IT POLICY

Introduction

Kidderminster Town Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer Usage Policy

Access to Council systems (I Drive/KTC network) is only permitted once the Computer Usage Policy has been read, understood, and signed. No individual is authorised to use council computers or access the I Drive or KTC network without having first completed this requirement.

Computer use

Hardware

- Council IT equipment is for official use; limited personal use is permitted only during breaks or outside work hours and must not disrupt council business.
- All users must lock devices when away from their desk; failure to do so may result in disciplinary action.
- All electronic equipment must be treated with care, kept clean, and protected from food and drink.
- All equipment will be asset-tagged and recorded in the council's asset register.
- Equipment must not be dismantled, modified, or reassembled without approval.
- Users must not purchase computer, mobile equipment, or software unless authorised.
- Personal storage devices (e.g., USBs, CDs, external drives) must not be used without CEO approval.
- Personal Wi-Fi hotspots that bypass council networks are prohibited.
- Any faults or required repairs must be reported to the Corporate Services Manager.

Equipment

Portable equipment

- Portable equipment includes laptops, tablets, and smartphones with email/internet access.
- Council backup procedures for portable equipment must always be followed.
- Portable devices must be stored securely, kept with the user where possible, never left unattended, and never left in parked vehicles.
- All portable devices holding council data must be encrypted and protected by a PIN; security settings must not be disabled.
- Multi-Factor Authentication (MFA) should be used to reduce the risk of unauthorised access and support data protection compliance.
- Any loss or damage to portable equipment must be reported to the Corporate Services Manager; users may be liable for costs if negligence is involved.

Use of personal devices (BYOD)

- Personal laptops or other devices must not be used to access council IT systems during working hours unless authorised by the CEO.
- The same security rules apply to personal devices as to council equipment.
- Work-related calls must be made using council phone numbers, and emails must be sent from a council email account (not personal addresses).
- All devices used to access council systems must be used ethically and in line with this policy; accessing inappropriate or illegal content via council infrastructure may result in termination or disciplinary action, regardless of device ownership.
- The council may take temporary possession of any device (council or personal) if required for legal proceedings.
- Users should keep a clear separation between council and personal data (use separate apps/profiles where available).

Data storage and handling

- Council personal data must not be stored on personal cloud accounts.
- Personal or sensitive council data must not be saved permanently on personal devices.
- Any data transferred via removable media (e.g., USB/CD) must be securely deleted after use.
- Cached copies of attachments must be deleted immediately after use.
- Before disposing of a device, or when leaving the council, users must allow the IT provider to remove all council data, passwords, and access shortcuts.

Responsibility and risk

- Users are responsible for understanding and following these rules when using personal devices for council work.
- The council will provide reasonable assistance, but users are personally responsible for risks or costs relating to their own devices.

Health and Safety

- Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.
- The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the council's expenses policy- Section 5.1.3

- Any VDU user who feels that their workstation requires changes to make it compliant must speak to the corporate services manager
- If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the corporate services manager or the IT provider

Password and Authentication Policy

Password Security

- All user accounts must be protected by strong, secure passwords.
- Multi-Factor Authentication (MFA) must be enabled wherever possible.

Password Creation and Management

- Initial user passwords must be generated by the IT provider.
- Default/vendor passwords must be changed immediately upon setup.
- Service/system account passwords are generated and managed by the IT provider.
- Council follows best practice to support compliance with UK GDPR and the Data Protection Act 2018 (see NCSC Password Guidance).

Access to Passwords

- Passwords are personal and must never be shared.
- Only the assigned user may use their account password.
- In exceptional circumstances, authorised IT personnel may access system credentials with appropriate approval and logging.
- Administrative credentials must be stored securely and restricted to authorised personnel.

Password Storage

- Passwords must not be stored in plain text or written in insecure locations.
- Passwords must be stored in a council-approved encrypted password manager.

Password Changes

- Passwords must be changed immediately if compromise is suspected.

Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Unauthorised attempts to access passwords will be treated as a security incident.

Responsibilities

- Users are responsible for maintaining secure passwords.
- The IT security provider is responsible for managing system credentials, enforcing policies, and auditing compliance.

Monitoring

- The council may monitor and log all computer, email, and internet use, and inspect any files stored on council systems to ensure policy and legal compliance.
- Monitoring is carried out in accordance with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.
- Monitoring will be necessary, proportionate, and based on a documented impact assessment, and is conducted in the council's legitimate interests.
- Information obtained through monitoring may be shared internally (e.g., councillors, IT staff) or with external HR/legal advisers where necessary and appropriate.
- Monitoring data will be retained only as long as necessary for any investigation or resolution of a breach.
- Users retain their data protection rights, including rights to access, rectify, or request erasure of their data, in line with the council's Subject Access Request policy.
- Monitoring may be used to check legitimate use, recover lost data, investigate wrongdoing, or comply with legal obligations.
- The council may inspect all files and monitor websites accessed, including outside working hours, to prevent misuse or reputational damage.
- Improper use of council systems may result in disciplinary action.
- All council computers will be regularly scanned for viruses and unauthorised software.

Remote Working

- Enhanced IT security measures apply when working away from council premises (e.g. travelling, working from home, or at other venues).
- When using non-council devices to access council systems, passwords must not be saved; users must log out and clear browser history/logs after use. If this cannot be done, council systems must not be accessed.
- Screens must be positioned to prevent others viewing confidential information.
- Any printed material must be collected and stored securely.

- Electronic files should be password protected and saved to council systems as soon as possible.
- Papers, files, or equipment must not be left unattended in non-council premises unless securely locked away.
- All data must be stored safely and disposed of securely.
- Council data or storage devices must not be left unattended in vehicles except for short, unavoidable periods, when they must be locked in the boot; overnight they must be taken into accommodation.
- Remote wipe capability should be enabled on mobile devices holding sensitive information where possible.
- Users working remotely with sensitive data should use a screen privacy filter on mobile devices at all times.

E-Mail

- Council email is provided for work purposes and should be used carefully to avoid security risks, including viruses.
- Email should not replace face-to-face or telephone communication where those are more effective.
- These rules aim to reduce legal risk; if unsure, users should seek guidance from the Corporate Services Manager.
- Users who require email for their role will be issued a council email account, which may be withdrawn if no longer needed or if misused.
- Council email accounts should be used only for council business; personal use is not permitted

Use of the Internet

<u>Copyright</u>

- Most material on the internet is protected by copyright; unauthorised copying (including software) is illegal and prohibited.
- Breaches of copyright may expose the council to legal action and may result in disciplinary action against individuals.
- The council will comply fully with copyright law and not "bend the rules."
- Users must not assume online material can be freely copied; public domain and copyright-free material are different.

- Website copyright conditions should be checked before downloading or copying material.
- If unsure about copyright or database rights, users must seek advice from the CEO.

Trademarks, links and data protection

- The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the CEO.
- Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection.

Use of Social Media

Social Media – General

- Social media includes blogs, wikis, video-sharing sites, social networks, messaging apps, virtual worlds, and traditional media. Care must be taken at all times when using social media.
- Personal use of social media during working hours should be limited to breaks (or outside working hours with permission).
- Use of social media for work-related purposes is acceptable where relevant to the role.

Standards of Conduct

- Inappropriate posts by employees (e.g., abusive, discriminatory, harassing, defamatory, or derogatory content) that could be associated with the council will be treated as a serious disciplinary matter, even if the council is not named. This applies to personal social media channels, as well as the Council's . For elected members, this may be a Code of conduct matter. For volunteers, their services may be discontinued.
- Users must be mindful that personal posts may be viewed by parishioners, partners, or the public.

Social Media Rules (apply to both personal and council use, at all times)

- Council contact databases must not be linked to personal social media accounts

- Any blog or post referring to the council must clearly identify the author and include a disclaimer that views are personal and not those of the council; users must not present themselves as speaking for the council.
- Users must act respectfully towards the council, its councillors, staff, and partners; unauthorised use of copyright or derogatory statements may constitute gross misconduct.
- Photos, videos, or audio recordings must not be taken or posted from council premises without permission; images of staff in council-branded clothing must not be posted if they could reflect negatively on the council.
- Online comments must be accurate, professional, and not compromise the council.
- Confidential, private, or internal council information must not be posted online; this includes personal data, internal documents, disciplinary matters, or sensitive operational/financial information.
- Users are personally liable for their online posts; councillors must observe the Members Code of Conduct and Nolan Principles; employees may face disciplinary action for inappropriate content.
- Posts must not breach copyright, defame individuals, or breach data protection law.
- Media enquiries relating to the council must be directed to the CEO or Corporate Services Manager.
- Social media profiles (e.g., LinkedIn/Facebook) must be accurate and updated on leaving the council.
- Professional contacts made through platforms such as LinkedIn in a council capacity are considered council property.

Monitoring and Data

- The council may monitor external social media postings. Users must not misrepresent their role with the council.
- Social media is not an appropriate forum for raising council complaints; these should follow formal procedures.
- External contact details remain council property; departing users must delete all council-related data and contacts from personal devices.

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.