Sarratt Parish Council

Policies and Procedures: Information & IT Systems & Data Security

Sarratt Parish Council holds a wide range of information, including data about other organisations and personal data about individuals in paper and / or electronic format. The Council needs to maintain public confidence by ensuring any information it processes, maintains and/or shares with other public-sector organisations is protected by appropriate levels of information security and is used for legitimate purposes.

This document describes the Information and Security Policy adopted by Sarratt Parish Council.

The objective of this policy is to ensure that appropriate standards of information security are always maintained across the Council such that:

- the public and all users of the Council's information and IT systems are confident of the security, integrity and availability of the information used and produced
- damage and interruption caused by security incidents are minimised
- all legislative and regulatory requirements are met
- the Council's equipment and facilities are always used responsibly, securely and with integrity.

This policy adopted by Sarratt Parish Council covers the following sub-policies:

- Email
- Internet Acceptable Usage
- Software
- IT Access
- Information Protection
- Computer, Telephone and Desk Use
- Legal Responsibilities
- Remote Working
- Removable Media
- Information Security Incident Management
- Office 365 Account
- Cybersecurity

The sections below cover each of the individual sub-policies, highlighting key messages that all staff and Councillors need to be aware of when using electronic systems and sharing information with partner organisations.

All staff and Councillors are required to read and understand their obligations as outlined in this policy document to confirm:

- That they have read and understood these key messages.
- That they understand the consequences of failure to comply with these policies.

- That they understand they have a responsibility to familiarise themselves with the information.

Email Policy:
Sarratt Parish Council will ensure all users (Councillors and staff) of Council email facilities are aware of the acceptable use of such facilities:

- E-mail address will be first name, followed by a full stop then surname, followed by @sarrattparishcouncil.gov.uk
- Individuals are responsible for ensuring the security of their email login identity and password and must not disclose their password or share accounts with colleagues.
- Individual user login identity and passwords must only be used by that individual user, and they must be the only person who accesses their email account.
- Users should not use non-work email accounts to conduct or support official Council business.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, offensive, or obscene.
- When an email from a suspicious source or with an odd or unexpected subject title is received, it should be treated with suspicion and, if unsure on how to proceed, referred to the Council's Data Protection Officer (DPO)
- An email has the same legal status as a paper document and may be disclosed under the GDPR or the Freedom of Information Act 2000. Further information on this can be obtained from the Council's Data Protection Policy or by contacting the Council's DPO.
- All official external e-mail will carry the official Council disclaimer.
- Automatic forwarding of email is not permitted to prevent confidential material being forwarded inappropriately.

Internet Acceptable Usage Policy:
Sarratt Parish Council will ensure all users of Council provided internet facilities are aware of the acceptable use of such facilities:

- Internet and email access is an important aide to productivity, but private internet and e-mail usage by Council staff must be in their own personal time.
- Individuals must not create, download, upload, display or access, sites that contain material that might be deemed illegal, obscene or offensive.
- Individuals must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.

Software Policy:
Sarratt Parish Council will ensure the acceptable use of software by all users of the Council's computer equipment or Information Systems.

- Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
- Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.
- Individuals are not permitted to bring software from home (or any other external source) and load it onto Council equipment.
- Security software firewalls must be used where available.
- Individuals must not attempt to disable or reconfigure the firewall or other security software on the Council's computer equipment.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

IT Access Policy:

Sarratt Parish Council will establish specific requirements for protecting information and information systems against unauthorised access and effectively communicate the need for information and information system access control. All staff and Councillors will have and use individual passwords.

- When setting up a new password, this must consist of 8 characters, a mixture of letters and numbers. At least one of the letters must be a capital letter.
- Passwords must be protected at all times.
- If individuals leave their desk, they must lock or log out from their computer.
- It is an individual's responsibility to prevent their user ID and password being used to gain unauthorised access to the Council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Council's equipment without permission from the Council.

Information Protection Policy:

Sarratt Parish Council will ensure the protection of all information within the custody of the Council. High standards of confidentiality, integrity and availability of information will be maintained at all times.

- Personal information will only be collected and processed when essential for Council business, and only for purposes defined in the Council's GDPR Policy and Privacy Notices.
- Anti-malware software has been installed onto the hardware being used within the Council office.
- The personal data held by the Council is backed up weekly to a cloud server in which restricted access has been created only for database administrators and IT support personnel. This copy is also held offsite to support the data recovery controls and procedures organised by the Council.
- Access to cloud applications used for the administration of payroll is accessed via segregated individuals using password security.
- Where information is shared or disclosed, it should only be done so in accordance with the Council's GDPR Policy and Privacy Notices
- Retention of information is to be handled in accordance with the Council's GDPR Policy, Privacy Notices, Data Retention Policy and Data Retention Schedule.
- Information should be destroyed appropriately.
- The Council must draw up and maintain inventories of all important information assets.

Computer, Telephone and Desk Use Policy:

Sarratt Parish Council will ensure that users are aware of, and understand, the acceptable use of the Council's computer and telephony resources and the need to operate a "clear desk" environment.

- Any IT equipment provided by the Council is for use on official business only.
- Where possible, private telephone calls should be made outside working hours.
- When driving on Council business, individuals must not answer a mobile phone, whether or not it is a hands-free set. The vehicle should be safely parked, and the engine turned off before answering or returning a call.
- When leaving the office for a period of time, or at the end of the working day, desks and other surfaces should be cleared of any information not for pubic viewing and stored in locked cabinets and drawers.

Legal Responsibilities

Sarratt Parish Council sets out the responsibilities of all staff under separate policy documents addressing the requirements of the GDPR and Freedom of Information Act 2000 and other relevant legislation.

- All Councillors and staff must accept responsibility for maintaining Information Security standards within the Council.

Remote Working Policy (Information Security)

Councillors and staff (as approved by the Council) may be allowed to work remotely in order to carry out Parish business.
Sarratt Parish Council will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

- Staff and Councillors should not email Council information or documents to their private email addresses to work on.
- Individuals may use their own home equipment when required for Council Business, but any Council data stored on the equipment should be appropriately managed in line with the Council's Data Retention Policy
- If individuals use a laptop or device provided by the Council it must not be used by other members of their family.
- If individuals need to take confidential or sensitive information off-site, they must get authorisation from the Council. This should be avoided where at all possible.
- Care and attention must be taken to protect against damage, loss or theft, when transporting equipment and data between, the Council office, home, and remote locations.

Removable Media Policy:
Sarratt Parish Council will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business. Removable media devices include: memory stick/USB keys, writeable CD/DVD, laptops, smartphones, cameras, memory cards, tapes, floppy disks.

It is Sarratt Parish Council policy to limit the use of removable media devices.
The use of removable media devices will only be approved if it is required for Council business.

- All data stored on removable media devices must be accessible by the DPO if needed and encrypted when required.
- Damaged or faulty removable media devices must not be used.
- If a CD or memory stick is received from a third party it must be virus checked using anti-virus software updated to current version prior to insertion into Council equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage.
- When not in use a Council owned storage device must be kept in a locked drawer / cabinet where there is no public access (e.g. the Parish office, or the Clerk's / Councillors' home).

Information Security Incident Management:
Sarratt Parish Council will ensure that it reacts promptly and appropriately to any actual or suspected incidents relating to information systems and information within the custody of the Council. Further detail on this can be found in the Council's Data Breach Policy.

Office 365 Accounts:

- All Office 365 accounts must be protected by a password.
- When an Officer ceases to be employed by the Council, access to their Office 365 account will be removed. Access to the account will usually be given to their replacement or another Officer.
- All updates to operating systems, security software, and applications used for Council work must be updated as soon as reasonably practical after they are made available by the manufacturer.

Cybersecurity Policy

When a Councillor ceases to be a member, or an Officer ceases to be employed, they must remove all Council data from all their devices. Similarly, when a Councillor or Officer no longer uses a device for Council business, all Council data on that device must be returned.

Data removal must be by either:

- physical destruction of the data storage,
- or wiping with a suitable utility.
- In addition, Council data must be permanently deleted on any associated cloud storage (other than the Council's Office 365 system).

If required by the Council or the Clerk, the Councillor or officer must sign a statement that all data has been removed.

Reviewed and adopted: 13 February 2024