SOUTH EAST LONDON COMMUNITY ENERGY

Data Protection Policy

Author	(Based on Directory of Social Change template 2nd Ed)
Issue Date	May 2026
Last Reviewed	n/a
Board Committee	HR Subcommittee
Frequency of Review	Annual
Next Review Date	May 2027

1 Who is covered by this policy?

All staff, directors, volunteers, beneficiaries and clients.

2 What is covered by this policy?

This policy covers data protection in relation to all areas of Selce's activities, including:

- client records;
- legal compliance (UK General Data Protection Regulation – UK GDPR);
- recruitment, promotion, training, redeployment and/or career development;
- administration and payment of wages;
- calculation of certain benefits, including pension;
- disciplinary purposes arising from an employee's conduct or inability to perform their duties;
- performance review;
- recording of communication with employees and their representatives;
- compliance with policy and/or legislation with regard to health and safety or other employment legislation and regulation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future employers;
- any use of Artificial Intelligence tools or technologies.

3 Purpose

The purpose of this policy is to protect Selce and its staff from the misuse of individuals' personal data and to ensure that Selce complies with all relevant legislation.

4 The policy

4.1 Recruitment and selection

If placing a recruitment advert, Selce must identify itself properly – people should know who they are applying to. If using a recruitment agency, Selce must ensure the agency identifies itself.

Information collected for recruitment or selection for an interview must be used for that purpose only and must be kept securely. Where sensitive personal data is collected, explicit written consent should be obtained from applicants at the point of data collection. CEO should ensure that equal opportunities data for applicants is anonymised before the applications are considered.

If verifying the information a person provides, Selce must ensure the person knows how this will be done and what information will be checked.

If Selce needs to verify criminal conviction information, it will only do this by getting a Disclosure and Barring Service (DBS) check. Selce must ensure it is entitled to receive this information and must follow the DBS's procedures strictly. Selce may only keep a record that a satisfactory/unsatisfactory check was made, but it may not store any detailed information.

4.2 Employment records

Selce is permitted to collect, maintain and use employment records. However, staff should know what information about them is kept and what it will be used for. Selce will not keep information for which it has no genuine business need or legal duty to keep.

Employment records must be kept in a secure, locked place, and computerised records must be password protected. Only authorised staff should have access to employment records (usually, the individual's line manager, relevant Finance/HR Coordinator and the Chief Executive).

Selce will keep employment records of staff who have left for three years to allow for information to be supplied for references. After this time, records will be destroyed.

4.3 Sickness records

Selce will collect information about a staff member's health in accordance with Selce's Sickness Policy and Procedure and record it on HR management system. Access to the information is strictly limited to authorised staff.

4.4 Pension scheme records

Selce will only use the information about a staff member for the administration of the scheme and will inform the staff member of what information the pension scheme provider will pass back to Selce.

4.5 Disclosure

Selce will only disclose information on a staff member if, in all the circumstances, it is satisfied that it is in line with GDPR and is reasonable to do so or as part of legal disclosure. Fairness to the staff member will always be Selce's first consideration. Selce will allow staff access to their own records to ensure the information is correct.

4.6 Selce's staff rights

Staff have a legal right of access to the information Selce holds on them and the right to challenge the information if it is thought to be inaccurate or misleading. If a staff member objects to Selce holding or using information about them because it causes them distress or harm, Selce will delete the information or stop using it in the way complained

about unless Selce has a compelling reason to continue holding and/or using that information.

To see what information Selce holds on you, ask the CEO for access to your records.

5 Client data

Selce will process personal data that may identify a client or prospective client according to the UK GDPR. Client data will be processed in the legitimate interest of Selce work and/or if Selce has a contractual or legal obligation. Such data may be retained indefinitely or in accordance with a legal or contractual obligation where such data is for accounting purposes.

6 Data storage and transfers

Selce may store data in the UK or the European Economic Area, or any country deemed to be adequate by either the UK or the EU. Where Selce stores data outside these jurisdictions, it may undertake a data transfer risk assessment. Selce will ensure appropriate UK safeguards are in place to protect the rights of those identified by personal data stored in such locations. All online platforms used by Selce to handle personal data are GDPR compliant or enable Selce to be GDPR compliant.

7 Records and legal compliance

Under the UK GDPR, 'personal data' (i.e. data about identifiable living individuals – 'data subjects') should be:

a) processed fairly and lawfully and in a transparent manner;
b) collected for specified, explicit and legitimate purposes;
c) adequate, relevant and limited to what is necessary;
d) accurate and, where applicable, kept up to date;
e) kept for no longer than is necessary;
f) processed in accordance with the rights of data subjects;
g) kept secure by the data controller (i.e. Selce, which holds ultimate responsibility for complying with data protection requirements), following appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal data;
h) only be transferred to a country outside the European Economic Area if that country has equivalent levels of protection for personal data.

GDPR applies to both automated and manual personal data filing systems, where personal data is accessible according to specific criteria.

In order to be able to carry out its functions, Selce needs to keep and use certain types of information about people and organisations, employees, associates, donors,

directors, volunteers and so on. This may include address and contact details, bank details, personal references and the legal status of groups.

Information is obtained, held, processed and disclosed for the purposes of the administration, management and business activities of Selce. These include:

- making and holding lists of beneficiaries, clients and relevant organisations;
- Providing energy or retrofit advice to clients
- Referring energy or retrofit advice clients to associated organisations for ongoing support
- statistical analysis and reporting to funders;
- maintaining relationships with external associates and other partners;
- reporting to donors and other partners;
- keeping beneficiaries and other partners informed of products and services that may help them;
- keeping beneficiaries and other partners informed of events, campaigns, etc.;
- using basic information in marketing materials, on any of the websites run by Selce or in the annual report;
- keeping business process records (including financial records such as purchase information, donations and grant details);
- maintaining lists of events delegates.

When collecting information, Selce will ensure that individuals:

- clearly understand why Selce needs to collect the information and receive sufficient detail on how it will be used;
- understand what it will be used for and what the consequences are should the individuals decide not to give/withdraw consent to processing;
- where required, provide explicit written or verbal consent (record of which should be kept) for data to be processed;
- give their consent freely and without any duress.

All employees, directors and volunteers are expected to maintain professional standards and respect confidentiality. Due to the size of Selce and nature of data processed, there is no requirement for a formal Data Protection Officer. However, ICEO should be the first point of contact with regard to any data protection issues, queries or complaints.

Selce will review all personal data held on its databases regularly to ensure it should be retained. The categories of data listed below must be retained under the following specific criteria:

- Personal data of donors associated with finance data must be retained for at least six years.
- Personal data associated with records of transactions/purchases needs to be kept for at least six years.

- Personal data of employees needs to be retained for six years with reference to payroll and ten years with reference to pension information.
- Personal data of volunteers and directors needs to be retained for at least six years if it is associated with financial transactions.
- Personal data of clients (both energy advice clients and retrofit clients) should be anonymised after three years

Selce complies with GDPR by providing the following rights for individuals:

- the right to be informed;
- the right to access to a copy of their personal data;
- the right of rectification of data;
- the right of erasure (or right to be forgotten);
- the right to restrict processing;
- the right to data portability (in relation to processing by automated means);
- the right to object to processing;
- rights in relation to automated decision-making and profiling.

The **right to be informed** encompasses Selce's obligation to provide information on how personal data is collected and used ('fair processing information'), , and to be transparent in how personal data is used. Prior to collecting any personal data Selce will inform and seek consent for use, storage and for any sharing of any personal information.

With regard to the **right of access,** Selce will provide confirmation that the data is being processed and, if requested, grant access to personal data free of charge within 28 days of receiving the request (this can be extended by a further month if the request is complex or onerous).

Under the **right of rectification,** Selce will correct any inaccurate or incomplete data within 28 days of notification. Selce will also inform any third parties, if applicable, of these rectifications.

In compliance with the **right to erasure,** Selce will delete data under the following specific circumstances:

- Personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- An individual withdraws their consent.
- The individual objects to the processing and there is no overriding legitimate interest for continuing processing.
- The personal data was unlawfully processed.
- The personal data has to be erased to comply with a legal obligation.
- The personal data is processed in relation to online services to children.

Selce will ensure that, in certain circumstances, the **right to restrict processing of personal data** is satisfied. This can include situations where data may be inaccurate or

where the individual has objected to the processing, and Selce is considering whether its legitimate grounds for processing data override the rights of the individual.

Under the **right to data portability**, an individual can ask for their data in a form that can easily and securely be transferred from one IT environment to another. Selce would ensure that data held can be securely transferred if a request is made.

Under the **right to object**, Selce will stop processing personal data where there is an objection unless there are compelling legitimate grounds to continue processing data, or if the processing is for the establishment, exercise or defence of legal claims. Selce will stop processing personal data for direct marketing purposes as soon as an objection is received. The right to object is included in the Selce's privacy notice.

Selce will secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and ensuring that it cannot be used to discriminate against the individual.

Should an individual wish to exercise any of the above rights, they can do so by contacting The Administrator. On request from an individual, CEO will supply details of what information is held, why it is held and to whom it may be disclosed. A copy of the relevant record of data on the individual may be supplied.

Selce will aim to comply with requests for access to personal data records within one month.

8 IMPORTANT: Breaches of procedure or loss of data

Any breach of confidentiality should be reported to the CEO, who will then appoint an appropriate independent person (e.g. a member of the board of directors or a senior member of staff) to investigate the matter. If, following a written summary of findings, the appointed person finds that a breach has occurred, they have the discretion to take appropriate action within 28 days. This may include consideration of pursuing disciplinary action or, in the case of a volunteer, asking the person to withdraw from Selce's service.

9 Guidance to staff

Selce's employees should bear in mind the following considerations:

- Sensitive and confidential information must be treated with particular attention.
- Personal data must not be shared by email – neither in the body of an email nor as an attachment. If you need to share a document containing personal data share a link to the document that only people with existing access to the document can use. The only exception to this is a requirement by a funder or local authority. If you are required to email a document containing personal data, you must password protect

the document, send the password in a separate email to the document and send both emails via a system that adds additional encryption such as Egress Switch

- Any personal data stored in paper format must be held securely locked in filing cupboards in Selce's office.
- All Selce personal computers must be password protected. All personal data should be kept in the appropriate IT system (i.e. client details in the CRM system and staff details in HR management system. If electronic equipment is lost or stolen, access to the server and database from that piece of equipment will be severed.
- The database holding clients' personal data must be accessed only via Selce's electronic equipment. All employees and volunteers will be trained on how to use the database relying on the written procedures for entering, amending and maintaining data. These procedures will be reviewed annually.
- In line with Selce's IT Security Policy, all personal data should be stored on Selce's drive. They should be stored in a location on Selce's drive to which only those members of staff who require access have such access. No personal data should be stored on the hard drive of a laptop or computer. If you download any files for ease of working, make sure you resave them in the appropriate place on Selce's drive and delete them from your computer hard drive once you have finished working with them. Whilst stored on a hard drive, any files must be, password protected. As soon as you have finished working on them and delete any local files.
- Any changes to personal data (e.g. a change in home address) must be updated on the HR folder (for staff, directors and volunteers or the CRM system for clients within 28 days of receipt.
- Personal data must not be given out to any third party unless the individual has agreed to release this information. This includes any staff members personal information
- Any personal data kept in paper format that is no longer required must be destroyed.
- Any personal data kept electronically that is no longer required must be deleted. Selce will carry out data minimisation as part of the annual data audit.
- If data needs to be processed for profiling or for other statistical information, pseudonymise it after 3 years. The procedures for this should be documented to ensure that the identification of the individuals is kept separate from the processed data.