Wyre Forest District Council

Data Protection Policy

Date of adoption 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.
- Security: Taking appropriate technical and organisational measures against accidental loss or unauthorised processing.

2. Background

2.1 The Data Protection Act 1998 (the Act) contains eight data protection principles which must apply to processing any personal data. The principles are set out in full in **Appendix 1**. In summary Personal Data must be:

- Processed fairly and lawfully.
- Processed for specified and lawful purposes.
- Adequate, relevant and not excessive.
- Accurate and where necessary kept up to date.
- Not kept longer than is necessary.
- Processed in accordance with the rights of the data subject.
- Transferred only to countries with adequate security.
- Kept secure.

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. Scope

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 Data Protection Act protects the confidentiality of personal data by controlling how it may be processed. It providing access rights only to the data subject whilst the other legislation listed above provides access rights to information to the wider public. When considering a request under the other legislation any possible disclosure of personal data must be compliant with the Data Protection Act., note particularly the exemption to personal data within the Freedom of Information Act 2000.

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 Leader of the Council 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 a data subject (listed at para. 2.7) can be fully exercised under the Act

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. Employee Responsibilities

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 Director 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 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:

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

Date of adoption 2011.

Wyre Forest District Council

Data Protection Policy

Appendix 1

The Eight Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
    - at least one of the conditions in **Schedule 2** (below) is met; and
    - in the case of sensitive personal data, at least one of the conditions in **Schedule 3** (below) is also met.

2. Personal data 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. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

7. Appropriate technical and organisational measures shall 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 shall 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.

NB. The European Economic Area is the 15 member countries of the European Union plus Iceland, Liechtenstein and Norway.

Date of adoption 2011

Schedule 2 to the Data Protection Act 1998

Conditions Relevant for Purposes of the First Principal: Processing of any Personal Data

1. The data subject has given his consent to the processing.

2. The processing is necessary:
   - for the performance of a contract to which the data subject is a party; or
   - for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary:
   - for the administration of justice;
   (aa) for the exercise of any function of either House of Parliament.
   - for the exercise of any functions conferred on any person by or under any enactment;
   - for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
   - for the exercise of any other functions of a public nature exercised in the public interest by any person.

6.1 The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

6.2 The Secretary of State may by order specify particular circumstances in which this condition is, or is not to be, taken to be satisfied.

Date of adoption 2011

Schedule 3 to the Data Protection Act 1998

Conditions Relevant for Purposes of the First Principal: Processing of Sensitive Personal Data

1. The data subject has given his explicit consent to the processing of the personal data.

2.1 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

2.2 The Secretary of State may by order:
- exclude the application of sub-paragraph 2.1 in such cases as may be specified; or
- provide that, in such cases as may be specified, the condition in sub-paragraph 2.1 is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary:
   - in order to protect the vital interests of the data subject or another person in a case where:
     i) consent cannot be given by or on behalf of the data subject; or
     ii) the data controller cannot reasonably be expected to obtain the consent of the data subject; or
   - in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing:
   - is carried out in the course of its legitimate activities by any body or association which:
     i) is not established or conducted for profit; and
     ii) exists for political, philosophical, religious or trade-union purposes;
   - is carried out with appropriate safeguards for the right and freedoms of data subjects;
   - relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
   - does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing:
    - is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
    - is necessary for the purposes of obtaining legal advice; or
    - is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7.1 The processing is necessary:
- for the administration of justice;
  (aa) for the exercise of any function of either House of Parliament;
- for the exercise of any functions conferred on any person by or under an enactment; or
- for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

7.2 The Secretary of State may by order:
- exclude the application of sub-paragraph 7.1 in such cases as may be specified; or
- provide that, in such cases as may be specified, the condition in sub-paragraph 7.1 is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7.3 The processing:
is either:
- the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or
- any other processing by that person or another person of sensitive personal data so disclosed; and
- is necessary for the purposes of preventing fraud or a particular kind of fraud.

7.4 In this paragraph "an anti fraud organisation" means any unincorporated association, body corporate or other person which enables or facilities any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8. The processing is necessary for medical purposes and is undertaken by:
- a health professional; or
- a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

8.1. In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. The processing:
   - is of sensitive personal data consisting of information as to racial or ethnic origin;
   - is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
   - is carried out with appropriate safeguards for the rights and freedoms of data subjects.

9.1. The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph 9.1a and 9.1b is, or is not, to be taken for the purposes of sub-paragraph 9.1c to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Date of adoption 2011

Wyre Forest District Council

Data Protection Policy

Appendix 2

1. Procedure for Dealing with Requests

1.1 Individuals have a right under the Data Protection Act 1998 to make a request in writing for a copy of the information held about them on computer and in some manual filing systems. This is called a subject access request. They are also entitled to be given a description of the information, what you use it for, who you might pass it on to, and any information you have about the source of the information.

1.2 To handle a subject access request under the Data Protection (DP) Act (the Act) the nominated officer will need to ask a series of questions. These are set out below and shown on pages 4 and 5 as process maps.

2. Is it a Subject Access Request?

2.1 A request for information may be covered by one, or all, of three information rights:

- A Data Protection enquiry (or Subject Access Request) is where the enquirer asks to see his or her personal information held by the Council. If the enquiry is a Data Protection request, the Council must follow its Data Protection Act guidance.
- An Environmental Information Regulations enquiry relates to air, water, land, natural sites, built environment, flora and fauna, and health, and any related decisions and activities. These could therefore include enquiries about recycling, phone masts, pollution, car parking etc. If the enquiry is about environmental information, the Council must follow its guidance on dealing with a request for information under the Environmental Information Regulations.
- A Freedom of Information enquiry is concerned with all other information and the reasoning behind decisions and policies. The request does not have to mention the Freedom of Information (FoI) Act. All requests for information that are not data protection or environmental information requests are covered by the FoI Act.

3. Has the requester's identity been checked?

3.1 Where a Subject Access Request is made it is critical that the information is given to the correct person. Wyre Forest District Council will request proof of identity before the search for relevant data is progressed.

4. Is more information required to enable an efficient search?

4.1 By engaging promptly with the requester, the Council can ensure that the appropriate information is provided.

4.2 A requester may sometimes ask to be supplied with all his/her personal data held by the Council where in fact the focus of the request is a specific service, for example a benefits case or correspondence focusing on a particular issue.

5. How much can we charge?

5.1 The Council follows the guidance of the Information Commissioner and charges a fee of £10.

6. Is the Council obliged to supply the information?

6.1 There may be circumstances where the Council is not obliged to supply certain information. If there are any concerns with the releasing of information, this must be discussed with the Council's legal officers who will determine whether any of the information held about the requester is exempt.

7. Could a third party's interests be affected by disclosure?

7.1 Consultation with third parties may be required if their interests could be affected by release of the information requested. Any such consultation may influence the decision. Consultation is not required where the information is not going to be disclosed due to the application of an exemption.

7.2 Consultation will be necessary where:

- disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights:
- the views of the third party may assist in the determination as to whether information is exempt from disclosure, or

7.3 Even where the third party's information should not be disclosed, as much information as possible can still be supplied by editing the references to the third party.

7.4 Even where the third party has not consented to the release of the information requested, it may be reasonable, given full consideration of all the circumstances, to provide the information to the requester. The reasoning behind any decision in such a case must be fully documented and not taken without the agreement of the Council's nominated legal officer.

8. Is there a time limit for replying to the enquirer?

8.1 Compliance with a request must be prompt and within the legally prescribed limit of 40 calendar days. Failure to comply with the statutory timescale could result in a complaint to the Information Commissioner.

8.2 The 40 day response time starts when the fee has been paid, the identity of the requester has been proven and all the information necessary to deal with the request has been received.

9. For how long are records retained that contain personal data?

9.1 Normally, records containing personal data are only kept for as long as is required by law after the service provided has ceased. Where there is no legal requirement to keep the information it is not normally kept for more than six years, however, in some cases it can be destroyed as soon as is practicable.

10. What if the information provided is incorrect?

10.1 If a requester believes that his/her personal data held by the Council is incorrect, the requester can contact the Council's nominated Data Protection Officer and ask for the information to be corrected. The Council must contact the requester with 21 days to advise as to whether the amendments have, or have not been made.

10.2 If the Council does not agree that the information held about the requester is incorrect, the requester can ask for his/her disagreement to be noted on the record itself.

11. What happens if someone complains?

11.1 Any written (including email) expression of dissatisfaction – even if it does not specifically seek a review – should be handled through the Council's existing complaints procedure which should be fair, impartial, clear and non bureaucratic. Wherever practicable the review should be handled by someone not involved in the original decision.

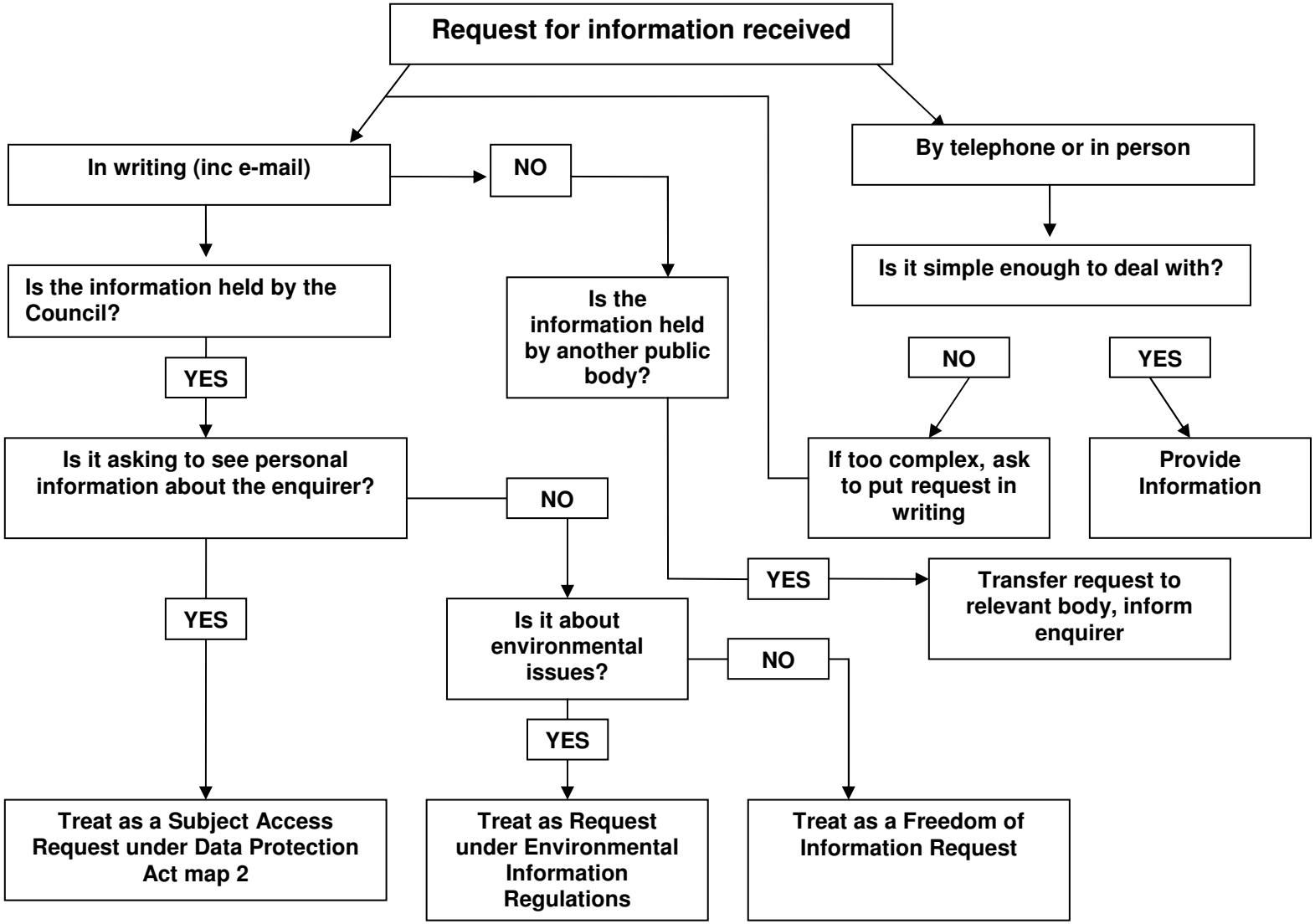
11.2 When an original request has been reviewed and the outcome is that information should be disclosed when the original decision was to withhold, this should be done as soon as practicable. When the outcome upholds the Council's original decision or action, the applicant should be informed of their right to appeal to the Information Commissioner at:

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
Date of adoption 2011

Process Map 1 for Dealing with Requests



Process Map for Handling a Subject Access Request