected members, employees, contractors, agents, consultants, partners or servants of the Council have a statutory responsibility to ensure compliance.

2.2 The Council will therefore follow procedures which aim to ensure that everyone who manages and handles personal information for, or on behalf of the Council, are fully aware of, and abide by their duties and responsibilities under the legislation.

2.3 In order to operate efficiently, Northumberland County Council has to collect and use personal information about people with whom it works and conducts its business. These people may include members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, the Council may be required by law to collect and use personal information in order to comply with the requirements of central government. Personal information must be handled and dealt with properly and securely, however it is collected, recorded, used, deleted and disposed of. There are safeguards within the Act to ensure this.

2.4 Northumberland County Council regards the lawful and correct treatment of personal information as very important to its successful operations, and to maintaining confidence between the council and those with whom it carries out its business. The Council will ensure that it treats personal information lawfully and correctly.

3. Definitions

3.1 Personal data is information which relates to a living individual who can be identified:

- from that data, or
- from that data when combined with other information which is either in the Council's possession or likely to come into the Council's possession.

3.2 For the purposes of the Act, and the Council's Data Protection Policy, it is safest to assume that all information about a living, identifiable individual is personal data and should be dealt with accordingly.

3.3 Sensitive Personal Data can include information relating to:

- Religious belief
- Sexual life
- Physical or mental health conditions
- Member of a trade union
- Political opinions
- Commission or alleged commission of an offence
- Proceedings for any offence committed or alleged to have been committed

3.4 Sensitive data must only be used for approved purposes (e.g. equal opportunities monitoring) and access to this data must be restricted to those who have a need to know. They should never be kept in a generally accessible record or file. Advice on the issue of sensitive data can be sought from the Information Governance Office.

4. Handling of Personal/Sensitive Information

4.1 Northumberland County Council will through appropriate management and the use of strict criteria and controls.

4.1.1 Ensure everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice

4.1.2 Ensure everyone managing and handling personal information are adequately trained and supervised to do so

4.1.3 Observe fully conditions regarding the fair collection and use of personal information.

4.1.4 Meet its legal obligations to specify the purpose for which information is used

4.1.5 Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements

4.1.6 Ensure the quality of information used

4.1.7 Apply strict checks to determine the length of time information is held

4.1.8 Take appropriate technical and organisational security measures to safeguard personal information

4.1.9 Ensure that personal information is not transferred abroad without suitable safeguards

4.1.10 Ensure methods of handling personal information are regularly assessed and evaluated

4.1.11 Ensure that the rights of people about whom the information is held can be exercised fully under the Act. These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 calendar days;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as inaccurate.

5. Responsibilities

5.1 Whilst the Council's Lead Executive Director is ultimately responsible, both personal and corporate responsibility applies. All employees are therefore responsible for ensuring compliance with the principles of the Data Protection Act by complying with this policy.

5.2 Line managers must ensure that those staff managing and handling personal information are adequately trained and supervised with regard to the requirements of this policy.

5.3 The Information Governance Lead Officers in services are responsible for ensuring that they and staff in their service are aware of the relevant documentation. Lead Officers will progress relevant data protection Subject Access Requests (See paragraph 13 below) and liaise with the Council's Data Protection and Information Governance Officer on any issues which may arise.

5.4 The Data Protection and Information Governance Officer will monitor the Council's compliance with the Act, ensure that the Data Protection Policy is implemented, advise and consult on responses to data Subject Access Requests and make regular reviews of this policy and associated documentation.

5.5 All Data Protection breaches must be reported to the Information Services Information Security Team following the Data Breach Management Policy.

6. The Principles of the Data Protection Act 1998

6.1 The eight principles which form the basis of the Act state that data must be:

6.1.1 **Fairly and lawfully processed**
Data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed.

6.1.2 **Processed for limited purposes**
Personal data can only be obtained for specified and lawful purposes with permission from the data subject for each purpose.

6.1.3 **Adequate, relevant and not excessive**
The data must be sufficient to meet their purpose but not provide more information than the purpose requires, or provide information outside the scope of the purpose.

6.1.4 **Accurate**
The personal data must be accurate when recorded, and accuracy must be maintained throughout the lifecycle of the data.

6.1.5 **Not kept for longer than is necessary**
Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained. If data is kept for too long, the accuracy and relevance may be compromised.

6.1.6 **Processed in line with the rights of the subject of the data**
Data subjects have the right to access their personal data and can request the termination of any processing that causes or is likely to cause them distress. They can insist that their data is not used for marketing and other purposes, and can request that inaccurate data is amended.

6.1.7 **Stored and processed securely**
All necessary measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction.

6.1.8 **Not transferred to countries without adequate protection**
Personal data must not be transferred to a country outside the European Economic Area (i.e. the EU member states, Norway, Iceland and Liechtenstein) unless that country has in place a level of data protection comparable to that in the EU. Advice should be sought from the Information Governance Officer.

7. Processing Personal Data

7.1 The definition of processing in relation to data protection is very wide. Obtaining, holding, filing, organising, transmitting, retrieving, disseminating, disclosing and destroying of data are all deemed to be processing in addition to any other process that is carried out on the data.

7.2 Members, employees and others acting on behalf of the Council must only have access to personal data that is necessary in order to carry out their duties and responsibilities.

7.3 All forms used to obtain personal data, such as application forms or registration forms must:

7.3.1 State the purpose/s for which the information is required.

7.3.2 Be reviewed regularly to check that all of the information asked for is still required and necessary.

7.3.3 Be checked for the accuracy of all data before it is used for any processing. If in doubt about the accuracy of the data it must be referred back to the data subject for confirmation.

7.4 Personal data must be collected and handled in a way that complies with the Act and meets the eight principles above. This imposes a duty on the Council to ensure that individuals are made aware of the uses that will be made of the information that they supply and give their consent to this.

7.5 If an outside agency provides data to the Council, it must be asked to confirm in writing that the data was obtained fairly and lawfully, in compliance with the Act.

7.6 Where personal data is provided for the purpose of placing a contract to which the data subject is a party then such data is considered to be fairly and lawfully obtained.

8. The Purpose of the Data/Notification to the Information Commissioner

8.1 In addition to obtaining consent, the data must be used only for the declared purpose/s, which the Council has notified to the Information Commissioner's Office.

8.2 The Information Commissioner maintains a public register of data controllers. Northumberland County Council is registered as such, Elected Members also have their own individual registration. The Council's registration entry can be seen via a link on our Data Protection Act webpage, the Information Commissioners website or from the Data Protection and Information Governance Officer.

8.3 The Act requires every data controller who is processing personal data to notify and renew their notification with the Information Commissioner on an annual basis. Failure to do so is a criminal offence.

8.4 The Data Protection and Information Governance Officer will review the Data Protection Register annually with designated officers, prior to notification to the Information Commissioner.

8.5 If there is a new purpose or change to an existing purpose on the Register then the Council's Data Protection and Information Governance Officer must notify the Information Commissioner within 28 days.

8.6 Processing of data cannot begin for the new or amended purpose until the Commissioner has accepted this notification.

8.7 To this end, any changes made between reviews must be brought to the attention of the Data Protection and Information Governance Officer immediately.

9. Relevant and Adequate Data

9.1 The Council must process only that information which is necessary to fulfill the business requirement or which is needed to comply with legal requirements. For example it is not necessary to ask about a driving licence on a job application form if the post applied for does not entail any driving duties.

10. Collecting Accurate Data

10.1 Errors in personal data that could or does cause data subjects damage or distress could lead to the Council being prosecuted. It is important therefore that all appropriate measures are put in place to verify the accuracy of data when it is collected, especially when any significant decisions or processes depend upon the data.

10.2 There is a requirement to ensure that data is kept up to date throughout the lifecycle of the data.

11. Keeping Data Only As Long As Necessary

11.1 Retention periods should be defined for personal data and procedures put in place to ensure compliance.

11.2 Retention periods must be for clear business purposes and must be documented to identify why certain records are retained for certain periods of time.

11.3 When no longer required, data must be deleted or disposed of securely.

12. Safeguarding the Rights of Data Subjects

12.1 Individuals have various rights under the Act. These are: -

- The right to be told that processing is being carried out.
- The right of access to their personal data.
- The right to prevent processing in certain cases.
- The right to have inaccurate or incorrect information corrected, erased or blocked from processing.
- The right to be informed if their data has been inappropriately used or released.

13. Subject Access Requests

13.1 The Council must make available details of how individuals can request access to their data, by means of a Subject Access Request. Please see our Subject Access Request Policy for further details.

14. Keeping Data Secure

14.1 The Council acts as custodian of personal data and must therefore ensure that necessary and sufficient precautions are in place to prevent misuse or unauthorised access to data as well as having security measures in place to prevent loss or damage to data. Please see NCC Personal Information Security Policy for further information on how to protect the data you hold.

14.2 Where outside bodies process or hold any of the Council's personal data then the Council must be satisfied that the data is held securely and with due regard to the obligations of the Act.

15. Transfer of Data

15.1 Data must not be transmitted or transferred out of the European Economic Area (i.e. the EU member states, Iceland, Norway and Liechtenstein) unless the country they are being transferred to has the same or equivalent standards of Data Protection. This has implications for data placed on the Internet and use of e-mail where servers are based abroad.

15.2 If information is required to be transferred abroad then checks must be made to ensure that the data is held securely during transfer and that data recipients apply data protection rules

equivalent to those in the UK Data Protection Act 1998. Advice on this should be sought from the Information Governance Officer.

16. Training and Awareness

16.1 All staff and Councillors will need to be aware of the Council's Data Protection Policy. To help staff understand the basic principles, data protection awareness training will be provided.

16.2 Some members of staff will require further training and guidance. Those members of staff will be identified through their work with initial discussion with their line manager.

16.3 When staff and Councillors join the Council, it is important that they are introduced to their basic responsibilities under the Data Protection Act. To ensure that they are aware, they will need to complete mandatory modules in Data Protection Awareness and Subject Access Awareness done in conjunction with reading the Data Protection Policy and Subject Access Policy.

17. Compliance

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

18. Implementation

18.1 This procedure is effective immediately.

19. Monitoring and review

19.1 This procedure will be monitored by the Information Governance Board and will be reviewed annually or where there are changes to Legislation.

20. Useful contacts

The Information Governance Office via Data.Protection@northumberland.gov.uk

The Information Commissioner's Office via www.ico.org.uk