

West Wycombe Parish Council

Information Security Policy

1 Introduction

1.1 West Wycombe Parish Council recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, the Council will facilitate the secure and uninterrupted flow of information, both within the Council and in external communications. The Council believes that security is an integral part of the information sharing which is essential to corporate endeavour and the policies outlined below are intended to support information security measures throughout the Council.

This policy is based on recommendations contained in British Standard 7799 – A Code of Practice for Information Security Management.

2 Definition

2.1 For the purposes of this document, information security is defined as the preservation of:

- **confidentiality:** protecting information from unauthorised access and disclosure;
- **integrity:** safeguarding the accuracy and completeness of information and processing methods; and
- **availability:** ensuring that information and associated services are available to authorised users when required.

2.2 Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

3 Protection of Personal Data

The Council holds and processes information about employees, councillors, customers, and other data subjects for administrative and commercial purposes. When handling such information, the Council, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). Responsibilities under the 1998 Act are set out in the Data Protection Policy.

4 Information Security Responsibilities

4.1 The Council believes that information security is the responsibility of all members of staff. Every person handling information or using Council information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the Council.

4.2 This Policy is the responsibility of the West Wycombe Parish Council; supervision of the Policy will be undertaken by the Clerk. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of information security policy is managed through the Clerk and other designated personnel with security responsibilities in specified areas of the Council.

5 Information Security Education and Training

The Council recognises the need for all staff, and other users of Council systems to be aware of information security threats and concerns, and to be equipped to support the Council's security policy in the course of their normal work. The Clerk shall implement a training programme for each class of users and shall provide information and further training in information security matters to answer particular requirements.

6 Compliance with Legal and Contractual Requirements

6.1 Authorised Use

Council facilities must only be used for authorised purposes. The Council may from time to time monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

6.2 Access to Council Records

In general, the privacy of users' files will be respected but the Council reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with Council policies and regulations, and to determine which records are essential for the Council to function administratively. Except in emergency circumstances, authorisation for access must be obtained from the Clerk, or nominee, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

6.3 Protection of Software

To ensure that all software and licensed products used within the Council comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, the Council will carry out checks from time to time to ensure that only authorised products are being used, and will keep a record of the results of those audits. Unauthorised copying of software or use of unauthorised products by staff may be grounds for disciplinary, and where appropriate, legal proceedings.

6.4 Virus Control

The Council will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of Council computers, including laptops, shall comply with best practice, in order to ensure that up-to-date virus protection is maintained on their machines.

7 Retention and Disposal of Information

7.1 All staff have a responsibility to consider security when disposing of information in the course of their work. Retention periods for some kinds of personal information are listed in the Document Retention Guidelines.

8 Reporting

8.1 All staff and other users should report immediately to the Clerk,

- any observed or suspected security incidents where a breach of the Council's security policies has occurred,
- any security weaknesses in, or threats to, systems or services.

8.2 Software malfunctions should be reported to the Clerk.

9 Disclosure of Personal Information

In most circumstances members of the council do not need to be aware of or hold personal information in order to carry out their duties however, in circumstances where personal information does become available to them this policy applies.

10 Information Retention

All personal information shall only be retained for as long as is necessary to complete the Councils business and should then be destroyed in line with the guidelines issued in the Data Protection Policy.

Adopted:9th June 2016