WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Information Security Policy

1 Introduction

1.1 Background

Wendover Parish Council has a large investment in information, which is an essential resource that is used either directly or indirectly in the delivery of all of the Council's functions. The Council is the custodian of electronically and manually stored information, much of it of a personal and sensitive nature. When we receive the information, we are trusted to look after it and to make sure we comply with our legal responsibilities. There is a high reputational risk attached to the misuse or unauthorised publication of sensitive information.

In order to carry out the business of the Council, much of this information must be accessed by computer application systems and transmitted across communications networks operated by the Council. It is vital therefore that it is protected from any form of disruption or loss of service, and it is essential that the availability, integrity and confidentiality of the IT systems and data are maintained to the highest standards.

Information Security is not limited to managing ICT. It also covers the physical security of buildings, equipment and manual records; procedures for starters and leavers; good practice advice, and a reporting mechanism should an incident occur. Staff guidance on the use of the network, email and the Internet exists in the Acceptable Use Policy (reproduced in Appendix F) to supplement the general guidance within this document.

Information is a valuable asset, which must be protected to ensure the effective and accurate operation of the systems on which the Council relies. There are legislative and regulative obligations placed on the Council in respect of the confidentiality of much of this information, which must be observed. Failure to protect information could jeopardise the ability of the Council to provide efficient, cost-effective services to the general public.

It is essential that all staff are aware of their responsibilities under the policy and that Information Security controls are established to prevent information being accidentally or maliciously misused, corrupted, lost or destroyed.

1.2 Information Security

The purpose of Information Security is to protect information in the following key areas:

- Confidentiality - ensuring that information is protected against unauthorised access or disclosure.
- Integrity - ensuring that information is accurate, complete and free from corruption.
- Availability - ensuring that information is available when it is required.
- Non-Repudiation - ensuring the ability to prove the origin of information or disprove a denial of receipt.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

1.3 Purpose of the Policy document

The purpose of this Information Security Policy document is to define the stance of Wendover Parish Council with regard to certain aspects of Information Security which are described in the body of the document.

The Policy document is a framework for the establishment of standards and procedures for Information Security Management and is based on the guidance contained in BS7799, a code of practice for Information Security Management.

The Policy Document has a number of appendices which give practical advice and guidance to users in specific areas of Information Security. Some of these appendices have been made available in the form of Information Leaflets.

1.4 Scope

The Information Security Policy applies to all Council locations and elsewhere where Council business is undertaken, and applies to all staff, Councillors, agents, contractors and volunteers working for, or on behalf of, the Council.

The Policy will form part of the standard contract terms and conditions, or other agreement, for external users working on behalf of the Council. Contractors or other external users are directed to their Client Monitoring Officer.

The generic terms user and users are used within this policy to refer any of above.

For the purposes of this document, the term 'information' covers:

- paper records, whether stored in Council premises, off site or in transit between the two.
- data, software, recorded data and images stored on and accessed by computer systems.
- data, software and images transmitted electronically across networks, both internal and external.
- data, software and images stored on removable media or storage.

The guidance within the Policy document also applies, where relevant, to other kinds of information which may be printed, sent or received by fax and stored on film.

The guidance will also apply to certain manual records covered under the General Data Protection Regulation. These will include records (e.g., application forms) relating to computerised information and may include manual filing systems where they are structured to enable easy reference to personal information e.g., a personnel filing system. If in doubt, please seek advice from the Clerk.

This Information Security Policy is a Council policy and infringements may result in formal action against those found to have breached it. The disciplinary process, offences and outcomes are documented in the HR policies file held in the Council's offices.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

1.5 Objectives

The objectives of the Council's Information Security Policy are:

- To ensure that all users of Council information and Information Technology systems are aware of the need for Information Security and have an appreciation of their responsibilities.
- To define broad organisational roles and responsibilities.
- To provide a framework which gives guidance on a number of aspects relating to information security, as defined in the policy document.
- To establish the need for every information system to have specific security controls, which are adhered to.
- To establish the corporate level controls to the IT network.

2 Roles and Responsibilities

2.1 Parish Clerk

The Parish Clerk has overall responsibility for the development and implementation of this Policy.

The Parish Clerk will, subject to approval by the Council, develop, publish and maintain Wendover Parish Council's Information Security Policy. These activities will include developing, reviewing and auditing procedures compliant with this Security Policy. They will also be responsible for the dissemination of the information contained within the policy. They will oversee the Information Management processes relating to Data Protection, Freedom of Information, compliance with records management good practice and corporate issues relating to records management.

2.2 All Users of IT systems – Members, staff and other authorised people

Users of IT systems must ensure that they comply with the guidance contained within the Information Security Policy and report any actual or suspected breaches via the appropriate channel. See Section 5 for further guidance on reporting security incidents.

2.3 IT development, support and maintenance staff

Phenom Networks are responsible for the support and maintenance of Wendover Parish Council computer systems. They may, therefore, have privileged access to computer systems and to personal and confidential information in order to carry out their normal responsibilities. They must ensure that they are aware of and comply with the information security provisions relating to each computer system as well as this general policy guidance.

Duties will include ensuring that regular back-ups of email software and data are taken, and copies are stored in a secure remote location and that changes to the system are authorised and made in a controlled and effective manner.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

2.4 Monitoring compliance

The diverse nature of this policy means that responsibility for monitoring its compliance will be shared between the Council and Phenom Networks depending on the facet of the policy being considered.

2.5 Physical Security

Unless otherwise stated, the enforcement of physical security measures is the responsibility of the Parish Clerk as the manager of the Council offices.

2.6 Personnel Security

The Parish Clerk is responsible for the security countermeasures to be used in recruitment, whilst staff and contractors are employed, and on termination. In addition, the policy addresses security awareness and training aspects to ensure that staff are fully aware of their security responsibilities and the necessary security procedures that they use.

3 Legal Requirements

The Council will observe all laws and regulations which apply to Information and computer systems. These include:

3.1 Data Protection Act 2018 and retained General Data Protection Regulation (GDPR)

Details of our obligations under this act are contained in the Data Protection Policy

3.2 The Copyright, Designs and Patents Act 1988

This Act makes it illegal to copy any piece of software without the owner's permission. Most proprietary software is supplied under a licence agreement which limits the use of the software to specified platforms and numbers of users. Copying of the software will normally be restricted to the creation of back-ups.

To comply with the law:

- all purchased software must have appropriate licence agreements.
- purchased software can only be used on platforms covered by the licence.
- definitive versions of proprietary software and the licence agreements must be stored in a secure place.

Criminal prosecutions may result from infringements of copyright law.

3.3 The Computer Misuse Act 1990

This Act recognises that certain activities constitute computer crime and provides legal redress against offenders.

Broadly speaking, computer misuse is categorised as:

- attempted unauthorised access to a computer system.
- attempted unauthorised access to information.
- access with a view to personal gain.

Users must report any instances of potential or suspected misuse of computers via the mechanism described in Section 5.

3.4 The Regulation of Investigatory Powers Act 2000 (RIPA)

The Regulation of Investigatory Powers Act 2000 (RIPA) governs the interception of communications, covert surveillance operations and access to encrypted data.

A Code of Practice on the Use of Personal Data in Employer/Employee Relationships has been developed and addresses the impact of the General Data Protection Regulation 1998 on the monitoring by employers of telephone calls, e-mails and Internet access involving their employees. The Council is authorised in relation to its internal communications network to monitor or record all communications transmitted over its system without consent for the following purposes:

(a) establishing the existence of facts.
(b) ascertaining compliance with regulatory or self-regulatory practices or procedures.
(c) ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system.
(d) preventing or detecting crime.
(e) investigating or detecting unauthorised use of the Council's telecoms system.
(f) ensuring the effect of the proper operation of the system.

The Council may monitor (but not record) communications to check whether or not communications are relevant to the Council.

The Council is required to "make all reasonable efforts to inform those people who use the Council's telecom systems that interceptions may take place". Wendover Parish Council through this Information Security Policy, informs all users of Council systems of its intention to access, record and monitor information in order to ensure the appropriateness of their use of information and activities performed through information systems, facilities, and processes established for Wendover Parish Council business purposes. If you require any guidance on RIPA please contact the Parish Clerk

3.5 Freedom of Information Act 2000 (FOI)

For further guidance on the Freedom of Information Act contact the Parish Clerk or see our Freedom of Information Policy

3.6 Human Rights Act 1998

Under article 8 of the Human Rights Act ‘everyone has a right to respect for his private and family life, his home and his correspondence’. Information should be kept securely and only shared in accordance with guidance mentioned elsewhere in this policy.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

4 Education and awareness

4.1 Job descriptions

The Council will ensure that:

- Where appropriate, specific security roles and responsibilities are defined and documented in job descriptions.
- Individuals who have a responsibility for the protection of information assets are aware of their specific responsibilities.
- All Council employees are aware of and have access to information relating to security procedures.

4.2 Recruitment

Appropriate security screening measures may be taken when dealing with applications for employment, especially when the job involves dealing with information which the recruiting officer considers to be sensitive. Certain job roles require CRB checks, and further checks will be carried out where the job role involves working with children. These screening procedures may also be invoked if employees change roles within the organisation, and their new role involves dealing with information of a sensitive nature.

There is a formal user registration and de-registration procedure for starters and leavers. As part of the induction process, the line manager of the new user is responsible for starting the process. On termination of employment/assignment by Wendover Parish Council, all access is revoked.

The Parish Clerk must sign a request for non-employee access to network. They will be expected to comply with the guidelines set out in this policy.

4.3 Leave of Absence

It is recommended that Phenom Networks be informed of staff being away for an extended length of time (i.e., sabbatical/sickness/maternity) so an account is not inadvertently deleted.

If a member of staff requires access to information held in the personal folders of an absentee, then the permission of Parish Clerk must be obtained in accordance with this policy.

4.4 Training

The Council will ensure that all users of IT systems are aware of security requirements and procedures as part of the induction process, and that training is available on the correct and secure use of IT facilities. This is the responsibility of the Parish Clerk.

4.5 Confidentiality

It is the duty of staff not to disclose to a third party or otherwise use any of the Council's confidential information either during or after the termination of employment with the Council.

Agency, contract staff and contractors must abide by the relevant conditions of contract with regard to security matters and may be required to sign confidentiality and nondisclosure undertakings prior to being allowed access to IT facilities, as may volunteers.

4.6 Leaving the Council

Before an employee leaves the Council's employment the Parish Clerk should be informed of important information held within their account – email or home directory.

5 Reporting security incidents

It is the responsibility of all users to report any observed or suspected security weaknesses in IT systems or services. The Council will maintain various methods for users to report actual or suspected breaches in security procedures.

Users must not attempt to test or prove suspected weaknesses themselves. Such action may be misconstrued as an attempted breach of security and investigated and dealt with in accordance with the Council's Disciplinary Procedure or Member Code of Conduct, as appropriate. For external users under contract to the Council, such action could be considered to be breach of contract or investigated under the provisions of the Computer Misuse Act 1990.

The Council's mail scanning or internet monitoring systems automatically flag hundreds of items and instances of events daily in an attempt to balance protection for the network and the individual users with the avoidance of delay. These will not be treated automatically as a security incident unless subsequent inspection by IT Staff reveals the need for this.

5.1 Who to report an incident to?

Where fraud and/or money laundering is suspected this should be reported in the first instance to the Parish Clerk. The anti-money laundering policy or the anti-fraud, corruption and whistleblowing procedure may be used for this purpose.

In other cases, staff should normally report actual or suspected breaches in security procedures via their Line Management. If this is not possible or appropriate it should be reported to either the Chair of Staffing or Chair of the Council.

Members should report actual or suspected breaches of the Policy to Parish Clerk. The Policy has been drawn to Members' attention by virtue of its inclusion on the Agenda of Audit Committee and Executive and by letter.

Full procedures are documented in the Wendover Parish Council Security Incident Handling and reporting guidelines (Appendix H).

5.2 Phenom Networks

Users should report or discuss security matters of a general systems nature rather than individual behaviour with Phenom Networks.

Phenom Networks record all incident reports and will maintain an incident category for security incidents. Phenom Networks will ensure that steps are taken to review suspected weaknesses, reconfigure systems where applicable and install updates and patches as available.

Issues relating to viruses should be reported to Phenom Networks.

5.3 Confidentiality

The Council's Whistleblowing Policy provides guidance as to how employees can raise a concern without fear of recrimination. These procedures, which are referred to in both the Policy on Anti-fraud and Corruption and the Code of Conduct, can be used, when necessary, by employees to report security matters. The Whistleblowing Policy details points of contact.

5.4 Disciplinary proceedings

This Information Security Policy is a Council policy and infringements may result in the invocation of the Council's Disciplinary Procedure (in respect of staff) or Member Code of Conduct (in respect of Members).

6 Policy Statements

Section six sets out all of the policy statements that inform the Information Security Policy. It explains how the Council will enforce information security. It is supported by a series of appendices and guidance notes to help users understand what is expected of them.

6.1 Identification and control of assets

The Council will identify all assets which are important for the provision of IT systems and services. Assets can be characterised as:

- Information databases and files, documentation and manuals, procedures and plans etc.
- Software applications, operating systems, tools and utilities which may be developed in-house, or bought-in packages.
- Physical computer and network hardware, ancillary equipment, furniture, telephones etc.

6.2 Procurement

All requests for new equipment and software must be agreed by the Parish Clerk and Phenom Networks to ensure that what is bought for use on the Council's network is both compatible and appropriate in terms of the requirements of this Policy.

6.3 Inventory

Assets which are deemed to be an important component of computer systems or service delivery such as base units and monitors will be physically identified, and their existence will be recorded in the asset register. This is used as a key component of the Council's system and provides information for insurance. Wendover Parish Council will maintain an inventory of the Council's software and software licences.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

6.4 Change Management

All changes to physical and software assets must be made under the advice of Phenom Networks and must ensure that any changes made to the assets are assessed as to whether there is any impact on security controls.

6.5 Physical and environment security

The Council will ensure that the following general controls on physical access and security are maintained.

- Council offices and areas accessible only by staff, Members and authorised visitors will be protected by appropriate security controls from areas of Council premises accessible by the general public.
- Wherever possible visitors to Council premises will be supervised. Staff are issued with personal alarms and must test these on a regular basis. If they are found to be not working, they must inform the Parish Clerk immediately. It is the responsibility of the staff to carry their alarms with them.
- Suitable secure accommodation has been created within Wendover Parish Council locations containing information or equipment in order to protect these facilities from unauthorised access.
- Fire Alarms are tested monthly, and the Council holds fire evacuation tests twice a year. Wendover Parish Council has fire extinguishers throughout its buildings, and these are tested annually by a competent company.

6.6 Information security

Users must ensure that information considered to be sensitive to which they have access, such as passwords, computer discs etc., are locked away when offices are unattended.

Managers must ensure that suitable facilities are provided for the storage of sensitive information. The nature of the information will determine what is suitable. This could include a locked desk drawer, locked cupboard or in some instances a safe.

Unwanted equipment and media must be disposed of under advice of Phenom Networks.

6.7 Maintenance of manual records

All staff should take steps to ensure that they comply with the Council's Document Retention Policy and ensure good practice for the management of paper records.

Steps must be taken to make sure that all records are accessible, including those held in personal files to ensure the Council can provide information on request. This is particularly important in relation to Access to Information requests (i.e., Freedom of Information, Data Protection, Environmental Information Regulations).

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

6.8. Off-site considerations

The Council must comply with the General Data Protection Regulation, which includes the principle 'to take appropriate technical and organisational measures' to guard against unauthorised or unlawful processing of data or accidental loss.

Management authorisation must be acquired prior to removing Council IT equipment offsite. For practical reasons, staff issued with laptops will be deemed to have received authorisation by virtue of the fact they have been issued with a portable PC.

It is the responsibility of the user removing equipment to ensure that appropriate security controls exist at the off-site location, and that sensible measures are taken to protect equipment whilst in transit. Users should also ensure the security of data in portable computer media e.g., memory sticks is only taken off site when absolutely necessary and the data removed as soon possible after use or transfer.

Managers must ensure that a record is maintained of either the current location of portable IT equipment, or the person responsible for it, and must be aware of any provisions regarding the insurance of items in transit or located off-site. Subject to normal domestic security arrangements being applied, items held at home are covered by insurance, but items are NOT covered if left in an unattended vehicle.

6.9 Supplied computers, terminals and tablets

The Council will provide Members and staff with appropriate computer equipment to carry out their Council function, and it is the duty of those individuals to ensure that basic security controls are applied to these items supplied, including computers, printers and other IT related equipment used by them.

These basic controls include:

- Ensuring that the correct start-up and close-down procedures are carried out at the beginning and the end of working periods. For safety, security and environmental reasons all PCs and equipment should be switched off at the end of the day and not left on overnight.
- Ensuring that computers are not left logged-in while unattended. The PC should be locked using Windows/L during any absences.
- Ensuring that no unauthorised software is introduced onto supplied computers. Phenom Networks are responsible for the installation of all software.
- Ensuring that password controls are understood and adhered to - this includes the procedures for changing and storing passwords. Passwords should not be shared with colleagues, family or partners.
- Ensuring that the standard build of the supplied computer is not altered.

6.10 Network

Phenom Networks are responsible for the installation, maintenance and management of the Council's internal data networks.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

6.11 The Internet and email

Members and Staff must ensure they comply with the Council's Acceptable Use Policy. The policy sets out a list things staff must or must not do relating to the network, internet and email. If any misuse is suspected, then managers may request a report of usage to establish whether an investigation is required.

6.12 Access to systems

The Council's computer systems and equipment must only be used by authorised personnel and only in pursuance of their duties.

Staff who require access to the Council's computer systems must first gain authorisation from the Parish Clerk Staff must make themselves familiar with the relevant log-on, logoff and password control procedures.

If access is required into another user's account, they should gain permission from the Parish Clerk.

6.13 Development and maintenance

Significant changes made to the Council's computer systems must be assessed for their security implications by the system owner together with Phenom Networks. The Council and Phenom Networks are jointly responsible for the procurement and installation of new computer systems and must ensure that appropriate Information Security controls are included in system design and specifications.

6.14 Back ups

Security copies (backups) of systems operating on the network will be taken on behalf of users by Phenom Networks at predetermined frequencies. These are automatically scheduled at regular intervals dependent upon the importance and quantity of the data concerned.

Backups of allocated mailboxes and data stored within the Microsoft Office 365 SharePoint solution is backed up 3 times per day.

A variable retention period has been deployed depending on the age of the backup.

0 to 4 weeks old – All three of the daily backups are retained.

4 to 8 weeks old – The final daily backup is retained.

Older than 8 weeks – A single weekly backup is retained indefinitely.

No information stored on the hard drive of a PC, other than that filed under the WPC SharePoint link, is backed up. Users should ensure that all important information is stored within the WPC cloud. Storage of data that might be required for legislative purposes must always be stored within the WPC cloud. Information stored on portable media such as CDs or DVDs is less secure and is therefore strongly discouraged unless it is for non-essential and non-sensitive material.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

6.15 Business Continuity Planning

The Council is responsible for maintaining the continuity of its business processes in the event of a major incident. Phenom Networks are responsible for the recovery of IT systems to support Council services.

6.16 Records Management - Information sharing

All staff who share information with other agencies must be aware of the data sharing guidance relating to personal information.

The Council maintains appropriate contacts with law enforcement authorities, regulatory bodies, service providers and telecommunications operators. These include: The Police (for relevant security incidents, especially breaches of the Computer Misuse Act); the Information Commissioner (for relevant Access to Information enquiries) and other public service agencies. Staff should familiarise themselves with the Access to Information guidance set out on the Council's intranet system and ask for advice if required.

Information required as part of the 'Council records' should not be stored solely in personal user areas that cannot be accessed by other officers. The use of shared folders is encouraged for Council records that will not be stored on a document management system or alternative central record.

6.17 Records Management – electronic and manual

The Council's responsibilities under section 46 of the Freedom of Information Act 2000 require that the Council properly manages the creation, management, archive and destruction of records, which includes written or recorded information.

Each section is responsible for the management of its retention schedules, ensuring the timely disposal of out of date or inaccurate information. Details of retention schedules can be found on the Council's intranet and website.

All electronic files and data (including digital photos and mapping) held on personal or shared network folders must be reviewed on a regular basis, in accordance with retention schedules, to ensure the folders do not exceed the agreed capacity limit.

Records are sent to the County Archives for long-term storage. Destruction dates are added to records in accordance with retention schedules. The County Archives operate their own procedures for destruction, which includes a review of the series of files for any information that should form part of the permanent record of the Council.

Categorisation

Committee reports are categorised as public or confidential according to the guidance on exempt information for Committee reports.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

6.18 Re-use of Council Information

The Re-use of Public Sector Information Regulations, encourage the re-use of public sector information - that is, information for which the Council holds the copyright. The Regulations allow any company or individual to re-use information held by Wendover Parish Council for commercial or non-commercial gain. To do so they must apply for a licence and pay any licence fees that the Council may impose.

'Re-use' means using the information for a purpose other than the purpose for which the document was originally produced. It is not compulsory for public authorities to allow reuse. At present, the Council does not apply any charge over and above those for research or photocopying.

There is separate legislation to cover the sale of the 'full' and 'public' register of electors, covered by Regulation 111 of the Representation of the People Regulations 2001.

6.19 Confidential waste disposal

The Council has a contract for the secure disposal of confidential paperwork and certificates of destruction are kept with invoices for this contract.

6.20 Removable Media

Removable media including floppy disks, CDs and USB memory sticks should only be used for transferring business-related data to and from the computer.

Media that has been used for home PCs previously must not be used and before the media is accessed on your work PC it must be scanned by the resident antivirus software for viruses and other malware.

6.21 Audit and control

The Information Security Policy has been authorised by the Council and it is reviewed annually. Any changes required that are other than of a minor factual nature must be authorised by the Council.

Empowerment to carry out spot checks and audits of equipment, software, users and procedures to ensure conformance to the Policy will be shared between Phenom Networks, Internal Audit and the Council depending on the facet of the policy being considered.

6.22 Bring Your Own Device (BYOD)

Wendover Parish Council recognised the benefits that can be achieved by allowing Councillors to use their own electronic devices for Council business, whether that is at home or at meetings. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD.

The use of such devices to create and process Council information and data creates issues that need to be addressed, particularly in the area of information security.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

The Parish Council must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering Councillors to ensure that they protect their own personal information.

The advice from the ICO states "Councils must ensure the confidentiality, integrity and availability of all personal data they hold, even if the data is being processed through personal email accounts or is stored on a privately owned device.

Councillors using BYOD must take all responsible steps to:

- Prevent theft and loss of data
- Keep information confidential where appropriate
- Maintain the integrity of data and information
- Take responsibility for any software they download onto their device

The Parish Council cannot take responsibility for supporting devices it does not provide.

By using their own device Councillors agree to:

- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.
- Ensure they regularly check for operating system updates and security fixes
- Ensure appropriate firewalls and anti-virus software are installed, up to date and on
- Where it is essential that information belonging to the Council is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails.
- Ensure that relevant information is copied back onto Council's systems and manage any potential data integrity issues with existing information.
- Report the loss of any device containing Council data (including email) to the Clerk.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately to the Clerk.
- Ensure that no Council information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party. Councillors are encouraged to allow Phenom Networks to download remote management software for a Council folder on their device and keep all Council information in that folder (The folder can be remotely wiped if required).
- Ensure they immediately delete all council data from their personal devices once they have left the Council
- Accept that their device may be called into the office at short notice and held at the office until processes are complete should there be a data breach or a FoI request

The Council will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either a wired or wireless network or both.
- Take all necessary and appropriate steps to retrieve information owned by the Council.

WENDOVER PARISH COUNCIL
Address: The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

The Council must process 'personal data' i.e., data about identifiable living individuals in accordance with the Data Protection Act 2018 and the General Data Protection Regulations. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

The Council, in line with guidance from the Information Commissioner's Office on BYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore, Councillors must follow the guidance in this document when considering using BYOD to process personal data.

A breach of the Data Protection Act 2018 or the GDPR can lead to the Council being fined. Any Councillor found to have deliberately breached the Act or the Regulations. may be subject to disciplinary measures or even a criminal prosecution.

Document History

Drafted by Parish Clerk	30/05/2016	(version 1)
Approved by Parish Council	03/07/2018	(version 1)
Reviewed by Parish Council	04/06/2019	(version 2)
Reviewed by Parish Council	06/07/2021	(version 3)
Reviewed by Parish Council	03/08/2021	(version 4) Inclusion of BYOD
Reviewed by Parish Council	04/07/2023	(version 4) with minor amends