

Selsey Community Forum



Confidentiality & Data Protection Policy

Aim

In order to satisfy the requirements of the relevant legislation, Selsey Community Forum aims to safeguard personal information that it needs to retain in order to undertake its various projects. This policy aims to give staff, volunteers and trustees a framework within which to responsibly safeguard personal information.

Confidentiality and Data Protection Legislation

The General Data Protection Regulation (GDPR) requires that personal information is:

- ◆ Used fairly, lawfully and transparently for specified, explicit purposes in a way that is adequate, relevant and limited to only what is necessary.
- ◆ Accurate and, where necessary, kept up to date.
- ◆ Kept for no longer than is necessary.
- ◆ Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There is a stronger legal protection for more sensitive information, such as: race or ethnic background, political or religious beliefs, trade union membership, genetics or biometrics (where used for identification), health and sexual orientation. In addition, there are separate safeguards for personal data relating to criminal convictions and offences.

Under the GDPR, individuals have the right to find out what information the government and other organisations store about them. These include the rights: to have access to their personal data and to be informed about how it is being used, to have incorrect data updated or erased, and to stop or restrict the processing of their data.

Data Protection Act 2018

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR and sets out the Information Commissioner's functions and powers.

UK General Data Protection Regulation

The UK GDPR is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

- (a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.
- (e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The UK GDPR sets out seven key principles:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability.

Management of Information and Data

Data protection strategies have three key focuses: Data security – protecting data from malicious or accidental damage. Data availability – Quickly restoring data in the event of damage or loss. Access control – ensuring that data is accessible to those who actually need it, and not to anyone else.

Data Controllers

Selsey Community Forum considers all managers and project leaders to be Data Controllers, responsible for meeting the requirements of this policy within their particular sphere of interest. They are to ensure that confidential systems and practices are in place to protect personal information relating to staff, volunteers and service users.

Personal Information

Personal information kept by Selsey Community Forum will include names, addresses, dates of birth and, possibly, photographs. For staff and volunteers, it will also usually involve application forms and DBS documentation. For service users, it might also include information about the services used, any medical conditions and emergency contacts. Except when it is in use, all personnel information retained by Selsey Community Forum on paper is to be stored in a locked container. Any information on paper for which there is no further requirement should be destroyed by shredding and not disposed of in normal waste bins. To secure any information stored electronically, all computers and other devices provided by the forum are to be password protected and shut-down when not in use. Passwords are to be strong and changed regularly; they are to be given to staff and

volunteers only on the basis of genuine need. In addition, the Selsey Care Shop computer is to be backed up at least weekly. Personal information is not to be retained on private computers or other devices. Personal telephone numbers and addresses of staff, volunteers and service users should not be shared with other staff, volunteers, service users or third parties unless there is a genuine need and the person whose information is to be shared has specifically consented. In an emergency, necessary personal information can be released provided the individual releasing it is prepared to justify the action after the event.

Staff, volunteers and service users should be asked on joining to agree to the taking of photographs at events and on occasions at which they might be present. If it is intended to publish any such photograph in any medium, then the specific written agreement of the individuals involved is to be obtained before publication.

Conversations, including those held by telephone and particularly those with service users, which involve confidential personal information are not to be held where they might be overheard and must take place in private. Similarly, all staff, volunteers and trustees should be aware of the need for care, when in public places, to avoid any discussion which might reveal confidential personal information of any kind.

Personal information should be periodically checked by appropriate managers or project leaders for accuracy and is only to be retained for as long as necessary - it should be destroyed or deleted when no longer required or relevant.

Other Matters

All staff and volunteers are to be provided with appropriate induction training and a handbook providing information and guidance on confidentiality and data protection. They will also be asked to confirm on joining that they will respect the confidentiality of personal information and informed that breach of this policy will usually result in being asked to leave Selsey Community Forum.

Prior to their participation, service users must provide written consent that their personal information can be held for the purposes of the service they are using.

This policy is applicable to all the activities in which Selsey Community Forum is or becomes involved; it is to be reviewed and updated as necessary at least annually.

Selsey Community Forum is to maintain its registration with the Information Commissioner's Office (Registration Reference: ZA326164).

Associated Forms: Service Users Joining Form
 Consent to Publish Photo Form

Reviewed and Approved by Trustees: October 2023

.....
Mike Nicholls, Chair, Selsey Community Forum