Selsey Community Forum

Digital Safety Policy

1. **Introduction:**
To ensure the continued delivery of services to our clients, Selsey Community Forum makes use of information technology (IT). The information that Selsey Community Forum holds, processes, maintains and shares with other organisations is an important asset that needs to be suitably protected to maintain public confidence and the highest standards of information security.

2. **Purpose:**
This document provides a summary of the Information Security and Digital Safety Policies developed by Selsey Community Forum to ensure that highest standards of information security are maintained at all times so that:
- The public and all users of Selsey Community Forum's information systems are confident of the security, integrity and availability of the information used and produced.
- Business damage and interruption caused by security incidents, should they occur, is minimised.
- All legislative and regulatory requirements are met.
- Selsey Community Forum's equipment and facilities are used responsibly, securely and with integrity at all times.
- Cybersecurity best practice is followed and maintained.

The Policies are based on legislation and good practice, and include:
- Cybersecurity Best Practice
- E-mail Policy
- Internet Acceptable Usage Policy
- Software Policy
- IT Access Policy
- Information Protection Policy
- Computer, Telephone and Desk Use Policy
- Legal Responsibilities Policy
- Removable Media Policy
- Information Security Incident Management Policy
- Communications and Operation Management Policy
- IT Infrastructure Policy

This document highlights key messages that all members of staff and volunteers need to be aware of when using electronic systems and sharing information with partner organisations.

Protected data is:
- Data that, if lost, could cause short-term distress for an individual such as loss of an individual's record containing personal data that could be used for criminal purposes.
- Data that, if lost, would breach statutory regulations such as the General Data Protection Regulations.
- Contract or tender documentation.

Restricted data is:

- Information relating to the award of withdrawal of a contract.
- Information that would prejudice the investigation of a crime.
- Data that, if lost, could cause risk to a third party's personal safety.

All staff are required to read this Policy document in order to:

- Understand the key messages.
- Understand that failure to comply with these Policies is a disciplinary offence.
- Understand they have a responsibility under the terms of their employment to familiarise themselves with all Information Security and Digital Safety Policies detailed in this document.

3. Digital Safety and Information Security Policies:

3.1 Cybersecurity Best Practice Statement

Cybersecurity's core function is to protect the devices we use, and the services we access and provide from theft or damage, as well as preventing unauthorised access to the vast amounts of data we store on these devices and online. Online safety is paramount to ensure that we protect ourselves, the work we carry out, the information we store, our service users and our partner organisations.

Key messages:

- Data Breach is any incident that results in confidential data or personal information being shared, stolen or otherwise transmitted; this must be reported immediately to the Manager.
- Malware is any malicious software intended to disable or infect a device's functionality. Some malware allows a hacker to control a device remotely. Any suspicion of this must be reported immediately to the Manager.
- Backing up data means saving a copy of the data on a separate storage device, eg. an external hard drive or cloud storage; new backups should be created regularly.
- All staff should create strong passwords and change them regularly.
- Staff should promptly install software updates, especially when they include important security upgrades; automatic updates should be set up.
- Connecting to unsecured public wifi networks should be avoided.
- Statements, receipts and bills should be checked to see if there is suspicious activity happening in any of the accounts.
- Be on the lookout for social media scams like fake profiles, catfishing, gossip clickbait, job offer scams and fake online scams; always check the validity of a website; never click on suspicious links, and do not fill out online forms unless the website is legitimate and secure.
- Always assume that if an offer seems too good to be true, it probably is.
- Selsey Community Forum will support vulnerable service users in the safe use of IT and inform them of current online scams and hoaxes.

3.2 E-mail Policy Statement

Selsey Community Forum will ensure all users of its e-mail facilities are aware of the acceptable use of such facilities.

Key messages:

- Staff personal e-mail address is the name followed by @selseycommunityforum.uk.
- Private e-mail usage must be in personal time.
- Staff must not use non-work e-mail accounts to conduct or support official Selsey Community Forum business.

- Under no circumstances should users communicate material (either internally or externally) which is defamatory, obscene, is terrorism related or does not comply with Selsey Community Forum's Equal Opportunities Policy.
- Although all e-mails received are virus scanned, an e-mail from a suspicious source or with an odd or unexpected subject title, must be treated with suspicion and reported to your Manager.
- An e-mail has the same legal status as a paper document and may be disclosed under the General Data Protection Regulations 2018 or the Freedom of Information Act 2000.
- Whilst respecting users' privacy, Selsey Community Forum may monitor and audit the use of e-mail to ensure adherence to this Policy.
- When staff are on leave, they are asked to put a message on their mailbox advising when they will return from leave using the 'out of office assistant'.
- All official external e-mails will carry the official disclaimer and signature profile.
- Automatic forwarding of e-mails is not permitted to prevent protected and restricted material being forwarded inappropriately.

3.3 Internet Acceptable Usage Policy Statement

Selsey Community Forum will ensure all users of Selsey Community Forum provided internet facilities are aware of the acceptable use of such facilities.

Key messages:

- Staff must familiarise themselves with this Policy and sign the Policy before using the internet facility provided.
- Internet and e-mail access is an important aide to productivity. Private internet and e-mail usage must be in personal time.
- Staff are responsible for ensuring the security of their log-in ID and password.
- Individual user log-in identity and passwords must only be used by that individual user, and they must be the only person who accesses their internet account.
- Do not create, download, upload, display or access sites that contain pornography or other 'unsuitable' material that might be deemed illegal, obscene or offensive. If staff inadvertently access an inappropriate site, immediately notify your Manager.
- Users must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.

3.4 Software Policy Statement

Selsey Community Forum will ensure the acceptable use of software by all users of Selsey Community Forum's computer equipment.

Key messages:

- All software must be approved before being purchased and installed.
- Under no circumstances should personal or unsolicited software be loaded onto Selsey Community Forum machines.
- Every piece of software is required to have a licence and Selsey Community Forum will not condone the use of any software that does not have a licence.
- Unauthorised changes to software must not be made.
- Staff are not permitted to bring software from home (or any other external source) and load it onto Selsey Community Forum equipment.
- Users must not attempt to disable or reconfigure the Firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

3.5 IT Access Policy Statement

Selsey Community Forum has specific requirements for protecting information and information systems against unauthorised access.

Key messages:

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of Selsey Community Forum systems and data.
- Passwords must be protected at all times.
- If staff leave their desk, they must lock or log out from their computer.
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Selsey Community Forum systems.
- Partner agencies, or third party suppliers, must not be given details of how to access Selsey Community Forum's network without permission from the Manager.

3.6 Information Protection Policy Statement

Selsey Community Forum will ensure the protection of all information within its custody. High standards of confidentiality, integrity and availability of information will be maintained at all times.

Key messages:

- Where information is shared or disclosed, it should only be done so in accordance with Selsey Community Forum's Confidentiality and Data Protection Policy.
- Users should not be allowed to access information until the Manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling, and are aware of any data that is regarded as Protected or Restricted.
- Protected and Restricted information must not be disclosed to any other person or organisation via any insecure methods including paper-based methods, fax and telephone.
- Information is to be handled and destroyed appropriately.

3.7 Computer, Telephone and Desk Use Policy Statement

Selsey Community Forum will ensure that every user is aware of, and understands, the acceptable use of Selsey Community Forum's computer and telephone resources and the need to operate within a 'clear desk' environment.

Key messages:

- Where possible, private telephone calls should be made outside standard hours of service.
- Phone use is audited and any abuse will be considered to be a disciplinary issue.
- When staff are driving on Selsey Community Forum business, they must not answer a mobile phone, whether or not it is a hands-free set.
- Users handling restricted data must maintain a clear desk at all times.
- Selsey Community Forum's Protected or Restricted information must be stored in a facility (lockable safe or cabinet) commensurate with this classification level.
- IT equipment is provided for use on official business only.

3.8 Legal Responsibilities Policy Statement

This Policy sets out the responsibilities of all staff under the General Data Protection Regulations 2018 and Freedom of Information Act 2000 and other relevant legislation.

Key messages:

- Personal data is that which relates to a living individual who can be identified.
- Individuals have the right to request access to their personal information held either in paper or electronic copy by Selsey Community Forum.
- If staff receive a request for information under the General Data Protection Regulations, it should be referred to the Manager.

- All staff must accept responsibility for maintaining Information Security standards within Selsey Community Forum.
- Written consent will be obtained before photographs of anyone attending Selsey Community Forum activities are published on any website/social media/local press.

3.9 Removable Media Policy Statement

Selsey Community Forum 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 Selsey Community Forum business. Removable media devices include:

- Memory stick/USB keys
- CD/DVD
- Laptop
- Camera
- Memory cards
- Floppy disks

Key messages:

- Only removable media device supplied by Selsey Community Forum can be used.
- All data stored on removable media devices must be assessed and encrypted when required.
- Damaged or faulty removable media devices must not be used.
- If staff receive a CD or memory stick from a third party, they must check it for viruses before inserting it into the PC or laptop.
- Special and reasonable care must be taken to physically protect the removable media device and stored data from loss, theft or damage.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage.

3.10 Information Security Incident Management Policy and Procedure Statement

Selsey Community Forum will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information in the custody of Selsey Community Forum.

Key messages:

- If staff lose or have a removable media device stolen, they must report this immediately to the Manager.
- Staff need to understand the importance of reporting abuse, misuse or access to inappropriate materials.

3.11 Communications and Operation Management Policy Statement

Selsey Community Forum will ensure the protection of its IT against malware and malicious and mobile code. Only authorised changes will be made to the Selsey Community Forum IT services. Information leakage will be prevented by secure controls.

Key messages:

- Any changes to a system, e.g. an upgrade, patch or additional software must be approved in advance.
- Regular backups of data are taken and stored off-site to ensure that Selsey Community Forum can recover from system downtime or error.
- If staff need to dispose of a CD or other form of media, arrange for its secure disposal.
- An annual health check will be made of all Selsey Community Forum IT infrastructure to maintain security.

3.12 IT Infrastructure Security Policy Statement

There shall be no unauthorised access to either physical or electronic information within the custody of Selsey Community Forum. Protection shall be afforded to:

- Sensitive paper records.
- IT equipment used to access electronic data.
- IT equipment used to access the Selsey Community Forum network.

Key messages:

- Protected or restricted information, and equipment used to store and process this information, must be stored securely.
- Keys to all secure areas housing IT equipment and lockable IT cabinets are held securely.
- Do not loan ID badge, keys or entry codes to anyone else.
- PCs must store all data on central network drives and never on local drives.
- Equipment that is to be reused or disposed of must have all its data and software erased or destroyed.

4. Policy Compliance

Any user found to have breached this Policy, may be subject to Selsey Community Forum's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender.

This Policy is to be read in conjunction with the Selsey Community Forum Communications Policy and the Selsey Community Forum Confidentiality and Data Protection Policy.

Reviewed and Approved by Trustees: March 2024

……
Mike Nicholls, Chair, Selsey Community Forum