



# Broseley Town Council

## Data Protection Policy

### Introduction

Broseley Town Council needs to collect and use certain types of information about people with whom it deals in order to operate. Information may be processed about employees, councillors, suppliers, residents of the town and others. Where necessary or required the Council sometimes needs to share the personal information with other organisations. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 1998. This policy sets out how Broseley Town Council will process data and comply with the Act.

### Principles of Data Protection

All personal data held by the Council will be processed fairly and lawfully in accordance with the eight principles of data protection as set out below:

#### Principle 1

*Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –*

*(a) at least one of the conditions in Schedule 2 is met, and*

*(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

(see "Conditions for Processing" below)

The Council will:

- a. only collect and use personal data where it has legitimate grounds for doing so;
- b. not use the data in ways that will have unjustified adverse effects on the individuals concerned;
- c. be transparent about how the data is to be used, and give individuals appropriate privacy notices when collecting their personal data;
- d. handle people's personal data only in ways they would reasonably expect; and
- e. ensure that nothing unlawful is done with the data.

#### Principle 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.*

The Council will:

- a. be clear from the outset about why it is collecting personal data and what it intends to do with it;
- b. comply with the Act's fair processing requirements, including the duty to give privacy notices to individuals when collecting their personal data;
- c. comply with what the Act says about notifying the Information Commissioner; and
- d. ensure that if it wishes to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

### **Principle 3**

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

The Council will:

- a. ensure that personal data held about an individual is sufficient for the purpose for which it is held in relation to that individual; and
- b. not hold more information than is needed for that purpose.

### **Principle 4**

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

The Council will:

- a. take reasonable steps to ensure the accuracy of any personal data it obtains;
- b. ensure that the source of any personal data is clear;
- c. carefully consider any challenges to the accuracy of information; and
- d. consider whether it is necessary to update the information.

### **Principle 5**

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

The Council will:

- a. review the length of time that personal data is kept;
- b. consider the purpose or purposes for which the information is held when deciding whether (and for how long) to retain it;
- c. securely delete information that is no longer needed; and
- d. update, archive or securely delete information if it goes out of date.

### **Principle 6**

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

The Council will ensure that individuals have the right to:

- a. access a copy of the information contained in their personal data;
- b. object to processing that is likely to cause or is causing damage or distress;
- c. prevent processing for direct marketing;
- d. object to decisions being taken by automated means;
- e. have inaccurate personal data rectified, blocked, erased or destroyed; and
- f. claim compensation for damages caused by a breach of the Act.

### **Principle 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.*

The Council will ensure that personal data is held securely and will take appropriate measures to:

- a. nominate a specific person to be responsible for data protection, currently the Clerk;
- b. secure personal data so that it can only be accessed by authorised persons;
- c. ensure appropriate policies and procedures are in place and that staff are well trained;
- d. respond to any breach of security swiftly and effectively.

### **Principle 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.*

The Council does not transfer any personal information outside the European Economic Area.

### **\* Conditions for Processing**

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever personal data is processed:

- The individual who the personal data is about has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.

Further information can be found on the website of the Information Commissioner's Office:  
<http://www.ico.org.uk/>

Approved 13<sup>th</sup> May 2014  
Reviewed 14<sup>th</sup> June 2016