Data Protection Policy

Document Management:

Action	Date	Responsible Party
V1.3 Approved	2 February 2016	Cabinet
V1.4 Formatting and proofreading amendments.	21 November 2018	Sabrina Doherty

1.0 Scope of the Policy

1.1 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.

1.2 This personal information must be dealt with and used in a correct and lawful manner regardless of the method of collection. This policy applies to all records of personal information, whether on paper, on computer or on any other material. The General Data Protection Regulations 2016 ("GDPR") and the Data Protection Act 2018 ("the Act") provide safeguards to ensure all personal information is collected and used in a lawful fair and transparent manner.

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

- Ensure that all officers understand their responsibilities regarding the GDPR and the Act and that they receive regular mandatory appropriate training/instruction and supervision to enable them to comply fully with the Data Protection Principles.
- Hold no more personal information than is necessary to enable it to perform its functions, and the information will be securely destroyed or 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.
- Ensure for notification purposes that the Council's Data Protection Officer or their deputy is informed of the details of all systems containing personal data and of any subsequent amendments likely to affect notification.
- Ensure that all reportable data breaches are reported to the Information Commissioner's Office within 72 hours of the Council becoming aware of the breach.

2.0 Definitions

2.1 Data breach

2.1.1 The accidental or deliberate unauthorised access, loss, destruction or damage of personal data which is likely to result in a risk to the rights and freedoms of natural persons.

2.2 Data controller

2.2.1 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.

2.3 Data processor

2.3.1 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 12.Security of Data).

2.4 Data subject

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

2.5 Direct marketing

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

2.6 Manual data

2.6.1 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.

2.7 Personal data

2.7.1 Any information relating to an identified or identifiable natural person. An identifiable natural person is on who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.8 Processing

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

2.9 Special categories of personal data

2.9.1 Personal data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation.

2.9.2 For the purpose of the policy personal information relating to criminal convictions and offences will be treated as being special categories of personal data.

2.10 Third parties

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

2.11 Vital interests

2.11.1 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.

3.0 Overview of the data protection legislation

3.1 The GDPR and the Act commenced on 25 May 2018. They replaced and broadened the Data Protection Act 1998. The purpose of the GDPR and 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 GDPR has a much greater focus on individuals and what rights they have over their personal data. It places a greater emphasis on transparency and requires the Council to have and maintain clear documentation and records to demonstrate accountability. The GDPR makes best practice a legal requirement and affords more rights to the data subject so the data subject can make informed decisions about how and why their personal data is processed. The GDPR and the Act cover personal data relating to living identifiable individuals, and defines special categories of personal data which are subject to more stringent conditions on their processing than other personal data.

3.2 The GDPR and the Act apply to all personal data regardless of whether it is held in electronic or paper form. The GDPR and the Act also recognise online indicators and activities, such as I.P addresses and location data, as personal data.

3.3 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 GDPR and 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 GDPR and the Act require that processing should be carried out according to six data protection principles. These are outlined below, together with the Council's commitments to upholding these principles:

4.0 Data Protection Principles

4.1 **Personal data** shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)

4.1.2 The Council will ensure that personal data is obtained fairly and that the Council has a lawful basis for processing. 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 within the relevant privacy notices. In order for processing to be fair and lawful, data which is not within the special categories of personal data will only be processed by the Council if at least one of the following conditions, set down in Article 6 of the GDPR, 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 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.
- The processing is required under a legal obligation to which the Council is subject.
- The processing is necessary to protect the vital interests of the data subject or of a natural person.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.

4.1.3 Processing of special categories of personal data is subject to more stringent restrictions under the GDPR. Processing of special categories of personal data will only be carried out by the Council if at least one of the above conditions, applicable to personal data, has been met. **In addition**, at least one of the conditions, set down in Article 9 of the GDPR relating to special categories of personal data, must **also** be met, examples of these are:

- The data subject has given his/her explicit consent.
- The processing is necessary for the purpose of carrying out obligations and exercising specific rights of the controller or the data subject in the field of employment.
- The processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.
- The processing is carried out in the course of legitimate activities relating to trade union membership.
- The information has been made manifestly public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for the purpose of preventive or occupational medicine, for the assessment of the working capacity of the employee,

medical diagnosis, the provisions of health or social care or treatment or the management of health and social care systems.

- The processing is necessary for reasons of public health.
- Processing is necessary for archiving in the public interest, scientific or historical research purposes.

4.2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (purpose limitation)

4.2.1 The Council will ensure that personal data which is obtained for a specified purpose are not used for a different purpose, unless that use is done with the consent of the data subject. The data subject will be informed of the purposes for which their personal data will be used in the privacy notice given at the time of collecting their personal data, or is otherwise permitted under the GDPR and the Act.

4.3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (data minimisation)

4.3.1 The Council will not collect personal data which are not strictly necessary for the purpose or purposes for which they were obtained.

4.4 Personal data shall be accurate and, where necessary, kept up to date. (accuracy)

4.4.1 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.

4.5 Personal data shall be kept in a form which permits identification of the data subject for no longer than is necessary for that purpose. **(Storage limitation)**

4.5.1 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 GDPR and the Act, subject to the conditions laid down in the GDPR and the Act for this type of processing. Where deletion of personal data is not possible the Council will anonymise any records containing personal data.

4.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing of personal data and the accidental loss, destruction of or damage to personal data using appropriate technical or organisational measures. (Integrity and confidentiality)

4.6.1 The Council will take steps to ensure the security of personal data, held electronically and in manual form, to prevent the unauthorised 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 12. Security of data).

5.0 General Responsibilities of Council Officers

5.1 The Council as a corporate body is a data controller under the GDPR and the Act. The Data Protection Officer and their deputy deals with day to day data protection matters, ongoing compliance with the GDPR and the Act, and is a point of contact for issues relating to data protection (see 17. Data protection contacts).

5.2 When processing personal data, Council Officers must ensure that they abide by the GDPR and the Act, this policy and any related policies and any data processing or information sharing agreements (see 16. Related guidelines and policies). In practice, most routine uses of personal data will be covered by the Council's privacy notices. 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.

5.3 **Before** such changes are introduced, staff must carry out a Data Protection Impact Assessment (DPIA) in consultation with the Data Protection Officer to ensure that the proposed changes will comply with the GDPR, the Act and this policy. Staff will also ensure that any changes are in accordance with the Council's privacy notices and are included on the Information Asset Register for the service area. Officers who are uncertain as to whether their processing of data meets these requirements should refer any queries to their Service Manager or line manager in the first instance. If there is any uncertainty as to whether the processing is covered by the Council's privacy notices then the Data Protection Officer and/or their deputy must be contacted before any changes to the processing can occur. 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.

5.4 Data should only be transferred internally within the Council when the privacy notice makes it clear that this is how personal data will be processed and the Council has a lawful basis to process under the GDPR and the Act. 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 GDPR and the Act.

5.5 Service Managers and line managers are responsible for ensuring that the

processing of personal data in their department conforms to the requirements of the GDPR, 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 attend mandatory training.

5.6 Service Managers must also see that correct information and records management procedures are followed in their departments (see 14. Records management). This includes complying with established retention periods to ensure that personal data are not kept for longer than is required (see 13. Retention of data).

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

6.0 Gathering Data

6.1 Any gathering of personal data by officers of the Council must be in accordance with the GDPR, the Act and the Council's privacy notices and the six data protection principles. (see 3.Overview of the data protection legislation). The Data Protection Officer and/or their deputy must be informed of any changes to or new forms of gathering data before they are implemented, so that the Data Protection Officer can advise whether a Data Protection Impact Assessment is required and ensure the Council's privacy notices are updated (see 17. Data Protection Contacts).

6.2 The majority of the processing of personal data carried out by the Council will be carried out under the ‘Public Task’ and/or ‘Legal Obligation’ lawful basis. However there will be occasions where consent of the data subject is required in order for the processing of their personal data to be fair and lawful. Where this is the case consent must be freely given, informed and a clear indication from the data subject that they consent to the processing is required to comply with the GDPR and the Act. (see 3. Overview of the data protection legislation).

6.3 **Paper and electronic forms** (including web based forms) created by the Council which gather personal data must include a short-form privacy statement explaining:

- Why the data needs to be gathered.
- Gather only the personal data required for the business need and not request excessive personal data.

- The lawful basis for processing contained within Article 6 of the GDPR, and where special categories of personal data are being collected the lawful basis under Article 9.
- The fact that completion of the form will be taken as consent by the data subject to the use of the data as outlined.
- The contact details of the Council and the Council's Data Protection Officer; and
- refer to the relevant privacy notice on the Council's website.

  (A template short-form privacy notice is available from the Data Protection Officer and/or their deputy).

6.4 Privacy notices on the Council's website will explain in detail

- Why the data needs to be gathered.
- The lawful basis for processing contained within Article 6 of the GDPR, and where special categories of personal data are being collected the lawful basis under Article 9.
- 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.
- 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 Data Protection Officer).

6.5 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.

6.6 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** contain a tick box to actively opt in to receive marketing communications. The form must also include:

- A statement explaining how the data will be used for direct marketing.
- Information on how the data subject can remove their consent to the use of the data for that purpose (e.g. by unsubscribing from emails).
- A short-form privacy notice.

7.0 Disclosure of Data to Third Parties

7.1 Officers must take particular care when disclosing personal data to third parties, to ensure that there is no breach of the GDPR and/or Act or the law of confidence. 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.

7.2 The disclosure of personal data represents a form of processing of the data. This means that the conditions for fair, lawful and transparent processing of personal data and special categories of personal data set out in first data protection principle must be met (see 3. Overview of the data protection legislation). 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 privacy notice and there is a data processing or information sharing agreement in place, 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.

7.3 The GDPR and 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, defence or public security.
- The disclosure is necessary for the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties.
- The disclosure is necessary for the assessment or collection of any tax or duty.
- The disclosure is necessary for the protection off judicial independence and judicial proceedings.
- The disclosure is necessary for the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions.
- The disclosure is necessary for the protection of the data subject or the rights and freedoms of others.
- The disclosure is necessary for the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control.
- 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 legislation). 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.

7.4 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 Data Protection Officer or their deputy (see 17. Data Protection Contacts).

8.0 Individual requests for personal data

8.1 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.

8.2 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 ‘Detailed Employee Guidance on Access to Information’.

8.3 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.

9.0 Regular Data Sharing

9.1 Where information is being disclosed or shared with third parties on a regular basis the GDPR and the Act Require that a data processing or information sharing agreement is in place. Where personal data is being shared in accordance with any agreements the disclosure of that data must be in accordance with the GDPR, the Act and the terms of the relevant processing of sharing agreement.

9.2 The GDPR and the Act lay 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 sixth data protection principle.

10.0 Transferring Data Outside the EEA

10.1 The GDPR 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.

10.2 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 be in breach of the GDPR. Similarly, the GDPR 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 'Privacy Shield' framework 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 'Privacy Shield' agreement and the EC's model contractual clauses is available on the website of the Information Commissioner.

10.3 Officers must ensure appropriate enquires are made to establish where hosted website and private email servers are located before transferring any personal data.

11.0 Publication of Data

11.1 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

Directory and Council's websites; and other information connected with annual reports, the Gen, intranet, guides, etc. this also includes routinely published contact details of Elected members.

11.2 Any individual who has good reason for wishing their details in such publications to remain confidential should contact the Council's Data Protection Officer (see 17. Data Protection Contacts).

12.0 Security of Data

12.1 The sixth 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. Officers must also ensure that they comply with the access controls set out in the Information Security Policy.

12.2 **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.

12.3 **Electronic data**

12.3.1 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.

12.3.2 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.

12.3.3 Personal data in both manual and electronic formats should only be destroyed in accordance with the Council's Records Retention and Disposal Policy (see 13. 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.

13.0 Retention of Data

13.1 The GDPR and the Act do 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, limitation periods, 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 sixth data protection principle.
- The exemptions provided by the GDPR and 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.

13.2 The Council has set out appropriate retention periods in the Records Retention and Disposal Policy.

13.3 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 GDPR 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).

14.0 Records Management

14.1 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.

14.2 Service Mangers 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

15.0 Access to Data

15.1 The GDPR and the Act give 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 Inforequest@gedling.gov.uk . The Council requires proof of identity to prevent the unlawful disclosure of personal data.

15.2 The Council will respond to subject access requests as quickly as possible, and is required by law to respond within 1 calendar month of receipt of the request and proof of identity. Where a request is deemed to be complex, the GDPR allows the Council an additional 2 calendar months to respond to the request. if this is the case the individual will be informed. In some cases, the Council may not release information because the data are subject to exemptions under the Act or doing so would release personal data relating to other individuals.

15.3 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 GDPR should pass the request on to their departmental FOI 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 13.Retention of data).

16.0 Related Guidelines and Policies

16.1 The following guidelines and policies are also relevant to the implementation of data protection at the Council:

- Data Protection Policy – Appropriate Policy Document
- Information Security Policy
- Records Retention and Disposal Policy
- Detailed Employee Guidance on Access to Information
- Freedom of Information Charging Policy
- Information Asset Register
- Any Data Processing or Information Sharing Agreements
- Records Management Policy
- Staff Handbook
- Policy governing the operation of CCTV

17.0 Data Protection Contacts

17.1 Data Protection enquiries should be directed to the Council's Data Protection Officer at the following address:

dataprotectionofficer@gedling.gov.uk

Data Protection Officer
Legal Services
Gedling Borough Council
Civic Centre
Arnot Hill Park
Arnold
Nottingham
NG5 6LU