

NORTH NORFOLK DISTRICT COUNCIL

DATA PROTECTION POLICY

Revised 09.09.11

1. Purpose of Data Protection Policy

The Data Protection Act 1998 (“the Act”) sets out a framework of rights and duties which safeguard personal data. Personal data is information relating to a living individual who can be identified from the data. The Act balances the legitimate needs of organisations to collect and process data against the rights of individuals to respect for their privacy.

North Norfolk District Council (“the Council”) is committed to ensuring compliance with the Data Protection Act 1998. The Council recognises the importance of personal data to its business and the importance of respecting the privacy rights of individuals. This Policy sets out the principles which it will apply to the processing of personal data so that the Council not only safeguards one of its most valuable assets but also process personal data in accordance with the law.

It is the responsibility of all of the council’s employees, Members and any person holding or processing personal data on behalf of the Council (“relevant persons”) to comply with this Policy. In order to assist with compliance, the Data Protection Officer has produced a [Data Protection Guidance document](#) (‘the Guidance’) which explains in more detail the requirements of the Act. Employees and relevant persons should familiarise themselves both with this Policy and Guidance and apply the provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to the dismissal of staff. In regard to Members, this could amount to a breach of the Code of Conduct for Members. Serious breaches could also result in personal criminal liability. This policy continues to apply to individuals even after their relationship with the Council ends.

In addition, a failure to comply with this Policy could expose the Council to enforcement action by the Information Commissioner or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

For these reasons, it is important that all employees and relevant persons familiarise themselves with this Policy and Guidance and attend all training sessions in respect of care and handling of personal data.

The Information Commissioner who oversees compliance and promotes good practice requires all data controllers who process personal data to be responsible for their processing activities and comply with the 8 Data Protection Principles of “good information handling”.

Data controller means: ...” a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.” The term person comprises not only individuals but also organisations such as companies and other corporate bodies of persons.

The Data Protection Principles:

The Act sets out eight principles to be complied with when personal data is processed. These principles are as follow:

- (1) Personal data shall be processed fairly and lawfully.
- (2) Personal data shall be obtained only for one or more specified and lawful purposes and must not be further processed in any manner incompatible with those purposes.
- (3) Personal data shall be adequate, relevant and not excessive.
- (4) Personal data shall be accurate and where necessary kept up-to-date.
- (5) Personal data shall not be kept for longer than is necessary.
- (6) Personal data shall be processed in accordance with the rights of data subjects. These rights are:
 - The right of subject access
 - The right to prevent processing likely to cause damage or distress
 - The right to prevent processing for purposes of direct marketing
 - The right to object to automated decision-taking
- (7) Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- (8) Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This policy applies to all personal data held by the Council however it is collected, recorded and used and whether it is on paper records, in computer records including the information gathered on CCTV systems at whatever location used by or on behalf of the Council.

In this Policy, “processing” means

Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-

- (a) Organisation, adaptation or alteration of the information or data,
- (b) Retrieval, consultation or use of the information or data,

(c) Disclosure of the information or data by transmission, dissemination or otherwise making available,

(d) or alignment, combination, blocking, erasure or destruction of the information or data.

and “processed” shall be construed accordingly.

2. Impact of the Data Protection Act

This Policy applies to all those who have access to personal data held by the Council not just employees but also agency staff, elected Members, contractors and consultants or other servants or agents of the Council.

3. Confidentiality and Security

Employees and relevant persons must not access, copy, alter, interfere with or disclose personal data held by the Council without official authorisation.

Access to and use of personal data held by the Council is only permitted to employees and relevant persons for the purpose of carrying out their official duties. Use for any other purpose is prohibited and any breach may result in disciplinary or legal proceedings.

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles. Confidential information can be the most valuable asset of a business and employees will automatically have duties to their employers to ensure that confidential information is not knowingly or recklessly misused. Individuals that process personal data must comply with the Council’s security measures to safeguard personal data as outlined in the Council’s ICT Policy.

Any employee or relevant person who becomes aware of a weakness in the Council’s data protection procedures or who becomes aware of any breach of the policy must report the concern to their line manager at the earliest opportunity.

4. Preventing abuse and discrimination

The Council processes **sensitive personal data** (as defined in the Act) on employees and services users. The Council will have regard to its various diversity and equality policies to ensure that if instances of data discrimination occur, appropriate action is taken.

Sensitive Personal Data

Consists of the following information as to:

- A racial or ethnic origin of the data subject
- Their political opinions/beliefs
- Their religious beliefs or other beliefs of a similar nature
- Trade Union membership
- Physical or mental health condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed.

Sensitive personal data is subject to much stricter conditions of processing.

5. Recording and Using the Data

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject.

The Council will endeavour to inform all individuals of why their personal data is being collected. In line with the first Data Protection principle, all information will be collected fairly and lawfully and processed in line with the purpose for which it has been given. The Council may need to hold and process the information in order to carry out any statutory obligations, where this process takes place all personal data will be processed fairly and lawfully.

The Council will endeavour to ensure that information kept is accurate and relevant. Where it is found that information is inaccurate, remedial steps will be taken.

Personal data will be kept no longer than is necessary and will be kept securely.

The Council can also process personal data if it has the consent of the data subject.

6. Obtaining

It is a requirement of any data collection form used in order to collect personal data will contain a **“fair obtaining”** or **“privacy”** statement. The statement will need to be clearly visible on this form and placed appropriately so the data subject (individual to whom the information

relates) is fully aware of the intended uses of their personal data. The information that will need to be supplied on a data collection form is as follows:

- The identity of a data controller or appointed representative
- A purpose or purposes for which the information is intended to be processed
- Any foreseen disclosures for the information to be obtained; and
- Any further information in order to make the processing fair.

Suggested statement when taking information from people.

The Council will use the information about you on this form to (detail of service/function) e.g. assess your housing needs

The Council delivers a range of services for the benefit of you and the local community. The personal information you provide may be shared between Council departments and other agencies where we are legally required to do so.

We have a duty to handle this information responsibly and to respect your privacy. Please ask any member of staff for details of our Data Protection Policy or view it at <http://www.northnorfolk.org>

It is also very important to remember that when collecting data via the telephone or face-to-face the above information should also be made clear to the data subject before any processing of personal data takes place.

7. Disclosing

Personal data must not be disclosed to anyone internally or externally, unless the person disclosing the information is fully satisfied that the requestor is authorised and legally entitled to the information.

Personal data may be disclosed to authorised persons if required under one of the **exemptions** within the Data Protection 1998.

These exemptions are:

- National Security
- Crime and Taxation
- Orders made in relation to health, education and social work
- Regulatory activity
- Processing for the special purposes
- Research, history and statistics
- Information made available to the public by or under enactment
- Disclosures required by law

- Disclosures made in connection with legal proceedings
- Domestic purposes (personal data processed only for the purposes of that individual's personal, family or household affairs) and

These exemptions are contained within The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (S.I. No 419).

8. The Right of Subject Access (Sections 7-9)

A written request received by a data controller (i.e. North Norfolk District Council) from an individual wishing to access the rights under the provisions of the Data Protection Act 1998 is known as a **subject access request**. Sections 7 - 9 of the Act gives an individual the right to request access to any "personal data" that they believe may be held about them. The Council may charge a fee of up to £10 for every request and will require proof of ID.

If the Council does hold the requested information, then it will provide a written copy of the information held by them and details of any disclosures which have been made. The information requested will be provided promptly and in any event within 40 calendar days of receipt of the subject access. If the information cannot be disclosed within the time period specified, the data subject will be kept fully informed of the process and given access to any personal data that may already have been gathered. There are some circumstances where the information requested contains information that relates to another person. Unless the other person gives their permission, or it is reasonable in all the circumstances to provide the information without permission, the Council is entitled to withhold this information. There are other circumstances where the Council can withhold information under the Act. For example, if it would put at risk a criminal investigation or catching an offender.

If the data subject believes that North Norfolk District Council has not responded correctly and is not happy with the Council's response for concerns they are able to complain to the Information Commissioner Office (ICO).

The ICO is the UK's independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken.

9. Further Information, Enquiries and Complaints

North Norfolk District Council

The Council's Data Protection Officer, Cara Jordan, is the first point of contact on any of the issues mentioned in this policy document. The Data Protection Officer will be responsible for dealing with all individual and external enquiries. All service areas will have a nominated Data Protection Contact Officer also known as the Freedom of Information Contact to create a network to assist the Council's Data Protection Officer when responding to subject access requests.

Data Protection Officer
North Norfolk District Council
Legal Services
Holt Road
Cromer
Norfolk NR27 9EN

Telephone: 01263 516373

Email: cara.jordan@north-norfolk.gov.uk

Information Commissioners Office

If you think you have a data protection problem, for example, if you have been denied any of your rights, including your right to see the information the Council holds about you, or if the information about you is used, held or disclosed then you have a right to complain to the ICO. You should fill in the 'Data Protection Act complaint form'. You can download the form from www.ico.gov.uk. This should help you give the ICO all the information it will need or you can ask for a copy from their Helpline on 01625 545 745.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF