

1. POLICY STATEMENT

- 1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information, and we recognise the need to treat it in an appropriate and lawful manner.
- 1.2 The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, hirers of the Tithe Barn, allotment garden holders, and others that we communicate with. The information, which may be held on paper or computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.
- 1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. STATUS OF THE POLICY

- 2.1 This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.
- 2.2 If you consider that the policy has not been followed in respect of personal data about yourself, or others, you should raise the matter with the Parish Council.

3. DEFINITION OF DATA PROTECTION TERMS

- 3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.
- 3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
- 3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as name, address or date of birth) or it can be an opinion (such as a performance appraisal).
- 3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in the business of running the Parish Council.
- 3.5 **Data users** include those whose undertakings involve using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.
- 3.6 **Data processors** include any person who processes personal data on behalf of a data controller.
- 3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising,

amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- (a) Processed fairly and lawfully.
- (b) Processed for limited purposes and in an appropriate way.
- (c) Adequate, relevant and not excessive for the purpose.
- (d) Accurate.
- (e) Not kept longer than necessary for the purpose.
- (f) Processed in line with data subjects' rights.
- (g) Secure.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subjects' explicit consent to the processing of such data will be required.

6. PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Clerk.

10. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- (a) Request access to any data held about them by a data controller.
- (b) Prevent the processing of their data for direct-marketing purposes.
- (c) Ask to have inaccurate data amended.
- (d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. DATA SECURITY

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or they put in place adequate measures themselves.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- (a) **Confidentiality** means that only people who are authorised to use the data can access it.

- (b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- (c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

11.4 Security procedures include:

- (a) **Entry controls.**
- (b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- (c) **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMS should be physically destroyed when they are no longer required.
- (d) **Equipment.** Data users should ensure that individual monitors do not show confidential information and that they log off from their PC when it is left unattended.

12. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them must be made in writing to the Clerk. A fee is payable by the data subject for provision of this information.

13. PROVIDING INFORMATION OVER THE TELEPHONE

Telephone enquiries should be carefully dealt with regarding the disclosure of any personal information held by the Parish Council. In particular:

- (a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- (b) Suggest that the caller put their request in writing if you are not sure about the caller's identity and when their identity cannot be checked.

