DATA PROTECTION POLICY

PREAMBLE

The processing of personal data by Newcastle City Council is essential to many of its services and functions, and this processing will often involve *sensitive* personal data. Compliance with the Data Protection Act 1998 will ensure that this processing is carried out fairly and lawfully.

Both the Data Protection Act and Article 8 of the Human Rights Act 1998 stress that the processing of personal data needs to strike a balance between, on the one hand, the needs of the organisation to function effectively and efficiently and, on the other, respect for the rights and freedoms of the individual. This policy sets out how Newcastle City Council will ensure that those rights and freedoms will be protected.

The Data Protection Act extends the data protection regime to cover manually held data in addition to data held on computer databases. Therefore, this policy applies to the acquisition and processing of all personal data within the City Council, whatever the format.

KEY DEFINITIONS

The Data Protection Act is in many ways a very technical piece of legislation. This policy incorporates a number of key terms used in Act, and these are defined below.

Personal data
Personal data includes any information relating to a living individual who can be identified from the data. This can include not only personal details, details of family and social circumstances, education, employment, business and financial details, but also goods or services received, expressions of opinions or intentions, and images such as those recorded on CCTV.

Processing of personal data
Processing is defined very widely in the Data Protection Act. It covers all actions and processes involved in the obtaining, recording, holding, carrying out any set of operations, storing or destroying such data.

Data subject
A data subject is any individual about whom personal data is held by another person or organisation.

THE POLICY

We will comply with all requirements of the Data Protection Act, and will meet the notification and transitional period deadlines. We will also comply with Article 8 of the Human Rights Act in respect of personal data processing.

We will aim to follow best practice in all our personal data processing.

We will keep individuals informed of the purposes for which we are processing personal data, and will seek their consent where possible and appropriate. Where data is used for another purpose, individuals will be informed of this. We will also provide general information to the public on their rights under data protection legislation.

We will hold the minimum personal data necessary to carry out the City Council's functions, and every effort will be made to ensure its accuracy. Where we record opinions or intentions, these will be carefully and professionally expressed. Data which is no longer required will be securely destroyed.

A risk assessment will be undertaken for all personal data processing, and technical and organisational security measures taken, appropriate to the level of risk identified. Processing will comply with the City Council's Information Security Policy, and we will follow the Code of Practice contained in British Standard 7799 (Information Security Management) where appropriate. Personal data will only be transferred by e-mail when it has been encrypted.

We aim to respond to all requests from individuals to access their personal data within the timescale set down in the Data Protection Act 1998. We can only respond to such requests:

where they are received in writing;
which are specific in the information they request;
which provide adequate information to be able to locate the data requested; and
which are accompanied by the relevant fee where appropriate.
We will charge the statutory maximum fee of £10 for subject access requests where the request is for information in more than one service area, or is a repeat request within 12 months of the original request. Requests for educational records will be charged in line with the scale of charges set down in the legislation.
We will only use personal data for the direct promotion or marketing of goods or services with the consent of the individual.

Data sharing with external agencies will be carried out under a written agreement setting out the scope and limits of the sharing, and the safeguards to be put in place. Any disclosure of personal data will be in compliance with approved procedures.
We will only use data matching techniques for specific purposes, and in line with published Codes of Practice. Where personal data is intended to be used for data matching, individuals will be informed of this.

The Data Protection Act allows exemptions from subject access, providing information to individuals, and non-disclosure of information, in specific and limited circumstances. We will normally only invoke an exemption where it is deemed necessary to the effective operation of the City Council, for the prevention and detection of crime, to protect the individual, or is required by law.

The City Council reserves the right to intercept and monitor the content of telephone calls, e-mails and Internet access in compliance with the Lawful Business Practice Regulations 2000. This will be subject to the Information Commission's Code of Practice on Employer/Employee Relationships.

Elected Members and staff will be trained to an appropriate level in the use and control of personal data.

Breaches of this policy will be subject to action under the City Council's disciplinary procedure.

IMPLEMENTATION

Designated Data Protection Officers have been identified in all Directorates, and they will be responsible for ensuring that the policy is implemented. Implementation will be monitored by the Corporate Information Governance Officer, and Internal Audit will review the procedures in place to ensure that the policy is implemented.