Selsey Community Forum
Data Protection Policy

Introduction

Selsey Community Forum collects and uses personal information relating to employees, workers, applicants, clients, customers, suppliers and other individuals in connection with its activities. Selsey Community Forum is committed to processing personal information lawfully, fairly, transparently and securely.

This Policy sets out the principles and responsibilities that apply when personal information is collected, accessed, used, stored, shared, transferred, retained or deleted. This Policy applies alongside Selsey Community Forum's Privacy Notices, Record Retention and Document Management Policy, IT Security Policy, Confidentiality Policy, Artificial Intelligence Use Policy and other relevant policies. This Policy does not form part of any contract of employment and may be amended from time to time.

Scope

This Policy applies to all employees of Selsey Community Forum and, where appropriate, to workers, agency workers, contractors, consultants, volunteers and others who process personal information on behalf of Selsey Community Forum. It applies to personal information held:

- electronically;
- on paper;
- in structured filing systems;
- in email;
- in cloud systems;
- in databases;
- in photographs;
- in audio or video;
- in CCTV footage;
- on mobile devices; and
- in any other format covered by applicable data protection law.

Data Protection Law

Selsey Community Forum will comply with applicable UK data protection legislation, including:

- the UK General Data Protection Regulation;
- the Data Protection Act 2018;
- the Data (Use and Access) Act 2025;
- the Privacy and Electronic Communications Regulations 2003 where applicable; and
- other relevant data protection legislation as amended from time to time.

The Data (Use and Access) Act 2025 amended parts of UK data protection law and all of its data-protection provisions are now in force.

Responsibility for Data Protection

Selsey Community Forum will identify an appropriate person responsible for overseeing data protection compliance. This may be:

- a Data Protection Officer where Selsey Community Forum is legally required to appoint one; or
- another designated Data Protection Lead where a formal Data Protection Officer is not required.

The relevant contact details will be communicated internally where appropriate. Not every organisation is legally required to appoint a Data Protection Officer.

Employee Responsibilities

Everyone covered by this Policy who handles personal information must:

- comply with this Policy;
- only access personal information where authorised;
- only use personal information for legitimate work-related purposes;
- keep information secure;
- follow applicable retention arrangements;
- report suspected personal data breaches promptly;
- refer data subject rights requests appropriately;
- seek advice before introducing new high-risk processing;
- complete appropriate training; and
- avoid disclosing personal information without authority.

Failure to comply with this Policy may result in action under the appropriate disciplinary or contractual procedure.

Data Protection Principles

Personal information must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where necessary;
- retained for no longer than necessary; and
- protected by appropriate technical and organisational security measures.

Selsey Community Forum must also be able to demonstrate compliance with its data protection obligations.

What is Personal Data?

Personal data is information relating to an identified or identifiable living individual. This may include information such as:

- name;
- address;
- telephone number;
- email address;
- identification numbers;
- online identifiers;
- IP address;
- employment information;
- financial information;
- location information;
- photographs;
- opinions about an individual; or
- other information that can identify someone directly or indirectly.

Information that has been effectively anonymised so that an individual can no longer be identified is not personal data.

Special Category Personal Data

Some personal data receives additional legal protection. Special category personal data includes information relating to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;

- trade union membership;
- genetic data;
- biometric data used for identification;
- health;
- sex life; and
- sexual orientation.

Special category data must only be processed where both:

- an appropriate lawful basis under Article 6 applies; and
- an additional condition under Article 9 applies.

Criminal Conviction and Offence Data

Personal data relating to criminal convictions, offences or related security measures is subject to additional legal protection. Such information will only be processed where:

- there is a lawful basis;
- processing is permitted under applicable law; and
- appropriate safeguards are in place.

This may include information obtained through lawful DBS or regulatory checks.

Lawful Bases

Selsey Community Forum will only process personal information where an appropriate lawful basis applies. Depending on the circumstances, this may include processing because:

- the individual has given valid consent;
- processing is necessary to enter into or perform a contract;
- processing is necessary to comply with a legal obligation;
- processing is necessary to protect vital interests;
- processing is necessary for a task carried out in the public interest or exercise of official authority where applicable;
- processing is necessary for legitimate interests pursued by Selsey Community Forum or a third party; or
- another lawful basis recognised under UK data protection law applies.

The appropriate lawful basis will depend on the purpose and circumstances of the processing.

Recognised Legitimate Interests

Where applicable under current UK data protection law, Selsey Community Forum may rely on a recognised legitimate interest where the statutory conditions are satisfied. Where a recognised legitimate interest applies, a separate balancing test may not be required in the same way as for ordinary legitimate interests. Advice should be sought where there is uncertainty.

Consent

Consent will only be relied upon where it is appropriate and valid. Consent must be:

- freely given;
- specific;
- informed;
- unambiguous; and
- capable of being withdrawn.

In employment situations, Selsey Community Forum will normally consider whether another lawful basis is more appropriate because the imbalance in the employment relationship can make consent unsuitable.

Purpose Limitation

Personal information must normally only be used for the purpose for which it was collected. Before using personal information for a new purpose, Selsey Community Forum will consider whether the new purpose is compatible with the original purpose. Where required, individuals will be provided with further privacy information.

Data Minimisation

Only personal information reasonably necessary for the relevant purpose should be collected, accessed or retained. Employees should avoid:

- collecting excessive information;
- requesting information "just in case";
- retaining unnecessary copies;
- sharing more information than required; or
- storing personal information in multiple locations without reason.

Accuracy

Reasonable steps must be taken to ensure that personal information is accurate and, where necessary, kept up to date. Where inaccurate information is identified, it should be corrected or appropriately marked without undue delay. Individuals should be encouraged to notify Selsey Community Forum where relevant information changes.

Retention

Personal information must not be retained indefinitely without a lawful and documented reason. Different categories of personal information may require different retention periods. Retention decisions may take account of:

- statutory requirements;
- limitation periods;
- regulatory obligations;
- contractual requirements;
- legal claims;
- safeguarding requirements;
- business need; and
- evidential requirements.

Retention periods should be set out in Selsey Community Forum's Record Retention and Document Management Policy or retention schedule where applicable.

Secure Disposal

Personal information that is no longer required must be disposed of securely. This may include:

- confidential shredding;
- secure deletion;
- destruction of storage media;
- deletion from approved systems; or
- another appropriate secure method.

Ordinary deletion may not always permanently erase data from all systems, so appropriate technical arrangements should be used where necessary.

Security of Personal Data

Selsey Community Forum will use appropriate technical and organisational measures to protect personal information. These may include:

- access controls;
- authentication;
- multi-factor authentication;
- encryption where appropriate;
- secure storage;
- security updates;
- backup arrangements;
- staff training;
- supplier controls;
- secure disposal;
- incident-response procedures; and

- restrictions on access.

Security measures should be proportionate to the nature, sensitivity and risks associated with the information.

Access Controls

Employees must only access personal information necessary for their role. Employees must not access information:

- out of curiosity;
- for personal purposes;
- for the benefit of another unauthorised person;
- outside their job responsibilities; or
- without appropriate authority.

The ability to access a system does not automatically mean the employee is authorised to access every record within it.

Passwords and Authentication

Employees must comply with applicable IT Security requirements. Passwords, authentication codes and access credentials must not be shared unless expressly authorised through an approved process. Suspected compromise of login credentials must be reported promptly.

Remote and Home Working

Personal information must be protected when employees work remotely. Employees must take appropriate precautions including:

- using approved systems and devices;
- locking screens when unattended;
- preventing household members from accessing work information;
- protecting paper records;
- avoiding confidential conversations being overheard;
- using secure connections; and
- following Selsey Community Forum's applicable Home Working, Hybrid Working and IT Security requirements.

Personal Devices

Personal devices must not be used to process personal information unless authorised. Where personal devices are authorised for work purposes, employees must comply with Selsey Community Forum's applicable security and data protection requirements. Personal information must not be transferred to personal email accounts, personal cloud storage or unauthorised applications.

Artificial Intelligence

Personal data must not be entered into artificial intelligence systems or other automated tools unless their use has been authorised. Before using personal data with AI, Selsey Community Forum will consider:

- lawful basis;
- transparency;
- data minimisation;
- security;
- accuracy;
- bias;
- automated decision-making;
- international transfers;
- supplier arrangements; and
- other applicable risks.

Any use of artificial intelligence involving personal data must be specifically authorised and comply with Selsey Community Forum's data protection and information security requirements.

Data Protection by Design and Default

Data protection considerations should be built into new projects, systems and processes from the outset. Where appropriate, Selsey Community Forum will consider:

- whether personal information is necessary;
- how much information is required;
- who needs access;
- how long information should be retained;
- what security controls are required;
- how individuals will be informed; and
- whether a Data Protection Impact Assessment is necessary.

Data Protection Impact Assessments

A Data Protection Impact Assessment should be carried out where processing is likely to result in a high risk to individuals' rights and freedoms. This may include certain uses of:

- systematic monitoring;
- special category information;
- biometric information;
- large-scale processing;
- automated decision-making;
- new technology;
- employee monitoring; or
- other high-risk processing.

Employees must seek appropriate advice before implementing processing that may require a DPIA.

Privacy Notices

Individuals must be provided with appropriate information about how their personal information is used. Privacy notices should normally explain matters including:

- the identity of the controller;
- what information is collected;
- purposes of processing;
- lawful bases;
- recipients;
- international transfers;
- retention;
- individual rights; and
- how to raise concerns.

Different privacy notices may be used for employees, applicants, clients, customers or other groups.

Sharing Personal Data Internally

Personal information should only be shared internally where there is a legitimate need to know. Employees should consider:

- whether sharing is necessary;
- whether all of the information needs to be shared;
- whether the recipient is authorised; and
- whether the method used is appropriately secure.

Sharing Personal Data Externally

Personal information must not be disclosed externally unless there is an appropriate lawful basis and legitimate reason. Examples may include disclosure:

- to service providers;
- to HMRC;
- to the Home Office;
- to regulators;
- to courts;

- to law enforcement;
- to professional advisers;
- to occupational health providers;
- to insurers;
- to pension providers;
- for safeguarding purposes; or
- where another lawful disclosure is required or permitted.

Only the information reasonably necessary should normally be shared.

Verifying Third Parties

Before disclosing personal information to a third party, Selsey Community Forum should take reasonable steps to verify:

- the identity of the requester;
- their authority;
- the purpose of the request; and
- whether disclosure is lawful.

Employees should seek advice where uncertain.

Data Processors

Where Selsey Community Forum uses a third party to process personal information on its behalf, appropriate contractual arrangements must be in place where legally required. Processor agreements should address matters including:

- documented instructions;
- confidentiality;
- security;
- subprocessors;
- assistance with rights requests;
- breach reporting;
- deletion or return of information; and
- audit or compliance obligations.

Supplier Due Diligence

Before appointing a supplier that will process personal information, Selsey Community Forum should consider whether the supplier provides sufficient guarantees regarding security and data protection compliance. The level of due diligence should be proportionate to:

- the sensitivity of the information;
- the volume processed;
- the nature of the service; and
- the potential risks to individuals.

International Transfers

Personal information must not be transferred outside the UK unless the transfer is lawful. Appropriate mechanisms may include:

- UK adequacy regulations;
- approved contractual safeguards;
- other recognised transfer mechanisms; or
- a statutory exception.

Where required, a transfer risk assessment or other appropriate assessment should be completed. Employees must seek guidance before using a new supplier or system that may process personal information outside the UK.

Data Subject Rights

Individuals may have rights including:

- access to their personal data;

- rectification;
- erasure;
- restriction of processing;
- objection;
- data portability;
- withdrawal of consent where applicable; and
- rights relating to certain automated decisions.

Rights are subject to statutory conditions and exemptions and do not apply in every circumstance. Any rights request received by an employee must be passed promptly to the appropriate person.

Subject Access Requests

Individuals have the right to request access to personal information held about them. A subject access request may be made verbally or in writing and does not need to use any particular wording. Employees who receive a request that may amount to a subject access request must forward it promptly to the appropriate Data Protection contact.

Selsey Community Forum will respond without undue delay and normally within one calendar month, subject to applicable extensions or pauses permitted by law. Following the Data (Use and Access) Act 2025, Selsey Community Forum is required to carry out a **reasonable and proportionate search** when responding to a subject access request.

Clarification of Subject Access Requests

Where reasonably required to identify the information requested, Selsey Community Forum may seek clarification from the individual. Where permitted by law, the statutory response period may be affected while clarification is awaited. Any clarification request should be reasonable and should not be used simply to delay responding.

Rectification

Individuals may request correction of inaccurate personal information. Where appropriate, incomplete information may also be supplemented. Selsey Community Forum will respond in accordance with applicable statutory timescales.

Erasure

Individuals may have the right to request deletion of personal information in certain circumstances. The right to erasure is not absolute. Information may need to be retained where, for example:

- there is a legal obligation;
- information is required for legal claims;
- another statutory exception applies; or
- a legitimate need to retain the information remains.

Restriction of Processing

Individuals may have the right to request restriction of processing in certain circumstances. This may apply, for example, where:

- accuracy is disputed;
- processing is unlawful but the individual does not want deletion;
- Selsey Community Forum no longer needs the information but the individual requires it for a legal claim; or
- an objection is being considered.

Right to Object

Individuals may have the right to object to certain processing, including some processing based on:

- legitimate interests;
- public task; or
- direct marketing.

Objections will be considered in accordance with applicable law. Where an objection relates to direct marketing, processing for that purpose must stop as required by law.

Data Portability

Individuals may have a right to receive certain personal information in a structured, commonly used and machine-readable format where the statutory conditions are met. This generally applies where processing is based on:

- consent; or
- contract,

and is carried out by automated means.

Automated Decision-Making and Profiling

Automated decision-making occurs where a significant decision is made using automated processing without meaningful human involvement. Profiling involves automated processing used to evaluate personal aspects relating to an individual.

Following the Data (Use and Access) Act 2025, significant solely automated decisions may be made in a wider range of circumstances than under the previous framework, provided applicable legal requirements and safeguards are met. Safeguards may include:

- providing information about the decision;
- enabling the individual to make representations;
- allowing the individual to obtain human intervention; and
- enabling the decision to be challenged.

Different or additional restrictions apply where special category personal information is involved. Employees must not introduce automated decision-making, profiling, AI recruitment tools or other high-risk automated processes without appropriate approval.

The ICO confirms that the DUAA expanded when significant solely automated decisions can be used, while preserving safeguards including information, representations and human intervention.

Monitoring Employees and Workers

Where Selsey Community Forum monitors employees or workers, monitoring must be:

- lawful;
- necessary;
- proportionate;
- transparent; and
- appropriately secure.

The least intrusive reasonable method should normally be used. Where monitoring is likely to create a high risk to individuals, a DPIA should be considered. Employees should be provided with appropriate privacy information about monitoring arrangements.

Data Protection Complaints

Individuals have the right to complain about how Selsey Community Forum has processed their personal information. Selsey Community Forum will provide an accessible method for raising a data protection complaint. Complaints will be handled in accordance with current legal requirements. Selsey Community Forum will:

- acknowledge a data protection complaint within **30 days**;
- take appropriate steps to investigate it;
- keep the complainant appropriately informed; and
- provide an outcome without undue delay.

The individual also retains the right to complain to the Information Commissioner's Office. Since 19 June 2026, all organisations handling personal data have been legally required to operate a data protection complaints process meeting these requirements.

Personal Data Breaches

A personal data breach is a security incident that results in the accidental or unlawful:

- destruction;
- loss;
- alteration;
- unauthorised disclosure of; or
- access to personal information.

Examples may include:

- sending information to the wrong recipient;
- losing a device or paper file;
- unauthorised system access;
- ransomware;
- accidental deletion;
- inappropriate access by an employee;
- lost documents; or
- disclosure of information without authority.

Reporting Personal Data Breaches

Employees must report a suspected personal data breach as soon as reasonably practicable. Reports should be made to the Data Protection Lead or another designated person. Employees should not delay reporting while trying to determine whether the breach is serious. Prompt reporting enables Selsey Community Forum to:

- contain the incident;
- assess risk;
- preserve evidence;
- meet regulatory deadlines; and
- take appropriate remedial action.

Breach Assessment

Selsey Community Forum will assess:

- what happened;
- the type and sensitivity of information involved;
- the number of people affected;
- potential consequences;
- existing security measures;
- whether the breach has been contained; and
- the likelihood and severity of risk to individuals.

Not every personal data breach must be reported to the ICO.

Reporting to the ICO

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, Selsey Community Forum will notify the ICO without undue delay and, where feasible, within **72 hours of becoming aware of the breach**. Where notification is made after 72 hours, reasons for the delay will be provided where required. The ICO confirms that reportable personal data breaches must normally be reported within 72 hours of awareness.

Informing Individuals About a Breach

Where a personal data breach is likely to result in a high risk to affected individuals, Selsey Community Forum will normally inform those individuals without undue delay unless a statutory exception applies. The communication should provide appropriate information about:

- the nature of the breach;
- likely consequences;
- protective steps;
- measures taken; and
- how further information can be obtained.

Breach Records

Selsey Community Forum will maintain an appropriate record of personal data breaches. This will include breaches that are not reported to the ICO. Records should include appropriate details of:

- what happened;
- the likely impact;
- the assessment carried out;
- action taken; and
- reasons for any decision not to notify.

The ICO requires organisations to keep records of personal data breaches whether or not they are reportable.

Direct Marketing

Where Selsey Community Forum carries out direct marketing involving personal information, it will comply with applicable data protection law and the Privacy and Electronic Communications Regulations where relevant. Individuals have an absolute right to object to processing for direct marketing purposes. Opt-outs and suppression preferences must be respected. Employees involved in marketing must follow any specific marketing procedures adopted by Selsey Community Forum.

Training

Employees will receive data protection training appropriate to their role. Training may cover:

- confidentiality;
- data security;
- phishing;
- individual rights;
- personal data breaches;
- special category information;
- sharing information;
- retention;
- remote working;
- AI;
- monitoring; and
- complaints.

Training should be refreshed periodically and where relevant changes arise.

Record Keeping and Accountability

Selsey Community Forum will maintain appropriate records to demonstrate compliance where required. Depending on the nature and size of the organisation, this may include:

- records of processing activities;
- privacy notices;
- processor agreements;
- DPIAs;
- data breach logs;
- retention schedules;
- international transfer assessments;
- training records;
- legitimate-interest assessments; and
- complaint records.

Regulatory Cooperation

Selsey Community Forum will cooperate appropriately with the Information Commissioner's Office and other relevant authorities where required. Employees must not obstruct a lawful regulatory investigation or provide misleading information.

Review

This policy will be reviewed periodically and may be amended to reflect changes in legislation, ICO guidance, technology, working practices or organisational requirements.

Version Control

Version Number	Date of Update	Amendments
1.0	October 2025	Policy reviewed
2.0	October 2026	Reviewed and updated in line with the UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025.