



## **Marchwood Parish Council Information Technology Policy**

### **This Policy is intended for Councillors and Staff at Marchwood Parish Council**

#### **Introduction**

Marchwood 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. The Council believes that the security of information is essential. The policy below is to protect all information assets owned and used by Marchwood Parish Council (MPC).

#### **Definition**

Information Security is defined as the preservation of:

- Confidentiality: protecting information from unauthorised access and disclosure;
- Integrity: safeguarding its accuracy and completeness; and
- Availability: ensuring that information is available to authorised users when required.

Information exists in many forms. It may be on paper, stored electronically, transmitted over a network, viewed in videos or films, or spoken in conversation. Whatever its form, or medium, appropriate protection is required to protect business continuity and to avoid breaches of the law, statutory, regulatory or contractual obligations.

#### **Privacy of Information**

It should be noted that MPC is a public body and will seek to carry out its business in a public and transparent way. Much of its business is conducted in meetings open to the public. All information given at a public meeting of MPC is in the public domain, is likely to appear in the minutes and may be reported by the press. The Council publishes many of its documents on its website.

#### **Protection of Personal Information**

The Council will hold and use information about employees, councilors, members of the public, and other data subjects for essential administrative and business purposes.

When handling such information, the Council must comply with the Data Protection Principles which are set out in the General Data Protection Regulation (GDPR).

[UK GDPR guidance and resources | ICO](#)

#### **Responsibility for Information Security**

Information security is the responsibility of all Members, employees (temporary or permanent), contractors, agents and anyone else processing information on our behalf. Every person handling information or using Council equipment IT is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the Council.



## **Marchwood Parish Council Information Technology Policy**

Members should have no expectation of privacy in their use of any MPC business system. Any correspondence, documents, records or handwritten notes, may be disclosable to the public under the Freedom of Information Act 2000 or the General Data Protection Regulation legislation. Any comments recorded or notes written must therefore be appropriate.

### **Use of MPC equipment**

Where Council IT facilities are provided, they must only be used for Council purposes. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

### **Use of Personal equipment**

Members and staff conducting Council business on their own personal equipment have a responsibility to follow established Good Practice to protect against malicious software and unauthorised external access to networks and systems.

### **Social Media and Online Participation**

This policy includes social media and Online Participation, i.e., forums, blogs, websites and so on.

Members and staff should not disclose personal information about MPC's staff, members or business online, unless expressly authorised to do so.

Members using social media should always be aware of their association with the Council and make sure that their posting is consistent with this.

Members are personally responsible and liable for the content they publish. They should be mindful that posts might remain public indefinitely.

### **Retention and Disposal of Information**

All members and staff have a responsibility to consider security when disposing of information in whatever format it is kept.

Specifically, all personal information shall only be retained for no longer than is necessary to complete the Council's business and should then be destroyed (for further information see MPC Document Retention Protocol).

### **Reporting**

All staff and members should report immediately to the Clerk, or to the Chair.

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



## **Marchwood Parish Council Information Technology Policy**

### **Staff – Information Technology**

Staff should refer to the staff handbook for further information relating to the use of Information technology usage.

All staff and councillors are responsible for the safety and security of Marchwood Parish Council's IT and email systems. By adhering to this IT and Email Policy the parish council aims to create a secure and efficient IT environment that supports its mission and goals.