Wyre Forest District Council

Data Protection Policy 2009-2011

Wyre Forest District Council is accountable to and holds personal data on behalf of the community it serves. For the purposes of this Policy, "personal data" means information, opinions or intentions held manually or electronically, which relate to a living individual ("the data subject") and from which that individual can be identified.

1. Introduction

1.1 Wyre Forest District Council needs to collect and use certain types of information about living individuals in order to carry on its business and meet its customers' requirements. This includes data about current, past and prospective employees, suppliers and clients/customers.

1.2 Data takes many forms. It can be stored on computers, transmitted across networks, printed or written on paper, or recorded. Appropriate security should be applied to all forms of data, however it is stored.

1.3 Data security relates to:

- Confidentiality: Protecting personal data from unauthorised disclosure.
- Integrity: Safeguarding the accuracy and completeness of information.
- Availability: Ensuring that information and vital services are available to users when required.

2. Background

2.1 The Data Protection Act 1998 (the Act) contains eight data protection principles which must apply; these are set out in **Appendix 1**. The Council takes any action necessary to ensure compliance with these principles.

2.2 Where 'sensitive' personal data is collected, Wyre Forest District Council takes the necessary steps to ensure that explicit written consent is obtained from the data subject for this information to be held, used and retained. 'Sensitive' personal data is defined as data about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs;
- membership of a trade union;
- physical or mental health;
- sex life;
- commission or alleged commission of any offence; and
- any court proceedings relating to the commission of an offence including the verdict in any such proceedings and any sentence passed by the court.

2.3 The Council is required to notify the Information Commissioner of its processing of personal data. The notification includes:

- a description of the purpose(s) for which the data is to be used;
- the categories of data subjects about whom data will be held;
- the classes of people or organisations to which information may be disclosed;
- limitations as to any overseas transfer of data that may be required.

2.4 It is an offence to process personal data contrary to the notification.

2.5 Notification does not legitimise processing which would otherwise be unlawful.

2.6 Personal data must not be disclosed, except to authorised users, other organisations and people who are pre-defined as a notified recipient or if required under one of the exemptions within the Data Protection Act 1998.

2.7 The Act gives rights to individuals in respect of personal data held about them by others. The rights are:

- Right of access by an individual (data subject) to any data being held about that individual by an organisation (data controller) that is using that data (Subject Access Request);
- Right of the data subject to prevent use of any data likely to cause damage or distress;
- Right of the data subject to opt out of any direct marketing;
- Right of the data subject to prevent use of any data in unauthorised or inappropriate automated decision-taking.
- Right of the data subject to take action to claim compensation if the individual suffers damage as a result of a contravention of the Act by the data controller; and
- Right of the data subject to take action to rectify, block, erase or destroy inaccurate data held by a data controller.

3. <u>Scope</u>

3.1 The Data Protection Act 1998 is part of a family of legislation governing access to information including the Freedom of Information Act 2000, Environmental Information Regulations and Re-use of Public Sector Information Regulations.

3.2 The Freedom of Information Act 2000 provides a legal right to any individual to ask for access to information held by a public authority. There is a duty to respond to all requests, telling the enquirer whether or not the information is held and supplying the information that is held, except where a legal exemption applies.

3.3 Requests for information about anything relating to the environment – such as air, water, land, the natural world or the built environment and any factor or measure affecting these – are covered by the Environmental Information Regulations (EIRs). Requests are dealt with in the same way as for those made under the FoIA, but unlike the FoIA, **requests do not need to be written and can be verbal**.

3.4 The Re-use of Public Sector Information Regulations allows individuals or organisations to request information from a public body which, if supplied, they can then, with the permission of that public body, re-use for their own commercial gain. This includes publishing, copying, adapting, developing, adding value, broadcasting and downloading. The Council can choose whether to allow the re-use free of charge or to apply a fee to cover reasonable costs in addition to a reasonable return on any investment.

4. Responsibilities

4.1 The Chief Executive is responsible for ensuring compliance with the Data Protection Act 1998. Each Head of Service is responsible for the management of information including the security of information in their division.

4.2 The Council's Cabinet will identify a Cabinet Member to take responsibility for data protection within the Cabinet and the Council.

4.3 The Chief Executive will nominate an officer to take responsibility for the management of Subject Access Requests received under the Act and the Head of Legal and Democratic Services will provide all relevant legal advice and support. All employees who receive a Subject Access Request will forward such a request to the Chief Executive's nominated officer for recording and resolution according to the requirements of the Act.

5. Obligations and Duties

5.1 The Council has a duty to ensure that the rights of people about whom personal data is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken and why; the right of access to one's personal data; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase personal data that is inaccurate.);

5.2 The Council has a duty to ensure that forms requiring the provision of personal data will contain a 'fair obtaining' statement giving details of why the information is required and what it will be used for. Where personal data is collected in person or by telephone, employees who are requesting the details will inform the individual why the data is required and how it will be used and will make a written record that they have done so unless a written statement to the same effect has

already been given. The data subject's consent will only be relied upon where it is freely given, specific and informed;

5.3 The Council has a duty to ensure that the minimum amount of personal data is held to enable it to perform its functions and all data is only used for purposes directly concerned with the Council's business;

5.4 The Council has a duty to ensure that the Office of the Information Commissioner receives appropriate notification of all data processing;

5.5 The Council has a duty to ensure that employees do not process personal data outside the scope of the specific categories and purposes notified to the Office of the Information Commissioner;

5.6 The Council has a duty to ensure that checks are applied to control the length of time personal data is held. Any such data which becomes irrelevant or excessive (over time or by virtue of changed circumstances) will be deleted;

5.7 The Council has a duty to ensure that only authorised employees access personal data and that precise instructions are given as to the limits of their authorisation to use and disclose that data;

5.8 The Council has a duty to ensure that everyone managing and handling personal data is informed of their obligations and liabilities under the Act;

5.9 The Council has a duty to ensure that employees receive training regarding their responsibilities under the Act, the Council's own procedures and the proper use of equipment and systems;

5.10 The Council has a duty to ensure that everyone who manages or handles personal data receives appropriate supervision;

5.11 The Council has a duty to ensure that relevant employees are made aware of all council policies, codes of practice and information-sharing protocols related to the Act;

5.12 The Council has a duty to ensure reasonable steps are taken to ensure the reliability of employees authorised to access personal data;

5.13 The Council has a duty to ensure that where data is to be processed by anyone other than employees of the Council, adequate security and monitoring measures are in place and a written contract is in force that complies with the requirements of the Data Protection Act 1998;

5.14 The Council has a duty to ensure that appropriate security arrangements are in place to ensure that employees who are not authorised to access personal data are unable to do so;

5.15 The Council has a duty to ensure that no personal data in any form is removed from council premises unless authorised by a Head of Service. Such authorisation may only be given where the authorising officer is satisfied that there will be no contravention of data protection legislation;

5.16 The Council has a duty to ensure that where the authorised removal of personal data from council premises takes place, employees are made aware of the appropriate security precautions that need to be observed when travelling. Such precautions will include not leaving such data in whatever media unattended in public places;

5.17 The Council has a duty to ensure that personal information is not transferred outside of the European Economic Area without suitable safeguards;

5.18 The Council has a duty to ensure that enquiries from data subjects are dealt with promptly and courteously and that a complaints mechanism is available;

5.19 The Council will provide advice and assistance to anyone making a Subject Access Request to ensure that the requester is provided with the information required. This will include helping enquirers to put such requests into writing so that they can be handled under the Act;

5.20 The Council will provide advice and assistance on request to the visually impaired or to individuals that do not use English as their first language;

5.21 The Council has a duty to ensure that operational practices and procedures provide adequate opportunity for data subjects to notify the council where personal data needs to be brought up to date;

5.22 The Council has a duty to ensure that a nominated Data Protection Officer will have responsibility for data protection matters within the Council; and

5.23 The Council has a duty to ensure that compliance with this policy is regularly assessed and maintained.

6. <u>Employee Responsibilities</u>

6.1 Employees must not access, copy, alter, interfere with or disclose personal data held by the Council without official authorisation. An employee who does so will be subject to disciplinary action which could lead to dismissal and/or legal proceedings.

6.2 An employee who becomes aware of a weakness in the Council's data protection practices must report that weakness to their line manager or Head of Service without delay.

6.3 An employee who becomes aware of the violation of any security procedures by a third party must report the violation to their line manager or Head of Service without delay.

6.4 An employee who loses their council identity card must report the loss to their line manager or Head of Service without delay.

6.5 Any employee who ceases to be employed by the Council, or any elected Member who ceases to act in their capacity as a councillor must return all identity cards, permits, access cards, manuals, equipment and other Council property before they leave the Council.

6.6 Keys for secure areas, safes and cabinets must be held in a secure place and must not be given to unauthorised individuals.

6.7 Employees must ensure that all personal data provided to the Council is accurate and up to date. Any change of address etc. must be notified to the Head of Human Resources without delay.

7. Dealing with Requests

7.1 The Council will respond to subject access requests according to the the requirements of the Act and the procedures laid down in **Appendix 2**.

8. Charging

8.1 The Council will charge a standard fee of £10 for the administration of a Subject Access Request as provided for within the Act.

9. Training

9.1 Wyre Forest District Council is committed to training its employees so that they understand the law, their responsibilities and are able to respond to Subject Access Requests. The Council will ensure that all new employees receive relevant training and that existing employees receive refresher training.

10. Complaints

10.1 Any member of the public that is dissatisfied with the Council's management of personal data or way that the Council has handled a Subject Access Request must, in the first place, complain to the Council using its complaints procedure.

10.2 If, following the exhaustion of the Council's own complaints procedure the member of the public is still dissatisfied, he/she may take their complaint to the Information Commissioner at:

Agenda Item No. 8.1
Appendix A

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

Telephone: 01625-545745
Website: http://www.ico.gov.uk/complaints/freedom_of_information.aspx

March 2009