

Introduction:

This policy sets out Northwards Housing obligations under the Data Protection Act (1998) as an organisation that collects personal data on individuals. The Act came into force on the 1st March 2000. Unfamiliar terms are defined in the jargon buster on page 4. This policy is accompanied by the 'Data Protection Guidance For Staff' document.

Purpose:

To provide the legislative background to the 'Data Protection Guidance For Staff' document and set out Northwards' obligations and commitments regarding personal data.

Scope of the policy:

1.0 The eight principles of data protection

Northwards Housing will comply with the **Eight Principles** of good practice in data protection. The following principles apply to all business procedures and activity. These eight principles are legally enforceable and state that data:

1. Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate

level of data protection.

The act makes a distinction between **personal data** and **sensitive personal data**.

Personal data is defined as data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexuality;
- Criminal proceedings or convictions.

2.0 Handling of personal/sensitive information

Northwards Housing will:

- Meet its legal obligations by specifying the purpose for which information is used;
- 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;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information (while inputting data from paper based documents, these will have to be locked away until they are ready to be put on the system);
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised 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 days;
- The right to prevent processing in certain circumstances;

- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, Northwards will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with; acknowledged within 7 working days (in line with Northwards' Service Standards) and requested data provided within 40 days;
- Methods of handling personal information are reviewed and evaluated;
- Performance with handling personal information is reviewed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All Board members must be fully aware of this policy and of their duties and responsibilities under the Act.

All staff within Northwards will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other manual records containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- If taking data electronically out of the office, it must be encrypted using TrueCrypt software. It is the responsibility of the officer removing data from Northwards (or between Northwards' different office locations) to seek the advice from the ITC team, if necessary, prior to the removal of any data.
- TrueCrypt should also be used to securely send information electronically (either by email, USB stick or CD) to parties outside of Northwards' Housing. Data must be encrypted and arrangements made with the intended recipients of the data to have access to relevant software and passwords to enable them to access the data. In all cases passwords must be sent separately from the data.

- Individual passwords should be such that they are not easily compromised.

All contractors, consultants and partners of Northwards must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of Northwards, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of the Act will be deemed as being a breach of any contract between Northwards and that individual, company, partner, organisation or firm;
- Allow data protection audits by Northwards Housing of data held on its behalf (if requested);
- Indemnify Northwards against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by Northwards will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by Northwards.

3.0 Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

4.0 Jargon Buster

Data Subject This is the living individual who is the subject of the personal information (data).

Data Controller A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Processing Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Information Commissioner The Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information.

Responsibility:

All members of staff have responsibility for data protection. If we receive a request verbally, in person or in writing from an individual or an organisation, then this policy as well as the information laid out in the document 'Data Protection – Guidance For Staff' will apply.

Performance Standards:

Northwards will comply with all of the above guidance. Managers will be required to audit their service checking every point within their service where data is collected or processed. The data check list form provided in the guidance for staff will help to complete the task and assist in periodic audits.

After each section is audited, managers will be in a position to ensure that data is collected, stored and destroyed in line with the Data Protection Act.

The Data Controller is the Head of Business Improvement who has day-to-day responsibility for ensuring Northwards Compliance with the policy.

Equality /Diversity considerations:

As with all newly implemented policies the data protection policy will go through the Equality Impact Assessment screening.

Generic Impact and risk assessments:

6 months after the policy has been agreed by the Resource and Audit sub committee, an impact assessment will be completed to assess the effectiveness of the policy.

Information sources and reference documents:

Linked document 'Data Protection - Guidance for Staff' and 'Subject Access Request flow chart'.

More information at <http://www.ico.gov.uk/>

Policy information:

This policy is linked to:	'Data Protection Policy: Staff Guidance'
This version:	1.0
Approved by:	
Next review:	
Lead Officer:	Marc Whalley
Policy reference number: (to be completed by	

Business Improvement Team)	
---------------------------------------	--