ICT Acceptable Use Policy

Introduction

This policy has been produced for all individuals who directly use any of the Information and Communication Technology (ICT) resources provided by Tewkesbury Borough Council and provides guidance on the acceptable use of our ICT services.

The purpose of this ICT policy is:

- To ensure ICT is used effectively.
- To protect the council.
- To protect all users and Members.
- To help procure, support and use ICT.

Ownership

All ICT equipment, services and intellectual property stored or transmitted on our ICT infrastructure are the property of Tewkesbury Borough Council unless there is a specific agreement to the contrary. We reserve the right to monitor and access all information stored or transmitted on it in ways that are consistent with relevant legislation and guidance provided by the office of the UK Information Commissioner.

Scope

This policy applies to all permanent and temporary staff, elected members, contractors, consultants, secondees and others who have access to the council's ICT services. For the sake of simplicity those covered by the scope will be referred to as users within this policy.

Responsible use of ICT services

All users of Tewkesbury Borough Council's ICT services are expected to act responsibly and in compliance with the Council's policies, procedures, and values. This includes but is not limited to:

- Using ICT services in a lawful and professional manner, in accordance with job duties, responsibilities and all relevant legislation.
- Using only authorised equipment, provided by the council, to carry out council business. Users must not use any unapproved equipment to access data or carry out council business. This includes personal mobile phones, tablets, computers and laptops. The use of unauthorised equipment could compromise the security and integrity of the council's systems and data, and users will be held responsible for any breaches or damages resulting from their actions.
- Protecting sensitive and confidential information by adhering to appropriate security protocols.
- Not engaging in any activities that may compromise the security, integrity, or availability of the Council's ICT infrastructure.
- Using appropriate language and tone when communicating through ICT services, avoiding any offensive, harassing, or discriminatory language.
- Complying with any applicable laws, regulations, and council standards when using ICT services.
- Immediately reporting any incidents of suspected or actual security breaches, violations of policies or procedures, or any other concerns related to the use of ICT services to the IT and

Cyber team. Incidents can be reported using the service desk, calling 01684 272231 or by emailing itsupport@tewkesbury.gov.uk

- Ensure that any equipment or software provided by the Council is used in a safe manner and for the purpose it was intended. If you notice any defects or damage, please report them to the IT and Cyber team as soon as you can. This is crucial because damaged equipment might not work correctly and could pose a risk of electrical shock to users due to exposed wiring, as well as a potential fire risk from short circuits or batteries.
- Downloading, copying, possessing and distributing information or other information from the internet or through email should only be carried out with the relevant licenses, intellectual property rights or copyright.

Exception. The use of personal mobile devices to facilitate multifactor authentication (MFA) is permitted for users. Whether these are push notifications to apps or text messages that contain access codes.

Business Use of Council Resources

All council resources, including but not limited to computers, mobile devices, software, and internet access, are provided for business purposes only. It is the responsibility of all users to use council resources solely for work-related activities and refrain from using them for personal activities, such as browsing social media, personal email, online shopping, personal business, political activities, or any other non-work-related activities.

Moreover, users must not use council resources to access or store any material that is illegal, offensive, discriminatory or inappropriate in any way. The misuse of council resources in this way can lead too disciplinary, gross misconduct and legal action. See council's disciplinary process.

By using council resources solely for business purposes, employees help to ensure the security and integrity of the council's systems and data.

Working from the UK

By default, access to ICT services and council data (including accessing Office 365, email or teams) is restricted to locations within the UK.

Systems that bypass location detection or content control systems such as VPNs and proxies are not permitted to be used with council equipment or data unless specifically authorised by the IT and Cyber team.

Working from outside the UK

On request access to email and teams will be granted to users travelling within the EU on their corporate mobile devices (phones and tablets). The devices must be kept securely locked away and it is expected they will be used in a safe way (not in the middle of the street). Access must be requested at least five working days in advance to balance the security of the organisation while offering additional flexibility to respond to urgent incidents.

It should be noted that by default council issued mobile devices are blocked from data roaming and connecting to non-UK mobile networks. If this functionality is required, then it should be requested prior to travel.

Access to corporate data from non-EU countries will not be authorised.

Passwords and login information

To maintain the security of our ICT services, it is essential that all users ensure the confidentiality of their login information and passwords. All passwords must be complex and unique, and must not be shared with anyone, including colleagues or third-party contractors.

Users are responsible for keeping their login information secure. Passwords must be at least twelve characters long and contain a combination of upper and lowercase letters, numbers, and symbols. Passwords must not contain easily guessable information such as personal information, dictionary words, or sequences of numbers or letters.

Multi-factor authentication (MFA) is an additional layer of security that helps protect your accounts. It requires you to provide two or more forms of authentication before accessing your accounts, such as a password and a code sent to a mobile phone. Wherever possible, users must enable MFA for any accounts. The IT and Cyber team will support where required to facilitate this. This will greatly reduce the risk of unauthorised access to your accounts and sensitive information.

If you suspect that someone has accessed your account or if you suspect any suspicious activity, you must notify the IT and Cyber team immediately.

Sharing login information or passwords is strictly prohibited and may result in disciplinary action or legal consequences. If access to our ICT services is required by a third party, such as a contractor or consultant, separate login credentials will be provided.

Remember, strong passwords and careful management of login information is critical to protecting the security and integrity of our ICT services.

Email use

Email is a primary means of communication within the council, and as such, users are expected to use email in a professional manner that is consistent with their job duties and the Council's policies, procedures, and values.

Users must take responsibility for the content of their emails and must ensure that they do not contain any offensive, discriminatory, or defamatory language, or infringe on the intellectual property rights of others.

In addition, users must take appropriate measures to ensure the security and confidentiality of all email communications. This includes using password-protected documents to transmit sensitive or confidential information, verifying the recipient's identity before sending the email, and following any encryption protocols set out by the IT and Cyber team.

Users must also be aware that email communications are subject to disclosure following freedom of information/subject access requests. Emails can also be subject to disclosure as part of legal proceedings. Therefore, users should think carefully before sending an email and ensure that they only send information that is necessary and appropriate for the recipient.

Users are expected to manage their email accounts efficiently, including regularly reviewing and archiving old emails, deleting any spam or junk emails, and reporting any suspected phishing emails to the IT and Cyber team.

To ensure the security of communication, only email addresses issued by the council can be used for official council business. Personal email accounts must not be used for any council-related activities. Using personal email accounts may compromise the security and confidentiality of council information and could violate council policies and procedures.

MS Teams

MS Teams is a collaboration tool provided by the council to facilitate communication and collaboration among users. MS Teams should be used in a manner consistent with the objectives of the Council and its policies, procedures, and values.

MS Teams is provided to enable effective communication and collaboration among users of the Council.

MS Teams must not be used for personal or non-business-related activities.

MS Teams must be always used in a professional and appropriate manner.

Users must only use their Council-provided MS Teams account for work-related activities.

Users must communicate with each other in a professional manner when using MS Teams.

Harassment, discrimination, or other inappropriate behaviour will not be tolerated.

All communication on MS Teams is subject to the Council's monitoring policy.

Users must immediately report any suspected or actual security breaches to the IT and Cyber team. Incidents can be reported using the service desk, calling 01684 272231 or by emailing itsupport@tewkesbury.gov.uk

Users must only share information on MS Teams that is necessary for their work.

Communications on MS Teams is subject to retention and archiving policies.

Users must ensure that their communication on MS Teams is consistent with the Council's policies and procedures.

Using alternative messaging, collaboration, sharing or productivity systems

Using non-council systems for work purposes should be done with caution. Examples of these are Slack, WhatsApp, Drobox, Google Drive or partners systems. These systems do not have the same levels of protection that council systems have built into them. Communications sent via these systems can also be subject to disclosure following freedom of information/subject access requests. Emails may also be subject to disclosure as part of legal proceedings. Prior to using any system for council business advice and specific approval must be sought from the IT and Cyber team and the Data Protection Officer (DPO).

Device responsibility

All users are responsible for the proper care and use of any corporate device assigned to them. This includes laptops, mobile phones, tablets, and any other electronic equipment provided for work purposes.

Use of assigned devices is restricted to the assigned employee and should not be lent or borrowed by any other individual.

If the assigned device is damaged or not functioning properly, users are required to report the issue to the IT and Cyber team immediately. The IT and Cyber team will assess the issue and determine whether the device can be repaired or must be replaced.

It is the user's responsibility to ensure they have the equipment needed to carry out their role. The IT and Cyber team do not have spare equipment available to lend out.

In the event of loss or theft of the assigned device, users must immediately report the incident to the IT and Cyber team and their line manager. When a device is not in use it should be securely stored away. In the offices this should be in a locker or other locked area. When stored at home, devices should be kept out of sight and preferably locked away. Devices must not be left unattended in vehicles.

Users should also ensure that they do not store any confidential or sensitive information on their assigned device without proper encryption or other security measures. All data and information stored on the device should be backed up regularly to ensure that it is not lost in the event of a device failure or loss.

Software, applications and apps

It is important to only use authorised software or apps on council devices to ensure security and confidentiality of council data. The use of unauthorised software or apps can lead to data breaches, malware infections, and other security issues.

The council maintain a list of authorised software and apps that can use on council devices. Users should not download or install any software or apps that are not on this list without prior approval from the IT and Cyber team.

In addition, users should not modify or alter any authorised software or apps without the IT and Cyber team's approval. This includes changing settings, adding plugins or extensions, or any other modifications.

If users have any questions about whether a particular software or app is authorised, they should contact the IT and Cyber team for clarification.

Acceptable use

We expect staff to use our ICT services to support the work of the Council. All use of our ICT services should be consistent with this Acceptable Use Policy.

Misuse of our ICT services may lead to disciplinary and/or legal action as set out in the Disciplinary Procedure. Gross misconduct may result in dismissal from the council.

Data protection

Monitoring or accessing personal emails is in the council's legitimate interests and is to ensure that this policy on email/messaging/online communications and internet use is being complied with and/or the security of council ICT infrastructure. Monitoring or accessing personal emails may also be carried out where it is a task vested in the authority or a task carried out in the public interest such as for the prevention and detection of crime or fraud. For further information about how the data will be used please see the council's Privacy Notice.

The officer responsible for overseeing this policy is the Associate Director: IT and Cyber.

Monitoring will normally be conducted by the council's IT and Cyber Team. The information obtained through monitoring may be shared internally, including with members of the HR team, Associate

Directors or above and IT and Cyber team if access to the data is necessary for performance of their roles. However, information would normally be shared in this way only if the council has reasonable grounds to believe that there has been a breach of the rules set out in this policy.

The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted. Data is normally securely destroyed in line with the council's data retention policy.

Information obtained through monitoring will not be disclosed to third parties (unless the council is under a duty to report matters to a regulatory authority or to a law enforcement agency).

Employees and Members have several rights in relation to their data, including the right to make a subject access request and the right to have data rectified or, in some circumstances, erased. You can find further details of these rights and how to exercise them in the council's data protection policy. If Employees and Members believe that the council has not complied with their data protection rights, they can complain in the first instance to the council's Data Protection Officer and if they are still dissatisfied to the Information Commissioner.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ICT security

All users are obligated to immediately notify the IT and Cyber team of any security incidents and breaches.