WYTHALL PARISH COUNCIL INFORMATION SECURITY POLICY

1. Introduction
Wythall Parish Council (WPC) recognises that information and the associated processes, systems 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 Wythall Parish Council.

2. 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 or spoken in conversation. Whatever its form, or medium, appropriate protection is required to ensure business continuity and to avoid breaches of the law, statutory, regulatory or contractual obligations.

3. Privacy of Information
It should be noted that WPC 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 WPC 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 www.wythall-parish-council.org.uk
The Council owns its own IT equipment, some business (principally by email) is conducted on Members' personal devices.

4. Protection of Personal Information
The Council may hold and use information about employees, councillors, members of the public, and other data subjects for essential administrative and business purposes. When handling such information, the Council, must comply with the General Data Protection Regulation (GDPR).

Responsibilities under current law are set out in the Council's Data Protection Policy.
http://www.wythall-parish-council.org.uk/council-function-and-structure/parish-council-policies-procedures/

5. Responsibility for Information Security

Information security is the responsibility of all Members, employees (temporary or permanent), contractors 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.

Employees should have no expectation of privacy in their use of any WPC business system. Any correspondence, documents, records or handwritten notes, may be disclosable to the public, under the Freedom of Information Act 2000 or the GDPR. Any comments recorded or notes written must therefore be appropriate.

6. Compliance with Legal and Contractual Requirements
6.1 Use of WPC equipment

Where Council IT facilities are provided they must only be used for authorised purposes. Limited personal use is permitted.

7. 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 WPC'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 ensure 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.

8. Retention and Disposal of Information

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

The Council's Data Retention policy provides guidance on retention periods.
http://www.wythall-parish-council.org.uk/council-function-and-structure/parish-council-policies-procedures/

Specifically, all personal information shall only be retained for no longer than is necessary to complete the Councils business and should then be destroyed in line with the guidelines laid out in the Data Retention Policy

9. Reporting

All staff and members should report immediately to the Executive Officer, or to the Chair;

- 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; and
- any Software malfunctions

Adopted: 20th Sept 2018