**Kingston on Soar Parish Council – IT Policy**

Adopted May 2025

**Introduction**

Kingston on Soar Parish Council recognises the importance of effective and secure information

technology (IT) usage in supporting its business, operations and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources

by council members, employees, volunteers, and contractors.

**Scope**

This policy covers the use of IT, both hardware and software, for all councillors, employees and third parties acting on behalf of the Council (Users), and the safekeeping of data.

**Definitions**

*Users* – councillors, employees and third parties acting on behalf of the Council.

*Data* – digitally stored information including (but not limited to) documents, images, personal information and accounting information.

*IT hardware/software* – includes, but is not limited to computers, internet access, remote access connections, email systems, file storage, webmail, smart phones, telephones, website, mobile phones etc.

**IT provision**

Any provided device, software, data access and services provided remain property of the Council and shall be recorded on the asset register. At the end of any period of holding office, employment with or work for the Council, all provided equipment must be returned to the Clerk, Chair or Vice-Chair within 14 days.

Users must comply with all relevant policies, procedures and UK legislation with respect to the use of IT hardware.

All IT provision should:

* demonstrate value for use of Council money;
* provide value for Council or clerk use, whilst enabling efficient working and not contributing to secondary waste;
* include consideration of cost vs time spent carrying out tasks which could be offset by the use of technology;
* maintain privacy of councillors, Council employees, subcontractors and parishioners.

A review of the Council’s IT requirement should be conducted at least every four years, when council elections take place and new councillors take office, or within three months of new members of staff starting with the Council.

**Privacy and data protection**

Users must:

* not leave their user accounts logged in on an unattended and unlocked device;
* use suitability secure methods for storing and accessing data and services;
* not perform any unauthorised changes to the IT systems or information; changes must only be made with agreement from the Chair and at least one other councillor, or at full Council where applicable;
* not attempt to access or use data or software that they are not authorised to use or access;
* not give or transfer Council data or software to any person or organisation outside the Council without the appropriate authority and reason to do so;
* adhere to the Data Protection Policy and Records Retention Policy;
* use antivirus software and keep this up to date;
* comply with all relevant policies, procedures and UK legislation with respect to the use of IT software; if unsure about this then users should check with the Clerk or Chair.

Where users use their own hardware to access Council systems or data they are responsible for ensuring the security of systems and data as per this policy, the Data Protection Policy and the Records Retention Policy.

An email address will be provided to all councillors and Council employees and this should be the only address used for official Council correspondence.

Personal use is not permitted for any Council provided communication services, software applications (downloaded or software as a service) or data, unless such data is already in the public domain.

Any correspondence undertaken on behalf of the Council on Council provided or personal devices or services, where retained in line with the Records Retention Policy, should be provided upon request to the Clerk or Chair, particularly, but not limited to the case of a Freedom of Information request.

**Passwords and access to systems and services**

Passwords should be either a minimum of 8 random letters, numbers or symbols, or four random words joined with non-alphanumeric characters.

Where a service offers two factor authentication then this must be used, if possible with a hardware security key or software two factor authentication (e.g. google authenticator) secured by a strong log-in or password.

Where a device is provided for a reasonable period of time to a Councillor or employee of the Council and this device offers biometric authentication, then this should be activated under a Council managed account.

**Risk Management**

As part of its risk management the Council maintains insurance on the equipment provided.

All equipment must be secured from theft or unauthorised use as far as is practical.  When travelling with equipment, it should not be left in an unattended vehicle unless there is no other option, in which case it should be secured out of sight.

Any loss of, or damage to equipment should be reported as soon as possible to the Clerk and Chair and any criminal damage will be reported to the Police by the Clerk.

Any loss of personal data as the result of loss or theft of equipment shall be reported to the Clerk and Chair and Information Commissioner’s Office (ICO).

An annual risk assessment should be undertaken regarding use and security of Council IT hardware, software and stored data.

**Application of the Policy**

Not adhering to the terms set out in this policy may result in disciplinary proceedings.