HEMYOCK PARISH COUNCIL
DATA PROTECTION POLICY

1. Introduction

The Data Protection Act 1998 establishes a framework of rights and duties which safeguard personal data. Personal data is information about a living individual who can be identified from the data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details. Hemyock Parish Council is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the Data Protection Act 1998. The Council has established the following policy to support this commitment. It is the personal responsibility of all employees, Members, contractors, agents and anyone else processing information on behalf of the Parish Council to comply with this policy. This policy continues to apply to employees and individuals even after their relationship with the Council ends. Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation. All incidents will be investigated and action may be taken by the Council's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and/or criminal action being taken.

2. Data Protection Principles

The Data Protection Act 1998 is underpinned by a set of eight common-sense principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data. Personal data must be

- processed fairly and lawfully
- processed for specified and lawful purposes
- adequate, relevant and not excessive
- accurate and, where necessary, kept up to date
- not kept longer than is necessary
- processed in accordance with the rights of the data subject
- kept secure
- transferred only to countries with adequate security

3. Access and Use of Personal Data

Access and use of personal data held by the Council is only permitted by employees, Members, contractors, agents and anyone else processing information on behalf of the Parish Council for the purpose of carrying out their official duties. Use for any other purpose is prohibited. Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and/or disciplinary offence. It is an offence under Section 55(1) of the Data Protection Act for any person to knowingly or recklessly obtain, procure or disclose personal data without the permission of the data controller (Hemyock Parish Council) subject to certain exceptions. It is also an offence for someone to sell or offer to sell personal data which has been obtained in contravention of Section 55(1).

4. Collecting Personal Data

When personal data is collected, for example on a questionnaire, survey or form, the person who the information is about must be told, (unless this is obvious to them) which organisation(s) they are giving their information to; what their information will be used for; who it may be shared with and anything else that might be relevant e.g. the consequences of that use. This is known as a Privacy Notice. Personal data collected must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where depersonalised (anonymous) information would suffice. If the information is collected for one purpose, it cannot subsequently be used for a different and unconnected purpose without the data subject's consent (unless there is another lawful basis for using the information – see section 5 below). It must be made clear to the person at the time the information is collected, what other purposes their information may be used for.

5. Lawful Basis for Processing

When Hemyock Parish Council processes personal data, it must have a lawful basis for doing so. The Data Protection Act 1998 provides a list of "conditions" when personal or sensitive personal data may be processed (Schedule 2 and 3 of the Act). The Data Protection Act 1998 defines "sensitive" personal data as information relating to a person's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; criminal offences (alleged or committed). Whenever the Parish Council processes personal data it must be able to satisfy at least one of the conditions in Schedule 2 of the Act and when it processes sensitive personal data it must be able to satisfy at least one of the conditions in Schedule 3 of the Act. The Parish Council can also process personal data if it has the data subject's consent (this needs to be explicit when it processes sensitive personal data). In order for consent to be valid it must be "fully informed" which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress.

6. Disclosing Personal Data

Personal data must not be disclosed to anyone internally or externally unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information. If personal data is disclosed to another organisation or person outside of the Parish Council, the disclosing person must identify their lawful basis for the disclosure and record their decision. This should include a description of the information disclosed; the name of the person and organisation to which the information was disclosed; the date; the reason for the disclosure; the lawful basis. In response to any lawful request, only the minimum amount of personal information should be disclosed. The person disclosing the information should ensure that the information is adequate for the purpose of the disclosure, relevant and not excessive.

7. Accuracy and Relevance

It is the responsibility of those who receive personal information to ensure so far as possible that it is accurate and up to date. Personal information should be checked at regular intervals to ensure that it is still accurate. If the information is found to be inaccurate, steps must be

taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Data subjects have a right to access personal data held about them and have inaccuracies corrected. More information about a person's rights can be found in Section 9 below.

8. Retention and Disposal of Data

The Data Protection Act 1998 requires that the Parish Council does not keep personal data for any longer than is necessary. Personal data should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it. The Parish Council's Record Management Policy must be checked before records are disposed of to see whether there is a prescribed retention period for that type of record. Members of the parish council - any records held on personal computers as a result of being a member of the parish council should be deleted on leaving office. Information should not be kept for longer than necessary, it should only be used for the purposes given, and the information should be kept securely.

9. Individual's Rights

Individuals have several rights under the Data Protection Act 1998. These include the right to access personal data held about them (Subject Access); the right to prevent their information being used in a way which is likely to cause damage or distress; the right to compensation for any damages as a result of their information not being handled in accordance with the Data Protection Act 1998; and the right to have inaccurate or misleading information held about them corrected or destroyed. A person wishing to exercise any of these rights must be given the Parish Clerk's contact details. It is particularly important that if a person has made a Subject Access request, this is forwarded to the Parish Clerk as soon as possible. The Parish Council has 40 calendar days in which to respond to a Subject Access request, provided the applicant has put their request in writing and suitable identification has been supplied.

10. Reporting Security Incidents

Hemyock Parish Council has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the Council can learn from its mistakes and prevent losses re-occurring.