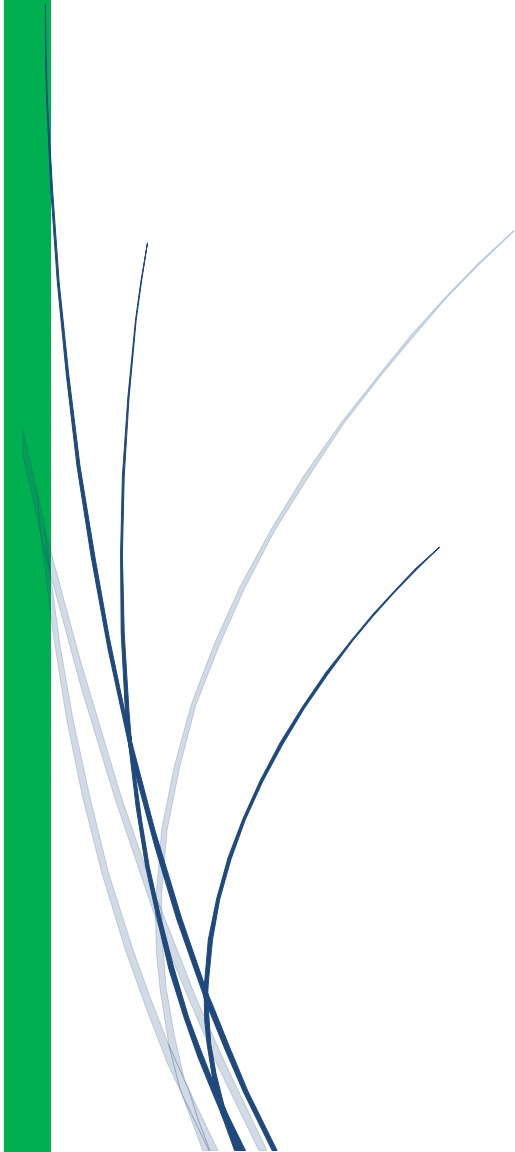




Winchcombe

Winchcombe Town Council

Acceptable Use Policy



WINCHCOMBE TOWN COUNCIL ACCEPTABLE USE POLICY

We must act appropriately with the information we obtain and hold, and with the systems we use and access. How you use our systems is important for information security, efficiency, collaboration and our reputation.

This Acceptable Use Policy covers the security and use of all IT. This policy applies to all employees, Councillors, voluntary workers, agency staff and contractors.

WTC commits to informing all employees, members, voluntary workers, agency staff, contractors, Councillors and other third parties of their obligations before they are authorised to access systems and information. Other organisations, and their users, granted access to technology managed by the organisation must abide by this policy.

Access to IT systems

- You must not allow anyone else to use your user username and password.
- You must not disclose your password to anyone or ask anyone else for their password. If you suspect your password has become known to anyone else, change it immediately and report it to ReformIT.
- You must not leave user accounts logged in at an unattended and unlocked device.
- You must not attempt to access data that you are not authorised to use or access.
- You must not install, access or modify applications, systems or data without authorisation.
- You must not conduct Council business using a personal account.
- If you receive or view email or other content not intended for you, you must protect its confidentiality.
- You must take care when replying or forwarding emails to ensure that only relevant parties are included.

Behaviour

- You must not participate in unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, material of a pornographic, sexual, violent, criminal, racist, sexist or otherwise discriminatory nature. Further, you must not use the systems to perpetrate any form of fraud or piracy.
- You must not publish defamatory or knowingly false material in any online publishing format.
- Only subscribe to services with your professional email address when representing the Council.
- You must not use the internet or email to make personal gains, conduct a personal business or to gamble.

Storage

- Documents must not be downloaded and/or stored locally (for example on your personal pc) on a desktop computer or laptop, as they are not backed up and information may be irretrievable if the device fails or is stolen.
- The use of mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be authorised by the Clerk.

Security and licensing

- You must have suitable anti-virus security installed on any personal pc or device through which you will access WTC IT systems.
- You must use a currently supported operating system for all devices you may use to access WTC IT systems.
- You must not attempt to disable or bypass anti-virus, malware or other security protection, and you should take care not to introduce viruses or malware. If you discover a virus or malware, you must notify the Clerk and ReformIT immediately.

Use of Microsoft Teams

- You must not attempt to access content for which you do not have permission.
- You must not circumvent security measures.
- You must maintain the Teams infrastructure setup by filing documents within existing folders.
- Data used must be kept confidential and secure by the user.
- Data can be shared with external people/organisations using for example the 'External sharing' SharePoint site. All documents shared must be removed once the need to share has expired. Any special category data shared in this way must be done with the appropriate set up of SharePoint permissions to ensure the security of that data.
- Personal data should not be shared via teams messaging.
- All users should ensure that permissions for documents are set appropriately.
- All users should ensure that only permitted participants are added to Teams channels.
- All users should ensure that only authorised parties join a call.
- Care should be taken when screen sharing and/or recording a meeting to make sure that personal data is not disclosed inappropriately.
- Permission should be sought from all attendees before recording starts.
- Ensure that when making video calls the environment you are calling from and any backgrounds you are using are appropriate for business use.
- Personal information relating to staff or customers should not be shared in Teams chats.

Monitoring

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the Council's procedures.

Policy review

The policy will be reviewed on an annual basis and updated as necessary.

Contacts

Clerk to WTC	clerk@winchcombetowncouncil.co.uk
ReformIT Support	support@reformit.co.uk
ReformIT Helpdesk	01242 236999