Northumberland County Council

Cambo First School
Data Protection Policy

Version History

Version	Date	Description	Author
0.1	28/07/2008	Content based on NCC auditor's template with additions and amendments from existing policies from all Northumberland councils	Chris Heane
0.2	21/10/2008	Final Draft	Chris Heane
1.0	**23/03/2009**	**Final Version**	**Chris Heane**

Distribution List

Name	Job Title	Date

Date of Next Review: 31/03/2010

Approval and Authorisation

Name	Job Title	Signature	Date
Author:- Chris Heane	Information & Network Security Manager, NCC		23/03/2009
Approved by:- Keith Taylor	Network Manager		
Authorised By:- Peter Gallon	Head of Information Services		

This Policy outlines how the Council and all of its employees must meet the requirements of the Data Protection Act 1998.

Any queries arising from this Policy or its implementation can be taken up directly with the Information Security Officer at ITSecurity@northumberland.gov.uk

The Information Security Officer is the Owner of this document and has approved management responsibility for its development, review and evaluation.

Summary of Contents:

1. Scope

1.1 This policy applies to all elected members, employees, or any other person with access to personal or sensitive information processed by Northumberland County Council.

1.2 The policy covers the obtaining of personal data, its storage and security, its use and its ultimate deletion or disposal

1.3 The policy should be read in conjunction with the Council's Code of Conduct and the ICT & Information Security Policy. These documents are available on the intranet, or from the Information Security Officer at ITSecurity@northumberland.gov.uk

2. Introduction

2.1 Everyone managing and handling personal information needs to understand their responsibilities in complying with the Data Protection Act 1998 (the Act).

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

2.3 It is a legal requirement that the Council complies with the Act, and all members of staff have a statutory responsibility to ensure the Council's legal compliance.

2.4 This policy is intended to facilitate compliance and all staff should be aware of its content and the key requirements of the Act. The Council's Code of Conduct also refers to staff obligations with regard to Data Protection and managers should ensure that staff are provided with the appropriate knowledge and training to ensure they can fulfill their responsibilities.

2.5 All of these documents are available on the intranet or from ITSecurity@northumberland.gov.uk Data Protection lead officers in each

service are responsible for making staff in their service aware of these documents

3. Responsibilities

3.1 Whilst the Council's Chief Executive 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.

3.2 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.

3.3 Data Protection 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 12 below) and liaise with the Council's Data Protection Officer on any issues which may arise.

3.4 The Data Protection 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.

4. Definitions

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

4.1.1 from those data
4.1.2 From those data when combined with other information which is either in the Council's possession or likely to come into the Council's possession.

4.2 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.

4.3 Sensitive Personal Data can include information relating to

4.3.1 Religious belief
4.3.2 Sexual life
4.3.3 Physical or mental health conditions
4.3.4 Member of a trade union
4.3.5 Political opinions
4.3.6 Commission or alleged commission of an offence
4.3.7 Proceedings for any offence committed or alleged to have been committed

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 Data Protection Officer.

5. The Principles of the Data Protection Act 1998

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

5.1.1 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.

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

5.1.3 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.

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

5.1.5 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 are kept for too long, the accuracy and relevance may be compromised.

5.1.6 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.

5.1.7 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.

5.1.8 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 Data Protection Officer.

6. Processing Personal Data

6.1 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.

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

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

6.3.1 State the purpose/s for which the information is required

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

6.3.3 Be checked for the accuracy of the data before they are used for any processing. If in doubt about the accuracy of the data they should be referred back to the data subject for confirmation

6.4 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.

6.5 If data are provided by an outside agency then the agency must be asked to confirm in writing that the data were obtained fairly and lawfully, in compliance with the Act.

6.6 Any information held regarding criminal convictions must be treated as sensitive information and handled accordingly. Any request made by the Council for such information must be fully justified. Advice should be sought from the Data Protection Officer.

6.7 Where personal data are 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.

7. The Purpose of the Data

7.1 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.

7.2 If there is a new purpose or change to an existing purpose then the Council's Data Protection Officer must notify the Information Commissioner's Office immediately.

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

7.4 The Council's registration entry with the Information Commissioner's Office can be seen via the intranet or from the Data Protection Officer.

8. Relevant and Adequate Data

8.1 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.

9. Collecting Accurate Data

9.1 Errors in personal data that 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 they are collected, especially when any significant decisions or processes depend upon the data.

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

10. Keeping Data Only As Long As Necessary

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

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

10.3 When no longer required, data must be deleted or disposed of securely. Further information on this is available in the ICT & Information Security Policy or from the Information Security Officer.

11. Safeguarding the Rights of Data Subjects

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

11.1.1 The right to be told that processing is being carried out
11.1.2 The right of access to their personal data
11.1.3 The right to prevent processing in certain cases
11.1.4 The right to have inaccurate or incorrect information corrected, erased or blocked from processing.

12. Subject Access Requests

12.1 The Council must make available details of how individuals can request access to their data, by means of a Subject Access Request.

12.2 Subject Access Requests must be made in writing and sufficient detail must be obtained to ensure that the request has been made by the data subject in person.

12.3 As proof of identity at least two identifying documents of the data subject, such as a driving licence, passport, recent utility bill etc must accompany the

request. If a third party is making the request, a signed letter of consent from the data subject should also be enclosed.

12.4 The request must then be passed to the appropriate service/s data protection lead officer to progress.

12.5 Subject Access Requests must be satisfied within 40 calendar days of their receipt by the Council.

12.6 Some Subject Access Requests may require further information before the process can commence. This information must be requested as soon as possible after the original request has been made. If this additional information is not received within 6 months, the request should be closed and a new request will have to be made.

12.7 It is not permitted to give personal data to third parties unless it is already in the public domain, or authorised by the data subject.

12.8 In certain circumstances, the courts, police or Inland Revenue may have the right of access to personal data without prior permission or knowledge of the individuals concerned. Any such request should be referred to the Data Protection Officer via the service's data protection lead officer.

13. Keeping Data Secure

13.1 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.

13.2 Filing cabinets containing personal data must be locked outside of normal working hours and keys must be held securely by nominated staff.

13.3 Electronic files must be password protected and passwords must be changed on a regular basis.

13.4 All such electronic data must be stored in secure server areas, not on computer hard drives, laptops or other mobile devices.

13.5 Any electronic data backed up to media such as CD must be kept physically secure.

13.6 If any data are to be taken from the office (e.g. to work at home) then the data must be held securely at all times whilst in transit and at the location they are being held. In particular data must be protected from unauthorised access.

13.7 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.

14. Transfer of Data

14.1 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.

14.2 If information is required to be transferred abroad then checks must be made to ensure that the data are 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 Data Protection Officer.

Data Protection Policy v1.0 Final Version
Chris Heane
Information & Network Security Manager
March 2009