The Use of Information and Communication Technology (ICT) Policy

Scope

This policy applies to **ALL** users of Shinfield Parish Council (SPC) ICT systems & equipment; whether this is at work, at home or elsewhere. This policy applies to employees, Councillors, contractors, temporary staff, agency staff or other staff and volunteers.

Policy

All users (including temporary, agency or other staff and volunteers) who breach any of the terms in this policy, deliberately or through negligence may be, where applicable, subject to disciplinary action.

Governance, ownership and review

- Policy owner: The Clerk (as Proper Officer) is responsible for maintaining this policy and associated procedures
- Approval: Shinfield Parish Council (Full Council).
- Review: This policy will be reviewed at least annually every FOUR years or sooner if there is:
    - A significant change to Council ICT systems
    - A change of IT Supplier
    - A significant change to legal/regulatory requirements

Introduction

Every user is responsible for the proper use of their SPC ICT software & equipment.

SPC equipment should not be used in any way for salacious, illegal, libellous or defamatory material or purposes that could bring the Parish Council into disrepute.

Legal and regulatory framework (UK)

This policy is intended to support compliance with applicable UK law and regulatory guidance, including (where relevant) the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR), the Computer Misuse Act 1990, copyright and intellectual property law, and employment/worker privacy expectations set by the Information Commissioner's Office (ICO). It should be read alongside the Parish Council's Data Protection Policy, Information Security arrangements and any published privacy notices.

Shinfield Parish Council

Definitions

- Council ICT systems: Any Council-owned or Council-managed device, account, application, cloud service, network, or data storage used for Council business (including systems provided by third parties on the Council's behalf).
- Council-approved systems: Systems and services authorised by the Clerk and/or the Council's contracted IT support provider for conducting Council business.
- Personal data: Any information relating to an identified or identifiable individual.
- Special category data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data (for identification), health data, sex life, or sexual orientation.
- Confidential information: Non-public Council information (including commercially sensitive information) and any information provided in confidence.
- Security incident / personal data breach: Any event that could compromise confidentiality, integrity or availability of Council systems/data (including loss/theft of devices, misdirected emails, unauthorised access, malware, or disclosure of personal data).

Responsibilities

Users of Shinfield Parish Council ICT facilities are responsible for:

- informing the Clerk, if you believe that others are using systems inappropriately
- notifying the Clerk and Air IT Service Desk if you think that someone else may be using your login details
- safeguard personal/confidential data and follow the Council's data protection and retention requirements
- report suspected data breaches, loss of devices, misdirected e-mails, or other information security incidents to the Clerk and ICT support without delay
- contacting the ICT Service Desk immediately in the event of a suspected virus infection
- ensuring that personal use of Shinfield Parish Council ICT equipment remains very occasional and reasonable and does not interfere with everyday workload and commitments or endanger the council's systems

Clerk & Line Managers responsibilities

- The Clerk and Managers are responsible for ensuring that all their employees and Councillors are aware of this policy and act in accordance with its requirements.

Shinfield Parish Council

Privacy

- The Council will respect users' privacy while ensuring Council systems are used lawfully and securely.
- The Council may monitor, log, and audit the use of Council ICT systems where it is necessary and proportionate for defined purposes such as
    - Protecting the security of systems and information,
    - Investigating suspected misuse or unlawful activity
    - Meeting legal/regulatory obligations, and
    - Ensuring business continuity.
- Access to user accounts/mailboxes during an individual's absence will only take place when there is a legitimate business need (for example, continuity of service), using an authorised process approved by the Clerk (or delegated manager).
    - Any access will be limited to what is necessary, and an appropriate record of the access will be kept.
- The Council reserves the right to monitor or obtain access logs from its IT Support provider (AIR IT) should there be reasonable suspicion of inappropriate activity during work hours involving parish council ICT equipment.
    - All information and data will be securely maintained by the Clerk and retained only for as long as necessary.

Legislation

- Information created/stored using council systems may be disclosable under:
    - Freedom of Information Act 2000
    - Environmental Information Regulations 2004
    - Subject Access Requests under data protection law
    - And any other relevant legislation
- Information created, received, or stored for Council business is a Council record, regardless of the device or account used

Shinfield Parish Council

Security & Integrity of Systems & Equipment

- Use of Shinfield Parish Council ICT equipment and access to Council systems must be authorised by the Clerk or another person authorised by the Council
    - Access will be granted on a need-to-know basis and only to the level required for the role
    - Access rights will be reviewed and removed promptly when roles change or end
- As a user, you will be issued with one user ID and associated passwords to enable authorised use.
    - Your user ID is intended for your use alone.
    - You must not permit its use by others except when required to do so in order to carry out an authorised Business Continuity Plan.
- Users must ensure that they:
    - Use strong passwords/passphrases (at least 10 characters, mix of numbers, letters, capitals and lower case and punctuation marks)
    - Never share passwords or other logins
    - Use multi-factor authentication (MFA) where available
    - Change passwords promptly if you suspect compromise or if directed by ICT support.
    - Do not remove security measures on any system.
    - Logout or lock your computer if you leave your workstation unattended.
    - Users of laptops must ensure that a PIN or password is required to use the device.
    - You must not use ICT facilities to access, transmit or share material that is confidential to Shinfield Parish Council, or is confidential to an individual, without the appropriate permission.

users are responsible for safeguarding credentials and may be subject to action where misuse results from deliberate breach or negligent failure to follow the policy.

- You **MUST**:
  - Obtain authorisation from the Clerk, Deputy Clerk or IT Officer, then contact the Council's contracted IT support provider for the installation of additional software on Council equipment
  - if you have a standalone machine, make sure it is registered with the ICT Service Desk for regular updates of anti-virus software
  - Make sure that all critical documents are held on a network drive rather than the PCs/laptop's hard drive
    - Council data must be stored in approved locations that are subject to managed backup/version control where provided
    - Users should not rely on local/manual copies as the primary record
    - Restore arrangements are managed through council systems/ICT support
  - If a Council device is lost or stolen (or you suspect unauthorised access), report it to the Clerk AND ICT support immediately so accounts can be secured and remote wipe/lock actions can be taken where available.
- You **MUST NOT**:
  - Change the configuration of installed ICT equipment UNLESS authorised to do so.
  - Access or attempt to access any ICT system for which you are not an authorised user.
  - Access any data (included personal data of residents, councillors or staff) UNLESS authorised to do so for work reasons.
  - Connect non-Council equipment to the Council network or Council-managed services UNLESS authorised to do so
  - Remove office-based ICT equipment or software without authorisation from ICT Services
  - Let friends or family use Council equipment assigned to you
  - Connect any digital media devices or load their associated software UNLESS there is a legitimate need for business purposes and this is authorised
  - Use removable media (e.g., USB sticks, external drives) UNLESS there is a legitimate business need and it is approved by the Clerk/ICT support (for example providing CCTV to Thames Valley Police)
    - Where permitted, removable media must be encrypted and kept secure.
  - Play or copy CDs/DVDs UNLESS there is a legitimate need for business purposes.

Shinfield Parish Council

Physical Security

- Users are responsible for the physical security of devices issued to them
  - Do not leave devices visible in cars
  - Keep devices secure in public places/home
  - Use privacy screens where appropriate
  - Take care when taking confidential calls in public/shared spaces

IT Training

- Users must
  - Complete all required ICT/data protection/cyber awareness training
  - Comply with security notices/instructions issued by the council or IT provider

Procurement & Licensing

- Unless specifically authorised by the Clerk, Deputy Clerk, Media & Communications Officer or ICT support provider, users must not use unapproved cloud services, AI tools, storage platforms, or software-as-a-service tools for Council business

Cyber Incidents

- In the event of any suspicious or malicious occurrences on your device e.g.
  - Ransomware
  - Suspicious pop-ups / account lockouts
  - Business email compromise / fraudulent payment requests
- Do NOT attempt to resolve the issue yourself
- You MUST
  - Disconnect from network/Wi-Fi if serious compromise suspected (where instructed)
  - Stop using the device
  - Report immediately
  - Not delete evidence or attempt to fix it themselves unless directed by ICT support

Shinfield Parish Council

Use of e-mail

- Users must not e-mail Council confidential information or personal data outside of Council-approved systems UNLESS appropriate safeguards are in place (for example, approved secure sharing, encryption, or password protection provided via an agreed method)
    - Where passwords are used, they must be shared via a separate channel and in line with Council procedures
- Council business should be conducted through council-approved accounts and systems wherever possible
- If council business is unavoidably conducted through a personal account/device, the record must be transferred promptly into council systems
- Users must cooperate with lawful retrieval/search of council records held in personal accounts/devices where those records relate to council business
- Users should
    - Maintain good data housekeeping e.g. deleting unwanted e-mails etc.
    - Look out for phishing scams; check the sender's email address.
    - Take care with recipients:
        - Check addresses before sending,
        - Use BCC where appropriate to avoid disclosing recipients, and
        - Avoid using large distribution lists unless necessary.
    - If you send an email or attachment to the wrong recipient, report it to the Clerk and ICT support immediately and follow the Council's incident/breach procedure.
    - Comply with the e-mail data archiving and retention policies as published.
- Users should NOT:
    - Click on any suspicious links within emails
    - Set up automatic forwarding of Council email to personal email accounts, and do not routinely forward Council emails or attachments to personal accounts.

Use of messaging apps

- Messaging apps include WhatsApp, Texts, Teams and similar applications
- Messaging apps may only be used for council business where approved
- They must not be used to make decisions outside proper governance processes
- Any substantive council business conducted via such channels must be captured into council records

Shinfield Parish Council

Use of AI

- Artificial intelligence (AI) tools may only be used for Council business where their use has been approved by the Clerk, Deputy Clerk or the Council's ICT support provider and where that use is lawful, proportionate and appropriate to the task.
- AI tools may assist with low-risk tasks such as drafting, summarising, formatting, transcription, research support or generating ideas, but they must not be treated as a substitute for professional judgement, officer decision-making, legal advice or proper governance processes.
- Users must not enter into public or unapproved AI tools any Council confidential information, personal data, special category data, unpublished Council documents, commercially sensitive information, passwords, security details, or any information provided in confidence, unless specifically authorised and subject to an appropriate risk assessment and any required data protection measures.
- AI outputs must be checked carefully for accuracy, bias, completeness, confidentiality and appropriateness before being relied upon, circulated, published or used to inform Council business. Users remain personally responsible for the content they submit, amend, approve or send onwards.
- Where outputs are predominantly AI generated this should be clearly stated at the start of the document
- AI must not be used to make, or appear to make, decisions about individuals, including residents, staff, contractors or councillors, where human review and accountability are required.
- Where AI is used to support the creation of a substantive Council document, report, communication or record, the responsible user must ensure that the final version is reviewed, corrected where necessary, and stored in the appropriate Council record system in line with Council procedures.
- Any proposal to adopt or procure a new AI-enabled system or service for Council business must be approved through the Council's normal governance, procurement, information security and data protection processes before use.

Shinfield Parish Council

Working at home/remote working using Council or personal equipment

This policy applies to employees when working from office, home or other location. Work carried out must always be with due regard to the terms of this policy and to data protection/ confidentiality issues.

- Confidential data and documents must not be stored long term on non-Shinfield Parish Council equipment.
- Very sensitive documents additionally should be password protected or otherwise encrypted to prevent unauthorised access.
- Do not share passwords. If encrypted information needs to be recoverable for business continuity, use an approved method (for example, a Council-managed password vault) as agreed with the Clerk and ICT support.
- Where personal devices (BYOD) are approved by the Clerk or Deputy Clerk for Council business, they must be:
    - Protected with a strong PIN/password,
    - Kept up to date (security patches), use device encryption where available, and support remote wipe/lock if required.
    - Cleared of all Council information when no longer needed or when requested (e.g., on leaving office/role).
    - Access may be withdrawn if the device is non-compliant

Data handling, storage and retention

- Store Council documents and records in Council-approved locations (e.g., Council file store/SharePoint/OneDrive as configured) rather than on local hard drives or personal email accounts.
- Do not use email as the long-term filing system for Council records, file important correspondence and attachments in the appropriate Council record location in line with Council procedures.
- Only collect, access and share personal data that is necessary for Council business.
    - Take extra care with special category data.
- When printing or working with paper records, keep them secure, avoid leaving them unattended, and dispose of them via secure shredding/confidential waste as applicable.
- Keep information only for as long as required and dispose of it securely in line with the Council's retention schedule.

Shinfield Parish Council

Social media and public communications

When using social media or other public communications in connection with Council business (including where you identify yourself as acting for the Council), you must:

- Be accurate
- Respectful and lawful, and
- Protect confidential information and personal data.

Only authorised officers/councillors may post on official Council accounts. These are:

- Clerk
- Deputy Clerk
- Media and Communications Officer
- Community Engagement and Events Officer
- Allotments Officer

Council business conducted via social media may constitute a record and must be retained in line with Council procedures.

Use of the Internet

Guidelines for acceptable use:

- Never attempt to access illicit or inappropriate web sites.
  - Inform your manager straight away if you accidentally access an illicit/inappropriate website
  - Our IT provider will flag and block most sites and inform the Clerk or IT Officer
- Respect the laws protecting copyright and intellectual property rights.
  - Downloading and storage of copyright material like music and video files may be illegal.
  - Where such files are found on ICT equipment without a bona fide business reason, files will be deleted.
- The council's ICT equipment and services should not be used for personal business activity, fundraising or advertising
- Access of non-work-related websites is permitted only in your own time.
  - Repeatedly access non-work-related websites while working for the council may result in disciplinary proceedings
- Accessing personal webmail in the user's own time is acceptable, provided personal emails are not stored on Parish Council systems and equipment.
  - This should only be done infrequently
- You must not use peer-to-peer file sharing technologies
- Instant messaging is not permitted other than using Council-supplied systems.
- Selling or taking part in online auctions etc is not permitted
- On-line gambling is not permitted

Shinfield Parish Council

Personal Use of Systems and Equipment

Examples of the acceptable personal use of systems are:

- **Limited** communications with family/friends
- Communications with professional service providers who are normally only contactable during standard office hours
- Communication with further education establishments and work-related professional associations
- Further education/learning opportunities/knowledge development with recognised institutions
- Online shopping from a secure site is permitted in user's own time.
    - Users must not have goods delivered to work, unless advance permission is given by the line manager.
    - The Council has no liability for any such transaction.
- Users need to make it explicit that they are buying goods for their own personal use and not on behalf of the Council.
- Employees must not use their status as employees of the Council to their personal advantage in ordering goods, etc.

Users of phones/mobile phones should ensure that:

- Private phone calls are restricted to non-work time wherever possible
- They adhere to the Council's specific policy on Mobile phone use in relation to driving
- They never use mobile phones to distribute, receive or store any material which is offensive or prohibited
- Personal calls and texts are paid for when using Council equipment

Monitoring

- Information about use of Council ICT systems (for example, log-in activity, device inventory, security alerts, network traffic metadata, and e-mail filtering outcomes) may be logged for defined purposes such as security, service management, legal/regulatory compliance, and investigation of suspected misuse.
- Automated controls may be used to protect the Council and users (for example, malware scanning, spam controls and filtering of inappropriate content) consistent with this policy.
- Access to monitoring logs will be restricted to authorised personnel (for example, the Clerk, delegated managers, and ICT support) and only where needed for the defined purpose.
- Monitoring will be proportionate and targeted where possible. Where investigation requires access to content (rather than logs/metadata), this will only occur where there is a clear, documented reason and appropriate authorisation.
- Logs will be retained in line with the Council's retention schedule and deleted securely when no longer required. Further details are provided in the Council's relevant privacy notice(s) and procedures.

Misuse of ICT equipment or systems

Where users make inappropriate or excessive personal use of systems or there is persistent or serious misuse, disciplinary action may result that could lead to dismissal. Where equipment or systems are used to access or engage in illegal activity, the police will be informed, and disciplinary action will also be taken.

Other related policies and documents (where adopted/published by the Council):

- Data Protection Policy and published privacy notices
- Information Security Policy / Information Security arrangements (including incident reporting)
- Records Management Policy and Retention Schedule
- Disciplinary Policy/Procedure (employees) and standards expected of councillors
- Councillor Code of Conduct and Officer/Staff Code of Conduct (where applicable)
- Complaints, Grievance and Whistleblowing (Raising Concerns) procedures

Leaving or Changing Roles

When a user of Council systems leaves or changes their role then:

- Accounts/access will be removed or amended promptly
- All council equipment must be returned
- Council information must be returned/deleted from personal devices/accounts where applicable