Northumberland
County Council

DATA PROTECTION AND CONFIDENTIALITY POLICY

DOCUMENT REFERENCE	VERSION	DATE OF THIS VERSION	DATE OF ORIGIN
NCC/IG02	5.3	08/05/18	28/07/2015

	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
Information Charging Policy	NCC.IG06	1.0
Information Complaints Policy	NCC.IG08	1.0
Information Security and Transportation, Transfer and Sharing of Data Policy	NCC.IG10	
Employee and Members Codes of Conduct		

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
5.0	12/11/2015	Merging of Data Protection and Subject Access Policies
5.1	21/07/2016	New format, minor amendments
5.2	22/11/2016	Changes made after consultation with the Information Governance Group, Digital Northumberland Board and Corporate Leadership Team
5.3	08/05/2018	Changes made to reflect the new General Data Protection Regulation 2018

Northumberland
County Council

Table of Contents

Northumberland
County Council

1. Scope

1.1 This policy applies to all Councillors, 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 (the Council).

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).

2. Purpose

2.1 The purpose of this policy is to ensure compliance with the General Data Protection Regulation (GDPR) 2018. This will be achieved by ensuring that personal information is processed as set out in this policy and as required by the GDPR.

2.2 This policy does not intend to replace the GDPR, it merely aims to simplify the content – referral to the regulation may be necessary in order to ensure compliance with requirements and any advice pertaining to this should be sought initially from the Data Protection Officer, Information Governance team and Legal Services Department within NCC.

2.3 This policy is part of a suite of Information Governance policies. A summary of these is provided in the Information Governance Policy Framework.

3. Introduction

3.1 The Council is fully committed to compliance with the requirements of the GDPR, which came into force on the 25th May 2018. It is a legal requirement that the Council complies with the regulation, and all elected members, employees, contractors, agents, consultants, partners or servants of the Council have a statutory responsibility to ensure compliance.

3.2 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, is fully aware of, and abide by their duties and responsibilities under the GDPR.

3.3 In order to operate efficiently, the 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 GDPR to ensure this.

3.4 The 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.

4. Definitions

4.1 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.

4.2 For the purposes of the GDPR, and the Council's Data Protection and Confidentiality 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 Special category data can include information relating to:

- Religious or philosophical belief
- Sexual life or sexual orientation
- health data
- trade union membership
- Political opinions
- Commission or alleged commission of an offence
- Proceedings for any offence committed or alleged to have been committed
- Biometric and genetic data

4.4 Special category 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.

5. The principles of the General Data Protection Regulation (GDPR) 2018

5.1 The seven principles which form the basis of the Regulation provide the foundation for the appropriate control and processing of personal data. They are as follows:

5.1.1 **Principle 1 - Legality, transparency and fairness**
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 **Principle 2 - Purpose limitation**

Personal data should be collected for specified, legitimate and explicit purposes and must not be further processed in a way which is incompatible with such purposes.

5.1.3 **Principle 3 - Minimisation**

The data must be relevant, adequate, and limited to what is necessary in relation to the purposes for which that data is processed.

5.1.4 **Principle 4 - Accuracy**

The personal data must be accurate when recorded, and accuracy must be maintained throughout the lifecycle of the data. Every reasonable step must be taken to update inaccurate personal records.

5.1.5 **Principle 5 - Storage limitation**

Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained.

5.1.6 **Principle 6 - Integrity and confidentiality**

Personal Data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical or organisational measures.

5.1.7 **Principle 7 - Accountability**

Both data controllers and data processors have responsibility for, and must be able to prove and demonstrate compliance with all principles outlined within the GDPR.

6. Handling of special category information

6.1 The Council will through appropriate management and the use of strict criteria and controls.

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

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

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

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

6.1.5 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

6.1.6 Ensure the quality of information used

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

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

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

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

6.1.11 Ensure that the rights of people about whom the information is held can be exercised fully under the Regulation. Please see Section 14.

7. Responsibilities

7.1 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 Regulation by complying with this policy.

7.2 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.

7.3 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 Officer on any issues which may arise.

7.4 The Data Protection Officer will monitor the Council's compliance with the Regulation, 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.

7.5 All data protection breaches must be reported to the Information Governance team immediately from being made aware of the Incident in line with the Security Incident and Data Breach Policy.

8. Processing personal data

8.1 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.

8.2 There is a requirement to inform the general public why the Council needs information about them, how this is used and to whom it may be disclosed.

8.2.1. The Council will ensure that individuals are made aware of personal information being held by the Council and how this information is being used, held, who can access it, with whom it is being shared and for how long it will be kept. This will be by Privacy Notices and will happen where the use of personal information is not obvious.

8.2.2 There is a corporate Privacy Notice on the Council's website. Additional more detailed, service or functional based Privacy Notices will (where applicable) be clearly stated on written literature, on Council web pages and verbally, if individuals are being spoken to face to face or by telephone.

8.2.3 There are instances, as permitted by the Regulation when individuals will not be made aware that their information is being processed, such as when the processing is in connection with the prevention and detection of crime.

8.3 Councillors, 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.

8.4 All forms used to obtain personal data, such as application forms or registration forms must include a Privacy Statement in clear and plain language, providing the following:

8.4.1 Stating the purpose/s for which the information is required, who it will be shared with, how long it will be retained and how it will be destroyed. It should also include a link to a more detailed Privacy Notice. The Data Protection Officer can support teams to write clear Privacy Statements and Privacy Notices.

All personal data obtained, must always:

8.4.2 Be reviewed regularly to check that all of the information asked for is still required and necessary. To ensure we comply with the minimisation principle.

8.4.3 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. To ensure we comply with the accuracy principle.

8.5 Personal data must be collected and handled in a way that complies with the Regulation and meets the seven 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.

8.6 If an outside agency provides data to the Council, the Council has the right to ask the agency to confirm in writing that the data was obtained fairly and lawfully, in compliance with the Regulation.

8.7 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.

9. Data Protection Impact Assessments (DPIA)

9.1 Data Protection Impact Assessments (DPIAs) are carried out on all Council significant decisions and as part of the start of any project, if personal information is involved and there are risks to the privacy of individuals. The DPIA will consider the risks of complying with legislation such as the GDPR and document work required to resolve any design issues, including the alternatives considered and why the option chosen was selected.

9.2 The size of the DPIA should reflect the scale of the project or change and the following questions should be considered when deciding whether or not to carry out a DPIA:

1. Will the project/decision involve the collection of new information about individuals?
2. Will the project/decision require individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
5. Does the project/decision involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition software.
6. Will the project/decision result in you making decisions, or taking action against individuals in ways that can have a significant impact on them? (including automated decisions).
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
8. Will the project/decision require you to contact individuals in ways that they may find intrusive?

10. The purpose of the data/notification to the Information Commissioner

10.1 In addition to obtaining consent, the data must be used only for the declared purpose(s).

10.2 The Information Commissioner maintains a public register of data controllers. The 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 Information Governance web page, the Information Commissioner's website or from the Information Governance Team.

10.3 The Regulation 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.

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

Northumberland
County Council

11. Relevant and adequate data

11.1 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.

12. Collecting and maintaining accurate data

12.1 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. Errors in personal data that could or does cause data subjects damage or distress could lead to the Council being prosecuted.

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

12.3 Users of software will be responsible for the quality (i.e. accuracy, timeliness, and completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

13. Keeping data only as long as necessary

13.1 Retention periods should be defined for personal data and procedures put in place to ensure compliance. Please refer to the Council's Records Management Policy.

13.2 Retention periods must be for clear business purposes/and or legal basis, and this must be documented to identify why certain records are retained for certain periods of time.

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

14. Rights of individuals

14.1 Safeguarding the rights of data subjects

14.1.1 The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification

- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

14.2 Subject access requests.

14.2.1 The Council must make available details of how individuals can request access to their data. This is known as a Subject Access Request (SAR).

14.2.2 Requests for personal information:

- Must be in writing.
- Must explain the information required (we may seek further clarification if this is too broad to enable a successful search).
- Must be accompanied by identification to help prevent fraudulent requests.
- Can be made via a 3rd party, such as a solicitor or someone holding power of attorney, with the permission of the data subject.

14.2.3 The council may be entitled to refuse any requests on procedural grounds such as when the above points are not complied with.

14.2.4 If we are able to release the information we will collate it, advise of the source and generally provide a permanent copy. We aim to provide it within 1 month as required by the regulation.

14.2.5 If we decide to deal with a request for information under another information request regime or as a combination of regimes we will advise accordingly. An example is when a request for the non-personal information is made under the Regulation. In this instance the request would be considered under the Freedom of Information Act.

14.2.6 If the information cannot be released within the timeframe there must be a valid reason for the delay, we will advise and requester and they will be kept informed of progress and given access to information as it becomes available. The information provided will be in permanent form, such as a written document, unless we are unable to provide a permanent copy.

14.2.7 If we are unable to provide some or all of the information because, for example it is exempt from disclosure, we will explain in writing within 30 consecutive days.

14.2.8 We will provide advice with each request about how to make a complaint, and how to appeal to the ICO.

14.3 Requests that inaccurate information is rectified, erased, destroyed or blocked

13.3.1 Individuals can ask that inaccurate personal information is corrected or deleted.

14.4 Prevent processing likely to cause damage or distress

14.4.1 Individuals can ask the council to stop handling their personal information if it is causing or is likely to cause substantial damage or distress to that individual or another person.

14.5 Prevent processing for direct marketing

14.5.1 Individuals can ask that their personal information is not used or is no longer used for direct marketing.

14.6 Prevent automated decision taking

14.6.1 Individuals have the right to prevent decisions, which significantly affect them; being made just by automated means.

14.7 Seek compensation

14.7.1 An individual, who suffers damage or distress as a result of the Council not complying with the Regulation principles, is entitled to seek compensation if it can be demonstrated that reasonable care to comply was not taken.

15. Requests for disclosure of personal information by third parties

15.1 The GDPR has an exemption that allows third parties to request personal information in some circumstances.

15.2 Personal information may be disclosed to a third party under the GDPR if the request is in connection with, for example for the prevention or detection of crime.

15.4 Other requests by third parties

15.4.1 We will only provide information to third parties if there is a legal requirement to do so or as part of a data sharing agreement in line with our corporate Privacy Notice.

16. Keeping data secure

16.1 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 the Council's Information Security and Transportation and Transfer and Sharing of Data Policy for further information on how we protect the data we hold.

16.2 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 GDPR.

17. Transfer of data

17.1 Data must not be transmitted or transferred out of the European Economic Area (i.e. the EU member states) unless the country they are being transferred to has the same or equivalent standards of Data Protection. Prior to any transfer of personal data, a legal agreement must be put in place and approved by the Information Commissioner's Office (Supervisory Authority, UK). This has implications for data placed on the Internet and use of email where servers are based abroad.

17.2 If information is required to be transferred abroad then advice on this process should be sought from the Data Protection Officer in the first instance.

18. Training and awareness

18.1 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 statutory training will be provided on an annual basis.

18.2 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. The Data Protection Officer can advise on appropriate training where this need is identified.

18.3 When staff and Councillors join the Council, it is important that they are introduced to their basic responsibilities under the GDPR. To ensure that they are aware, they will need to complete a mandatory learning module on the GDPR.

Northumberland
County Council

19. Compliance

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

20. Implementation

20.1 This policy is effective immediately.

21. Monitoring and review

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

22. Useful contacts

Data Protection Officer: Informationgovernance@northumberland.gov.uk

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