Selsey Community Forum
IT Security Policy

Introduction

Selsey Community Forum relies on information technology, electronic communications and digital information to support its activities. The purpose of this Policy is to establish appropriate security standards for the use of Selsey Community Forum's IT systems, devices, networks, accounts, applications and information.

Effective IT security depends on both technical controls and responsible user behaviour. All users therefore have a responsibility to protect Selsey Community Forum's systems and information from loss, unauthorised access, misuse, cyber attack and other security threats. This Policy should be read alongside Selsey Community Forum's Data Protection Policy, Communications and Social Media arrangements, and any other relevant policies or procedures relating to information security, confidentiality and the use of technology.

Scope

This Policy applies to employees, workers, agency workers, contractors, consultants, Trustees, volunteers and any other individuals who have authorised access to Selsey Community Forum's systems, devices or information. It applies to:

- computers, laptops and tablets;
- mobile phones;
- servers and networks;
- email and messaging systems;
- cloud services;
- business applications;
- websites and online accounts;
- removable media;
- remote-access systems;
- personal devices authorised for business use; and
- any other technology used to access, store or process Selsey Community Forum information.

User Responsibilities

Users must:

- use Selsey Community Forum's IT systems lawfully and responsibly;
- comply with applicable security and data protection requirements;
- follow reasonable security instructions;
- protect passwords, passkeys, authentication devices and access credentials;
- use only authorised systems and software;
- take reasonable care of devices and equipment;
- remain alert to phishing, fraud and other cyber threats;
- report suspected security incidents promptly; and
- avoid any action that could compromise the security, availability or integrity of Selsey Community Forum's systems or information.

Users must not deliberately bypass security controls or attempt to gain access to systems, information or accounts they are not authorised to use.

Access Control

Access to systems and information will be granted according to business need and the responsibilities of the individual concerned. Selsey Community Forum will seek to apply the principle of least privilege so that users are given access only to the systems and information reasonably required for their roles. Access rights may be reviewed periodically and when:

- an employee changes role;
- responsibilities change;
- access is no longer required;
- employment or engagement ends; or
- a security concern arises.

Privileged or administrative access should be restricted to appropriately authorised individuals.

Passwords, Passkeys and Authentication

Users must protect access credentials and must not knowingly allow another person to use their account. Where available and appropriate, Selsey Community Forum may use:

- passkeys;
- multi-factor authentication;
- two-step verification;
- passwords;
- biometrics;
- authentication applications; or
- other secure authentication methods.

Passwords should be strong and unique and should not be reused across unrelated business and personal accounts. Users must not share passwords or authentication codes unless an authorised technical process specifically requires it. Default passwords supplied with systems or devices must be changed before use where appropriate.

Where a user suspects that a password, passkey, authentication code or account has been compromised, the matter must be reported promptly and access credentials changed where appropriate. Password managers approved by Selsey Community Forum may be used to store credentials securely.

Multi-Factor Authentication

Multi-factor authentication or another suitably strong authentication method should be enabled where available and proportionate, particularly for:

- email accounts;
- cloud services;
- remote access;
- administrator accounts;
- HR or payroll systems;
- financial systems; and
- other systems containing sensitive or important information.

Users must not approve an unexpected authentication request. Unexpected login prompts, authentication requests or security alerts should be treated as potential security incidents and reported where appropriate.

Software and Security Updates

Software, operating systems, applications, firmware and other technology should be kept appropriately supported and updated. Security updates should be installed within a reasonable period having regard to:

- the seriousness of the vulnerability;
- the importance of the affected system;
- supplier recommendations;
- compatibility requirements; and
- operational risk.

Automatic updates should be enabled where appropriate. Unsupported or obsolete systems should be replaced, upgraded, restricted or otherwise appropriately managed. Users must not deliberately disable security updates or security controls without authority.

Software Installation

Users must not install unauthorised software, browser extensions, applications or other programs on Selsey Community Forum systems. Software should only be installed where it:

- is required for legitimate business purposes;
- has been appropriately authorised;
- is obtained from a legitimate source; and
- does not create an unacceptable security, licensing or data protection risk.

Selsey Community Forum may restrict users' ability to install software through technical controls.

Malware Protection

Selsey Community Forum will use appropriate technical measures to reduce the risk of malware, ransomware and other malicious software. Depending on the systems in use, these measures may include:

- anti-malware or endpoint protection;
- firewalls;
- email filtering;
- web filtering;
- application controls;
- security updates;
- access controls; and
- system monitoring.

Users must not deliberately introduce malicious software or disable malware protection. Any suspected malware infection must be reported promptly. Where appropriate, users should disconnect or stop using an affected device and follow instructions from Selsey Community Forum or its IT support provider.

Phishing and Fraudulent Communications

Users must remain alert to suspicious emails, messages, calls and websites. Indicators of phishing or fraud may include:

- unexpected requests for passwords or authentication codes;
- urgent requests for payment;
- changes to bank details;
- unexpected attachments or links;
- unusual login notifications;
- messages requesting confidential information;
- impersonation of colleagues, suppliers or senior managers; or
- requests that depart from normal procedures.

Users must not provide passwords or authentication codes in response to an unexpected request. Requests involving payments, bank-detail changes or other high-risk transactions should be independently verified using an established contact method where appropriate. Suspicious communications should be reported promptly.

Email Security

Selsey Community Forum's business email accounts should be used for business communications where reasonably practicable. Users must take reasonable care when sending email and should:

- verify recipients before sending;
- check attachments before transmission;
- use appropriate security for sensitive information;
- avoid sending information to unnecessary recipients;
- be cautious when using "reply all";
- remain alert to impersonation and phishing;
- use approved file-sharing systems where these are more appropriate than email; and
- comply with confidentiality and data protection requirements.

Users must not routinely send Selsey Community Forum documents or confidential information to personal email accounts unless specifically authorised. Personal information should only be transmitted using security measures appropriate to its sensitivity and risk.

Internet Use

Internet access provided by Selsey Community Forum is intended primarily for legitimate business purposes. Reasonable personal use may be permitted where this does not:

- interfere with work;
- compromise security;
- incur unreasonable cost;
- breach another policy;
- expose Selsey Community Forum to legal or reputational risk; or
- involve unlawful or inappropriate material.

Users must not use Selsey Community Forum's systems to access, download, create or distribute unlawful material.

Cloud Services and File Sharing

Only approved cloud storage, collaboration and file-sharing services should be used for Selsey Community Forum information. Before confidential, commercially sensitive or personal information is stored or shared through a cloud service, appropriate consideration should be given to:

- access controls;
- authentication;
- data protection;
- security;
- supplier arrangements;
- sharing permissions;
- retention; and
- client or contractual requirements.

Users must not transfer business information into personal cloud-storage accounts unless specifically authorised.

Removable Media

Use of USB devices, external hard drives and other removable media should be limited to legitimate business needs. Where removable media is used, appropriate security measures may include:

- using authorised devices;
- encryption;
- malware scanning;
- secure storage;
- secure disposal; and
- limiting the data stored.

Unauthorised or unknown removable media must not be connected to Selsey Community Forum systems.

Devices and Physical Security

Users are responsible for taking reasonable care of devices provided to them.
Devices must:

- be protected by an appropriate locking or authentication method;
- be locked when left unattended;
- be stored securely where practicable; and
- not be left unnecessarily exposed to loss or theft.

Portable devices should not normally be left unattended in public places. Where a device is temporarily left in a vehicle, users should take reasonable steps to reduce the risk of theft, including keeping the device out of sight. Lost or stolen devices must be reported promptly. Where appropriate, Selsey Community Forum may use device management, encryption, remote-locking or remote-wiping capabilities.

Personal Devices and Bring Your Own Device

Employees must not use personal devices to access or store Selsey Community Forum information unless such use is authorised.

Where personal devices are permitted for business use, Selsey Community Forum may impose security requirements including:

- device passwords or biometrics;
- encryption;
- supported operating systems;
- security updates;
- approved applications;
- separation of business and personal information;
- multi-factor authentication;
- remote-access controls; and
- remote removal of business information where technically appropriate.

Users remain responsible for protecting Selsey Community Forum information accessed through personal devices. Selsey Community Forum will not normally require access to purely personal information unless there is a lawful and proportionate reason to do so.

Remote Working

Users working remotely must take appropriate steps to protect Selsey Community Forum's information and systems. This includes:

- using secure devices;
- following authentication requirements;
- taking care when using public or shared networks;
- preventing unauthorised individuals from viewing confidential information;
- locking screens when unattended;
- securely storing equipment and documents; and
- following any applicable Selsey Community Forum remote-working and information-security requirements.

Users should avoid discussing confidential information where conversations can easily be overheard.

Data Storage and Protection

Business information must be stored in systems or locations authorised by Selsey Community Forum. Users must take reasonable steps to prevent:

- unauthorised access;
- accidental disclosure;
- loss;
- alteration;
- destruction; or
- inappropriate sharing.

Security measures should reflect the sensitivity of the information concerned. Personal data must be handled in accordance with Selsey Community Forum's Data Protection Policy and applicable data protection legislation. Users should avoid storing unnecessary duplicate copies of sensitive information.

Encryption

Encryption should be used where appropriate to the sensitivity of the information and the risks associated with its storage or transmission. This may include encryption of:

- laptops or mobile devices;
- removable media;
- sensitive files;
- backups; or
- data transmitted electronically.

The level of protection required will depend on the nature of the information and the systems involved.

Backups

Selsey Community Forum will maintain appropriate backup arrangements for important business information and systems. Backup arrangements should, where proportionate:

- cover information required for business continuity;
- operate at an appropriate frequency;
- be protected from unauthorised alteration or deletion;
- avoid unnecessary dependence on a single copy or location;
- be secured appropriately; and
- support restoration following loss, corruption or cyber-attack.

Restoration arrangements should be tested periodically where appropriate. Users must store business information in approved locations so that applicable backup arrangements can operate effectively.

IT Asset Management

Where appropriate, Selsey Community Forum will maintain records of significant IT assets such as:

- computers;
- laptops;
- mobile devices;
- servers;
- business-critical systems; and
- other important technology.

Equipment issued to users remains the property of Selsey Community Forum unless otherwise agreed. Users must return company equipment when requested and on termination of employment or engagement.

Supplier and Third-Party Access

External IT providers, contractors and other suppliers should only be given access to Selsey Community Forum's systems where this is reasonably required. Access should be:

- appropriately authorised;
- limited to what is necessary;
- subject to suitable security controls; and
- withdrawn when no longer required.

Where suppliers process personal data or other sensitive information, appropriate contractual and data protection arrangements must be considered.

Artificial Intelligence and Online Tools

AI tools, online applications and other third-party digital services must only be used in accordance with Selsey Community Forum's applicable policies and approval arrangements. Users must not upload confidential, personal or sensitive information into an AI system or online service unless its use for that purpose has been appropriately authorised. Any use of artificial intelligence or online tools involving confidential, personal or sensitive information must comply with Selsey Community Forum's applicable data protection and information-security requirements.

Cyber Security Incidents

Users must report suspected or actual security incidents promptly. Examples include:

- lost or stolen equipment;
- compromised passwords or accounts;
- unexpected login alerts;
- phishing;
- malware or ransomware;
- unauthorised access;
- accidental disclosure of information;
- suspicious system behaviour;
- unauthorised payments;
- unusual emails sent from a user's account;
- loss of business information; or
- another suspected cyber-attack.

Employees should not attempt to conceal or independently investigate serious security incidents. Where appropriate, Selsey Community Forum may isolate systems or devices, restrict access, engage external IT or cyber-security support, preserve evidence and activate business continuity or disaster recovery arrangements.

Personal Data Breaches

Where an IT security incident involves personal information, the matter must also be reported and managed in accordance with Selsey Community Forum's applicable data protection and personal data breach procedures. Employees must report suspected personal data breaches promptly so that Selsey Community Forum can assess any legal or regulatory notification requirements. Employees should not delay reporting because they are unsure whether an incident amounts to a personal data breach.

Security Incident Response and Recovery

Selsey Community Forum will maintain proportionate arrangements for responding to significant cyber-security incidents. Depending on the incident, action may include:

- containing the incident;
- protecting people and information;
- isolating affected accounts or systems;
- changing access credentials;
- obtaining specialist assistance;
- assessing the extent of compromise;
- restoring clean systems and data;
- making required notifications;
- communicating with affected stakeholders; and
- reviewing lessons learned.

Significant incidents may be managed alongside Selsey Community Forum's Business Continuity and Disaster Recovery arrangements.

Account and Access Changes

Selsey Community Forum will seek to ensure that system access is amended or removed promptly when:

- an employee leaves;
- a worker, contractor or consultant's engagement ends;
- a Trustee or volunteer ceases their role;
- a person's responsibilities change;
- access is no longer needed; or
- a security concern requires access to be restricted.

Managers or other appropriate role holders should notify the relevant IT or system administrator promptly of starters, leavers, changes in role or any other change affecting access requirements. Shared accounts should be avoided where individual accounts are reasonably available.

Working in Public Places

When working in cafés, public transport, hotels or other shared environments, users should take reasonable precautions including:

- positioning screens to reduce unnecessary viewing by others;
- avoiding confidential conversations where they can be overheard;
- keeping devices under control;
- locking devices when unattended;
- avoiding unnecessary use of insecure public networks; and
- protecting confidential paperwork.

Clear Screen and Secure Workspace

Users must lock computers and devices when leaving them unattended. Sensitive documents and information should not be left visible or accessible where unauthorised individuals could view them. At the end of the working day or when leaving a work area for a significant period, confidential material should be secured appropriately.

Monitoring

Selsey Community Forum may monitor the use and security of its IT systems where this is lawful, necessary and proportionate. Monitoring may be undertaken for legitimate purposes including:

- protecting systems and information;
- detecting cyber threats;
- investigating suspected misuse;
- maintaining system availability;
- ensuring compliance with legal and regulatory obligations; and
- enforcing applicable policies.

Employees will be provided with appropriate information about workplace monitoring arrangements. Any workplace monitoring will also be carried out in accordance with Selsey Community Forum's Data Protection Policy and applicable privacy information.

Personal Use

Reasonable personal use of Selsey Community Forum's IT systems may be permitted unless Selsey Community Forum has notified employees otherwise. Personal use must:

- be limited;
- not interfere with work;
- not create unreasonable cost;
- not compromise IT security;
- not involve unlawful or inappropriate activity; and
- comply with applicable policies.

Employees should not assume that information stored or transmitted through Selsey Community Forum's systems is necessarily private.

Prohibited Activities

Users must not:

- deliberately introduce malware;
- attempt to bypass security controls;
- access systems or information without authority;
- share access credentials improperly;
- install unauthorised software;
- use unauthorised cloud services for business information;
- deliberately interfere with systems or networks;
- use systems for fraudulent or criminal purposes;
- disclose confidential information without authority;
- deliberately disable security software or updates; or
- use Selsey Community Forum's systems in another way that creates a serious security risk.

Reporting Security Concerns

Users must report suspected security concerns as soon as reasonably practicable to their manager, designated IT contact, IT support provider or another person specified by Selsey Community Forum. Employees should report concerns promptly even where:

- they caused the incident themselves;
- the incident appears minor;
- a technical system appears to have resolved it automatically; or
- they are uncertain whether a security breach has occurred.

Prompt reporting allows Selsey Community Forum to take appropriate action and reduce potential harm.

Misuse and Breaches of this Policy

Suspected breaches of this Policy may be investigated in accordance with Selsey Community Forum's applicable procedures. Depending on the individual's relationship with Selsey Community Forum, a breach may result in disciplinary, contractual, volunteer or governance action. Serious breaches, including deliberate cyber-security compromise, fraudulent access, deliberate introduction of malicious software, serious unauthorised disclosure

of confidential information or intentional circumvention of security controls, may constitute gross misconduct for employees and may result in dismissal where appropriate. Equivalent action may be taken in relation to workers, contractors, volunteers or Trustees in accordance with the arrangements applicable to them. Some conduct may also constitute a criminal offence and may be reported to the appropriate authorities.

Training and Awareness

Selsey Community Forum will provide users with appropriate information, guidance or training on IT and cyber security, having regard to their role and level of access. This may include:

- phishing awareness;
- account security;
- password and authentication practices;
- data protection;
- secure use of devices;
- remote working;
- reporting incidents;
- ransomware and malware;
- fraud prevention; and
- safe use of cloud and online services.

Training arrangements will be proportionate to Selsey Community Forum's size, activities and cyber-security risks.

Review

This policy will be reviewed periodically and may be amended to reflect changes in legislation, ICO or NCSC guidance, technology, cyber-security threats, organisational requirements or best practice.

Version Control

Version Number	Date of Update	Amendments
1.0	October 2025	Policy reviewed
2.0	October 2026	Reviewed and updated in line with current NCSC, ICO and data protection guidance