Atworth Parish Council

Data Protection Policy

1. Introduction

1.1 The 1998 Data Protection Act came into force from 1 March 2000. Atworth Parish Council supports the objectives of the Act and will comply with it.

1.2 The purpose of this policy is to formalise the position of the Council and state its commitment to maintaining confidentiality of personal information within its record systems. Detailed guidelines are attached as an appendix.

1.3 The Clerk to the Council is Atworth Parish Council's nominated Data Protection Officer, to whom all enquiries should be directed.

2. Scope

2.1 The obligations contained in this Policy Statement apply equally to both Council Members and Employee(s).

3. Definitions

3.1 ***Personal Data:*** any data that relates to a living individual who can be identified from that data. This includes any expression of opinion about the individual and any indication of the intentions of the Council in respect of the individual.

3.2 ***Processing:*** processing information or data means obtaining, recording or holding the information or data or carrying out set operations on it, including disclosure.

3.3 ***Data Subject:*** an individual who is the subject of personal data.

4. Policy

4.1 Atworth Parish Council is committed to maintaining the strictest level of confidentiality for any personal data it is responsible for processing. The Council will only process or disclose Personal data for purposes necessary for official Council business and that we have notified to the Data Protection Commissioner. The Council will adhere to the principles outlined in the 1998 Data Protection Act for processing that data.

4.2 We will design computer and manual systems to comply with the principles of the Data Protection Act and will train staff involved in processing personal data accordingly. The eight principles are:

i) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

(1) at least one of the conditions in Schedule 2 of the 1998 Data Protection Act is met:

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

2. The processing is necessary—

(a)for the performance of a contract to which the data subject is a party, or

(b)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—

(a)for the administration of justice,

(b)for the exercise of any functions conferred on any person by or under any enactment,

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d)for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. 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.

(2) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met:

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

2. 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.

3. The processing is necessary—

(a)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

(b)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—

(a)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,

(b)is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c)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

(d)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—

(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b)is necessary for the purpose of obtaining legal advice, or

(c)is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. The processing is necessary—

(a)for the administration of justice,

(b)for the exercise of any functions conferred on any person by or under an enactment, or

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

8. The processing is necessary for medical purposes and is undertaken by—

(a)a health professional, or

(b)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.

9. The processing—

(a)is of sensitive personal data consisting of information as to racial or ethnic origin,

(b)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

(c)is carried out with appropriate safeguards for the rights and freedoms of data subjects.

ii) 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.

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

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

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

vi) Personal data shall be processed in accordance with the rights of data subjects under this Act.

vii) 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.

viii) Personal data shall not be transferred to a country or territory outside of 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.

4.3 The Council carries out its affairs in an open manner. Apart from exceptional circumstances as outlined in the Act, we will make information about a data subject available, upon request, in an intelligible form.

4.4 Where a data subject asks the Council for access to data, the request must be attended by a fee amount of £10, set by the Council, in accordance with the Act.

4.5 The Council will try to hold only the minimum data necessary to perform its business, and will erase or destroy the data in such a manner that confidentiality is maintained. We will try to ensure that data is accurate and up to date, and correct inaccuracies without unnecessary delay.

DATA PROTECTION POLICY GUIDELINES

1. Introduction

1.1. These guidance notes expand on some of the information in the Council's Data Protection Policy, and you should use the two documents together.

1.2. The Data Protection Act 1998 repeals the earlier 1984 Act. The 1984 Act covered data that was "processed by means of equipment operating automatically in response to instructions

given for that purpose", i.e. personal data held on computer systems. The 1998 Act widens the description to include "relevant filing systems" or manual data. Relevant filing systems are "structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".

1.3. The Act reinforces the principles of confidentiality for personal data.

1.4. Note - the Act only covers information that relates to living individuals.

2. Responsibilities

2.1. The Data Protection Officer will notify the Office of the Data Protection Commissioner of the systems in use and their stated purpose.

2.2. New "systems", new uses or changes to "systems" will be notified to the Office of the Data Protection Commissioner before the changes are implemented.

2.3. The Data Protection Officer is responsible for ensuring that notifications are up to date and renewals are effectively processed.

2.4. Every Member and employee of the Council is responsible for keeping to the Data Protection Act 1998 when processing personal data.

3. System Contents

3.1. Only the minimum data necessary to carry out a function will be held. The information held must be relevant to the purpose. For example some systems allow users to make notes, and these facilities must not be used to record remarks that have no bearing on the purpose of the system, especially if such comments are derogatory or they cannot be substantiated.

3.2. Information can be irrelevant if it is held for too long. Information must be both accurate and current. Inaccurate or out of date records must be amended without undue delay.

4. General Access to Personal Data

4.1. When information is gathered either in writing or verbally it is essential that the data subject is told what the information will be used for and to whom else the information may be disclosed. That information cannot then be used for any other purpose or disclosed to any other individual.

4.2. Information must only be provided to the person to whom it relates unless prior consent is obtained. If information identifies someone else who has not consented to their details being disclosed, any details identifying the third party must be removed before releasing any information.

4.3. There is an obvious risk that others may attempt to obtain confidential information relating to someone else. Awareness is particularly important where requests are made over the telephone or if the correspondence address is different from that held on any Council system. Checks must be made to verify the identity of the individual by telephoning the individual back, asking them to confirm something personal such as their account number or by checking an actual signature against others held by the Council.

5. Data Subject Access Request

5.1. The Data Protection Act allows individuals to make a Data Subject Access Request. In such a case an individual is entitled to receive, in an intelligible form, all information held relating to them. There are temporary transitional relief periods for manual records that were already in operation before 24 October 1998. Any new processing from that date must comply with the Act.

5.2. It is essential that both computer and manual systems are designed in such a way that access requests can be dealt with quickly and effectively.

6. Security

6.1. Appropriate measures will be taken to ensure that personal data is secured. In computer operations this includes control over password access and making sure that only authorised persons use the facilities.
6.2. Manual records containing personal data will be accessible only to individuals that have legitimate use for the data. Waste will be disposed of with care with documents shredded when appropriate.

7. Disciplinary Action

7.1. The Council may consider disciplinary action against any Member or Employee who deliberately disregards any provisions of the Data Protection Policy.
7.2. Everyone should also be aware that the Act provides for separate personal liability for any offences in the Act. Where an offence is committed, individuals may be prosecuted and punished accordingly.

ANNEX A - GDPR

GDPR

1. The GDPR (General Data Protection Regulation) will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

3. For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

How can I demonstrate that I comply?

You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - Data minimisation;
    - Pseudonymisation;
    - Transparency;
    - Allowing individuals to monitor processing; and
    - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

You can also:

- Adhere to approved codes of conduct and/or certification schemes. See the section on codes of conduct and certification for more detail.

Records of processing activities (documentation)

As well as your obligation to provide comprehensive, clear and transparent privacy policies (see section on Individual rights), if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

• processing personal data that could result in a risk to the rights and freedoms of individual; or

• processing of special categories of data or criminal convictions and offences.

What do I need to record?

You must maintain internal records of processing activities. You must record the following information. There are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.

- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.