Report to Cabinet

Date: 14 December 2006

Author: Head of Legal and Democratic Services

Subject: Data Protection Policy

---

1. **Purpose of the Report**

To approve the policy for Data Protection.

2. **Background**

Since the introduction of the Data Protection Act 1998 (DPA) in October 2001 and the Freedom of Information Act 2000 the Council's previous policy on Data Protection required up dating.

The DPA is intended to deal with the collection, recording and use of personal information whether on paper or held on computer. The Act also ensures safeguards are put in place to deal with the processing of personal information.

The DPA and the guidance issued suggests that an Authority maintain a policy with which the Council can operate which should be publicly available as a publication or on the website. Attached at **Appendix 1** is a draft of the Data Protection Policy for discussion.

3. **Resource Implications**

None.

4. **Recommendation**

Members are asked to approve the Data Protection Policy.

APPENDIX 1

GEDLING BOROUGH COUNCIL

DATA PROTECTION POLICY STATEMENT

1. Scope of the Policy

The Council needs to collect and use certain types of information about people with whom it deals in order to operate and provide services to the residents of the Borough. These include current, past and prospective employees, suppliers, clients, customers and others with whom it communicates.

This personal information must be dealt with properly however it is collected, recorded and used, whether on paper, held on a computer, or recorded on other material and there are safeguards to ensure this in the Data Protection Act 1998 ("the Act").

Gedling Borough Council recognises its responsibilities regarding the information it holds about people and is committed to upholding the principles of the Act and shall:

- Ensure that all officers understand their responsibilities regarding the Act and that they receive the appropriate training/instruction and supervision to enable them to comply fully with the Data Protection Act Principles;
- Hold no more personal information than is necessary to enable it to perform its functions, and the information will be erased once the need to hold it has passed.
- Seek to ensure that information is accurate, up-to-date, and that inaccuracies are corrected without unnecessary delay.
- Ensure that there are sufficient safeguards and controls in place for security of data.
- Ensure requests for access to personal data will be dealt with promptly and appropriately, ensuring that either the person requesting the data or their authorised representative has a legitimate right to access and that the request is clear and unambiguous. The Council will determine what fee, if any, is to be charged for this service, in accordance with the Council's Requests for Information Charging Policy (currently £10)
- Ensure for notification purposes that the Council's nominated representative is informed of the details of all systems containing personal data and of any subsequent amendments likely to affect notification.

Status of the Policy

This policy statement has been adopted by the Council and was approved by the [Cabinet] on

2. Definitions

Data controller
A person or organisation who makes decisions with regard to personal data, including decisions regarding the purposes for which and the manner in which personal data may be processed.

Data processor
An individual or organisation other than an employee of the data controller who processes personal data on behalf of the data controller: e.g. a firm which collects and processes data on the Council's behalf under contract. Data controllers are responsible for the processing which is carried out for them by data processors, and have to ensure that this processing takes place within appropriate security arrangements (see 9.Security of Data).

Data subject
A living individual who is the subject of personal data.

Direct marketing
The communication of advertising or marketing material directed to particular individuals.

Manual data
Personal data which are not being processed by equipment operating automatically, or recorded with the intention that they should be processed by such equipment: e.g. data held in paper form.

Personal data
Data relating to a living individual who can be identified from the data, or from the data and other information which is in the possession of (or likely to come into the possession of) the data controller. Personal data include information such as an individual's name, home and work addresses, educational background, images and photographs (including CCTV footage), expressions of opinion about the individual, and the intentions of the data controller with regard to the individual.

Processing
Any operation on personal data, including obtaining, recording, holding, organizing, adapting, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying and otherwise using the data.

Public Authority
Has the same meaning as in the Freedom of Information Act 2000.

Relevant filing system
A filing system for paper or other manual data which has been constructed in such a way that specific categories of information relating to a particular individual are readily accessible.

Sensitive personal data
Personal data relating to racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences, and criminal proceedings.

Third parties
An individual or organisation other than the data subject, the data controller or a data processor acting on behalf of the data controller.

Vital interests
Although not defined in the Act, the Information Commissioner has advised that "vital interests" should be interpreted as relating to life and death situations: e.g. the disclosure of a data subject's medical details to a hospital casualty department after a serious accident.

3. Overview of the Data Protection Act

The Data Protection Act 1998 commenced on 1 March 2000, with most of its provisions being effective from 24 October 2001. It replaced and broadened the Data Protection Act 1984. The purpose of the Act is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their consent wherever possible. The Act covers personal data relating to living individuals, and defines a category of sensitive personal data which are subject to more stringent conditions on their processing than other personal data.

The Data Protection Act covers data held in electronic formats, and also applies to manual data which are held in what the Act calls a relevant filing system. While this might appear to limit the categories of non-electronic data to which the Act applies, the definitions of personal data in the Data Protection Act have been broadened by the Freedom of Information Act 2000 in respect of public authorities like the Council to which the Freedom of Information Act applies. The main effect of this is that since 1 January 2005 (when the Freedom of Information Act came into force), unstructured personal information held by the Council in manual form - i.e. not in a relevant filing system - is covered by the Data Protection Act, except for unstructured data relating to appointments, removals, pay, discipline and other personnel matters, which remain outside the scope of the Act.

The Council is a data controller in respect of the data for which it is responsible. This means that the Council is responsible under the Act for decisions with regard to the processing of personal data, including the decisions and actions of external data processors acting on the Council's behalf. The Act requires that processing should be

carried out according to eight Data Protection Principles. These are outlined below, together with the Council's commitments to upholding these Principles:
Data Protection Principles

(a) Personal data shall be processed fairly and lawfully.
The Council will ensure that data are obtained fairly, and will make reasonable efforts to ensure that data subjects are told who the data controller is, what the data will be used for, for how long the data will be kept and any third parties to whom the data will be disclosed. In order for processing to be fair and lawful, data which is not sensitive personal data will only be processed by the Council if at least one of the following conditions, set down in the Act, has been met:

- The data subject has given his/her consent to the processing.
- The processing is necessary for the performance of a contract to which 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.
- The processing is required under a legal obligation other than a contract.
- The processing is necessary to protect the vital interests of the data subject.
- The processing is necessary for the administration of justice, any functions of either Houses of Parliament, the exercise of functions under an enactment, the exercise of functions of the Crown or a government department, or any other functions of a public nature exercised in the public interest.
- The processing is necessary to pursue the legitimate interests of the Council or of third parties, and does not prejudice the rights, freedoms or legitimate interests of the data subject.

Processing of sensitive personal data is subject to more stringent restrictions under the Act. Processing of sensitive personal data will only be carried out by the Council if at least one of the above conditions, applicable to non-sensitive data, has been met. **In addition**, at least one of the conditions, set down in the Act at Schedule 3, must **also** be met, examples of these are:

- The data subject has given his/her explicit consent.
- The processing is required by law for employment purposes.
- The processing is necessary to protect the vital interests of the data subject or another person.
- The information has been made public by the data subject.
- The processing is required for the administration of justice, legal proceedings, the defending of legal rights, the exercise of functions under an enactment, or the exercise of functions of the Crown or a government department.

- The processing is necessary for medical purposes, and is carried out by a health professional or a person with an equivalent duty of confidentiality.
- The processing is necessary for equal opportunities monitoring.

Data relating to the disabilities of officers and other individuals are sensitive personal data under the Data Protection Act.

(b) Personal data shall be obtained only for a specified and lawful purpose or purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.
The Council will ensure that data which are obtained for a specified purpose are not used for a different purpose, unless that use is done with the consent of the data subject, is covered by the Council's registration with the Information Commissioner, or is otherwise permitted under the Act.

(c) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
The Council will not collect personal data which are not strictly necessary for the purpose or purposes for which they were obtained.

(d) Personal data shall be accurate and, where necessary, kept up to date.
The Council will take reasonable steps to ensure the accuracy of personal data which it holds, and will take steps to correct inaccurate data when requested to do so by a data subject.

(e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
The Council will ensure that personal data are not kept for longer than is required by the purpose or purposes for which the data were gathered. The Council may retain certain data indefinitely for research purposes (including historical or statistical purposes), as permitted under the Act, subject to the conditions laid down in the Act for this type of processing.

(f) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
The Council will ensure that personal data are processed in accordance with the rights of data subjects under the Act. These rights include the right to:

- Make subject access requests (see 13.Access to data) to find out what information is held about them, the purposes for which it will be used, and to whom it has been disclosed.
- Prevent the processing of data which is likely to cause them substantial damage or substantial distress
- Prevent processing for the purposes of direct marketing.
- Be informed about automated decision making processes that affect them.

- Prevent significant decisions that affect them from being made solely by automated processes.
- Seek compensation if they suffer damage through contravention of the Act.
- Take action to require the rectification, blocking, erasure or destruction of inaccurate data.
- Request an assessment by the Information Commissioner of the legality of any processing that is occurring.

(g) Appropriate technical and organisational measures shall be taken to prevent the unauthorised or unlawful processing of personal data and the accidental loss, destruction of or damage to personal data.
The Council will take steps to ensure the security of personal data which are held electronically and in manual form, to prevent the unauthorized disclosure of data to third parties, and loss or damage to data that may affect the interests of data subjects. The Council will also ensure that data processors provide an appropriate level of security for the personal data which they are processing on the Council's behalf (see 9. Security of data).

(h) 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.
The Council will not transfer data outside the European Economic Area unless the transfer would be permitted under the Act (see 7. Transferring data outside the EEA).

The Act requires bodies which record and use personal information to register with the Information Commissioner. The Council's registration details are included in the Public Register of Data Controllers which is available on the website of the information Commissioner (www.esd.informationcommissioner.gov.uk\esd.search.asp, the Council's notification number is Z7097798) It records the purposes for which the Council gathers personal data, the types of data subjects covered by each purpose, the classes of data gathered, recipients to whom the data will be disclosed, and countries or territories to which the data may be transferred. Any use by the Council of personal data must be in accordance with the terms of the Council's registration.

Information about how the Council processes data relating to its employees is contained in the Staff Handbook.

Further information about the Act is available on the website of the Information Commissioner (www.informationcommissioner.gov.uk)

4 General Responsibilities of Council Officers

The Council as a corporate body is a data controller under the Act. The Senior Solicitor deals with day to day Data Protection matters, such as subject access requests (see

13.Access to data), and is a point of contact for issues relating to Data Protection (see 15. Data protection contacts).

When processing personal data, Council Officers must ensure that they abide by the Act, this policy and any related policies (see 14. Related guidelines and policies). In practice, most routine uses of personal data will be covered by the Council's registration with the Information Commissioner. However, this will not necessarily be the case where changes are introduced to the way in which data are processed - such as using the data for a purpose for which the data have not previously been used, or transferring the data to a new source.

Before such changes are introduced, staff should check to ensure that the proposed changes will be in accordance with the Council's registration with the Information Commissioner, and will comply with the Act and this policy. Officers who are uncertain as to whether their processing of data meets these requirements should refer any queries to their Head of Service, Head of Unit or line manager in the first instance. Officers should also ensure that any personal information for which they are responsible is accurate and up to date, including information which the Council holds about themselves (e.g. their home address), and that data for which they are responsible are kept secure and are not disclosed to unauthorised parties.

Data should only be transferred internally within the Council when there is a genuine business need to do so. Officers who receive transferred data are equally responsible for ensuring that the data are processed in accordance with this policy and the Council's obligations under the Act.

Heads of Service or Head of Unit are responsible for ensuring that the processing of personal data in their department conforms to the requirements of the Act and this policy. In particular, they should ensure that new and existing officers who are likely to process personal data are aware of their responsibilities under the Act. This includes drawing the attention of officers to the requirements of this policy, and ensuring that officers who have responsibility for handling personal data are provided with adequate training.

Managers must also see that correct information and records management procedures are followed in their departments (see 12. Records management). This includes establishing retention periods to ensure that personal data are not kept for longer than is required (see 11. Retention of data).

Officers should also note that the Council is not responsible for any processing of personal data by them which is not related to their employment with the Council, even if the processing is carried out using the Council's equipment and facilities. Officers are personally responsible for complying with the Act in regard to data for which they are the data controller.

5. Gathering Data

Any gathering of personal data by members of the Council must be in accordance with the Council's registration with the Information Commissioner (see 3.Overview of the Data Protection Act 1998). Officers should check the register before introducing any new form of data gathering or making changes to existing methods of data gathering. If it appears that the collection of the data would not be covered by the Council's existing registration, the Senior Solicitor must be informed before the changes are implemented, so that the Council's register entry can be updated (see 15. Data Protection Contacts).

While it is not always necessary to have the consent of the data subject in order for the processing of data to be fair and lawful, it is advisable to seek consent wherever possible, particularly with regard to sensitive personal data where explicit consent should normally be obtained (see 3. Overview of the Data Protection Act 1998).

Paper and electronic forms (including web based forms) created by the Council which gather personal data should normally include a statement explaining:

- Why the data needs to be gathered.
- How the data will be used.
- The parts of the Council that will use the data.
- Any third parties outside the Council to whom the data will be disclosed or transferred.
- How long the data will be kept.
- The fact that completion of the form will be taken as consent by the data subject to the use of the data as outlined.
- How the data subject can exercise his/her rights under the Data Protection Act (e.g. by linking to the Council's Data Protection pages or by providing contact details for the Council's Senior Solicitor).

Forms and other methods of data collection should not gather more data than are necessary for the task at hand. Officers who are responsible for the design of forms should ensure that there is a clear business need for each data item requested. Otherwise, the form should be amended to remove the data item.

Data subjects have the right to prevent the processing of their data for direct marketing purposes (e.g. promotional mailshots). If personal data gathered via a form is to be used for direct marketing, the form must also include:

- A statement explaining how the data will be used for direct marketing.

- Information on how the data subject can opt out of the use of the data for that purpose (e.g. by ticking a box).
- Where direct marketing is involved, the form should indicate that it is assumed that the data subject consents to the use of the data for direct marketing purposes unless he/she specifies otherwise.

6. Disclosure of Data

Officers must take particular care when disclosing personal data to third parties, to ensure that there is no breach of the Act or the law of confidence. When dealing with third parties, before data is processed, officers must satisfy themselves that any necessary consents have been obtained

Disclosure may be unlawful even if the third party is a family member of the data subject, or a local authority, government department or the police. A key point to consider is whether the disclosure is relevant to and necessary for the conduct of the Councils business. For example, it would generally be appropriate to disclose a officers work contact details in response to an enquiry relating to a function for which they are responsible, but it would not be reasonable or appropriate to disclose a staff member's personal address or bank account details.

The disclosure of personal data represents a form of processing of the data. This means that the conditions for fair and lawful processing of personal data and sensitive personal data set out in first Data Protection Principle must be met (see 3. Overview of the Data Protection Act 1998). Consideration should also be given as to whether the disclosure was one of the purposes for which the data were originally gathered; in particular, whether the disclosure is covered by the Council's entry in the Information Commissioner's Public Register of Data Controllers, or is a purpose to which the data subject has consented. If not, the disclosure is likely to represent further processing contrary to the second Data Protection Principle.

The Act also allows personal data to be disclosed to third parties without the consent of the data subject, in the following circumstances:

- The disclosure is necessary for safeguarding national security.
- The disclosure is necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders.
- The disclosure is necessary for the assessment or collection of any tax or duty.
- The disclosure is necessary for the discharge of regulatory functions (including the health, safety and welfare of people at work).
- The data are information which the Council is obliged by legislation to provide to the public.

- The disclosure of the data is required by legislation, rule of law or the order of a court.
- The Freedom of Information Act 2000 (FOI Act) sets out certain circumstances in which personal data can be disclosed to a third party (i.e. someone other than the data subject) who has submitted a Freedom of Information request. In particular, the FOI Act provides that personal data can be disclosed where doing so would not breach any of the Data Protection Principles (see 3. Overview of the Data Protection Act 1998). Guidance from the Information Commissioner suggests that this is likely to apply to data relating to an individual's official or work capacity which it would normally be reasonable to release, such as name, job title, official functions, grade, decisions made in an official capacity, and salaries of senior officers.

FOI requests for the release of personal data to third parties need to be handled according to the rules set down in the FOI Act, which are different from those in the Act. Any release of personal data in response to an FOI request should be cleared in advance with the Council's Senior Solicitor (see 15. Data Protection Contacts).

Officers should always exercise caution when dealing with requests from third parties for the disclosure of personal data. Disclosure requests should be in writing, and should be responded to in writing. Where reasonable, the party making the request should be required to provide a statement explaining the purpose for which the data is requested, the length of time for which the data will be held, and an undertaking that the data will be held and processed according to the Data Protection Principles.

Where the request relates to the prevention/detection of crime, the apprehension /prosecution of offenders, assessment/collection of any tax or duty, or the discharge of regulatory functions, appropriate paperwork should be produced by the enquirer to support their request (e.g. official documentation stating that the information is required in support of an ongoing investigation). Guidance for staff on how to respond to requests for data from the police and similar agencies is available in the Jupiter in Nottinghamshire Data Sharing Protocol Environmental Health Enforcement Protocol.

Personal data should only be disclosed over the telephone in emergencies, where the health or welfare of the data subject would be at stake. If data have to be disclosed by telephone, it is good practice to ask the enquirer for their number and to call them back. If an officer is unsure about disclosure the matter should be referred to their Line Manager or Head of Service before disclosure is made.

7. Transferring Data Outside the EEA

The eighth Data Protection Principle requires that personal data must not be transferred outside the European Economic Area (the European Union member states plus Iceland, Norway and Liechtenstein), unless the country or territory to which the data are to be transferred provides an adequate level of protection for personal data.

The European Commission has recognised a number of non-EEA countries which it deems to provide an adequate level of protection for personal data. Transfer of data to these countries will not violate the eighth Data Protection Principle. Similarly, the eighth Data Protection Principle will not be violated if transfer occurs in the following circumstances:

- The data is transferred to a company in the United States which has signed up to the 'Safe Harbour' agreement (a set of rules similar to those found in the UK's data protection law).
- The transfer is made under a contract which includes the model clauses adopted by the European Commission to ensure that there will be adequate safeguards for data transferred to a source outside the EEA.
- Further information about the EC's list of approved countries, the 'Safe Harbour' agreement and the EC's model contractual clauses is available on the website of the Information Commissioner.

8. Publication of Data

The Council routinely publishes a number of items that include personal data, and will continue to do so. These include staff information (such as name, department, job title, email address and telephone number) in the Council's Year Book, the Council Directory and Council's websites; and other information connected with annual reports, the Gen, intranet, guides, etc.

Any individual who has good reason for wishing their details in such publications to remain confidential should contact the Council's Senior Solicitor (see 15. Data Protection Contacts).

9. Security of Data

The seventh Data Protection Principle requires that precautions should be taken against the physical loss or damage of personal data, and that access to and disclosure of personal data should be restricted. Officers of the Council who are responsible for processing personal data must ensure that personal data are kept securely, and that personal information is not disclosed orally or in writing, by accident or otherwise, to unauthorised third parties.

Manual data

- When not in use, files containing personal data should be kept in locked stores or cabinets to which only authorised staff have access.
- Procedures for booking files in and out of storage should be developed, so that file movements can be tracked.

- Files should be put away in secure storage at the end of the working day, and should not be left on desks overnight.

Electronic data

Care must be taken to ensure that PCs and terminals on which personal data are processed are not visible to unauthorised persons, especially in public places. Screens on which personal data are displayed should not be left unattended. Particular care must be taken when transmitting personal data.

As well as preventing unauthorised access, it is equally important to avoid the accidental or premature destruction of personal data which could prejudice the interests of data subjects and of the Council.

Personal data in both manual and electronic formats should only be destroyed in accordance with the Council's File Retention and Disposal Policy (see 11. Retention of data). Care must be taken to ensure that appropriate security measures are in place for the disposal of personal data. Manual data should be shredded or disposed of as confidential waste, while hard drives, disks and other media containing personal data should be wiped clean (e.g. by reformatting, over-writing or degaussing) before disposal.

The Act lays particular obligations on data controllers to ensure that there are adequate safeguards for processing which is carried out on their behalf by data processors. Whenever personal data is to be processed by an external body acting on the Council's behalf, the Council must:

- Choose a data processor which provides sufficient guarantees in regard to its technical and organisational security measures;
- Take reasonable steps to ensure that the data processor complies with these measures, and
- Ensure that the processing takes place under a written contract which stipulates that the processor will act only on instructions from the Council, and that the processor will have security measures in place that ensure compliance with the seventh Data Protection Principle.

10. Confidential References and Recruitment

Confidential references for employment purposes will involve the disclosure of personal information, often of a private nature. Officers who are requested to provide references in their work capacity must ensure that they do so in accordance with the Council's Staff Handbook.

References given by a data controller are exempt from data subject access requests under the Data Protection Act (see 13.Access to data). In practical terms, this means that the Council is under no obligation to disclose the data contained in copies of

references given by Council officers. However, references received by a data controller are not exempt from subject access requests.

Officers involved in recruitment and selection should be aware that information in documents such as interviewers' notes could potentially be disclosed to data subjects in response to access requests. Officers should therefore ensure that any feedback which is provided to candidates after interview is consistent with and can be supported by the documentation relating to the recruitment and selection process, including the person specification. Feedback should be provided in a manner which complies with the Council's Recruitment Procedures/Staff Handbook.

11. Retention of Data

The Act does not specify periods for the retention of personal data. It is left to data controllers to decide how long personal data should be retained, taking into account the Data Protection Principles, business needs and any professional guidelines. In the context of the Council, the following factors need to be taken into consideration:

- The need to balance the requirement of the fifth Data Protection Principle - that personal data should not be kept for longer than necessary - against the need to prevent the premature or accidental destruction of data which would damage the interests of data subjects, contrary to the seventh Data Protection Principle.
- The exemptions provided by the Act which allow the permanent retention of data for historical and statistical research. The Council's history should not be endangered by the overzealous destruction of data that could be retained as historical archives.
- The fact that the Act does not override provisions in other legislation (e.g. health and safety legislation) which specify retention periods for personal data.

Officers should note that under the Freedom of Information Act, it is a criminal offence to deliberately alter, deface, block, erase, destroy or conceal data which has been the subject of an access request under the Data Protection Act or the Freedom of Information Act with the intention of preventing the release of the data. However, data may be amended or deleted after receipt of the access request but before disclosure of the data, if the amendment or deletion would have taken place regardless of the request (e.g. under a retention and disposal policy).

12. Records Management

Effective management of paper and electronic records is essential for compliance with the Act and other legislation, such as the FOI Act. In the context of Data Protection, good records management ensures that personal data contained in records:

- Can be located in response to subject access requests and business needs.
- Are protected from accidental loss or destruction.

- Are retained according to established retention periods.
- Are secured against unauthorised access and disclosure.
- Are preserved for future use, where necessary, in formats suitable for long-term preservation.

Heads of Service or Head of Unit are responsible for ensuring the effective management of records in their sections. To assist managers in these functions reference should be made to the Records Retention and Disposal Policy

13. **Access to Data**

The Act gives data subjects the right of access to personal data which the Council holds about them. Anyone who wishes to exercise this right should apply in writing to the Senior Solicitor. The Council charges a fee (currently £10.00) for each Data Subject Access Request, and requires proof of identity to prevent the unlawful disclosure of personal data.

The Council will respond to subject access requests as quickly as possible, and is required by law to respond within 40 days of receipt of the request, fee and proof of identity. In some cases, the Council may not release information because the data are subject to exemptions under the Data Protection Act, or doing so would release personal data relating to other individuals.

If the requested data are located and can be released, the data subject will normally be provided with the information in permanent form on paper: e.g. as a printout, photocopy, transcript or transcription.

Officers who receive a request which they believe to be a request for data under the Act should pass the request on to their departmental representative. Under no circumstances should officers deliberately alter, conceal or destroy data which has been the subject of an access request in order to prevent the release of the data (see 11.Retention of data).

14. Related Guidelines and Policies

The following guidelines and policies are also relevant to the implementation of Data Protection at the Council:

- Data Protection Act: Requesting Access to Personal Data
- Freedom of Information Charging Policy
- Information Commissioner – Compliance Guidance
- Records Management Policy
- Jupiter in Nottinghamshire Data Sharing Protocol

- Staff Handbook
- Nottinghamshire Food Liaison Group – Joint Enforcement Protocol with Trading Standards
- Policy governing the operation of CCTV

15. Data Protection Contacts

Data Protection enquiries should be directed to the Council's Senior Solicitor at the following address:

Senior Solicitor
Legal and Democratic Services
Gedling Borough Council
Civic Centre
Arnot Hill Park
Arnold
Nottingham
NG5 6LU

Telephone: 0115 9013896
Fax: 0115 9013920
Email: anita.Bradley@gedling.gov.uk