
GDPR Data Protection Policy

POLICY INTENDED FOR:	All stakeholders
CATEGORY:	Governance and Compliance
POLICY IMPLEMENTED BY:	Head of Events
POLICY MONITORED BY:	Operations Team
REVIEWED BY:	CEO
EFFECTIVE DATE:	01/10/2025
REVIEW DATE:	01/10/2025 or as required

SSEF is committed to protecting the personal data of all individuals associated with our organisation, including employees, students, parents, and contractors, in compliance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines how we handle, store, and process personal data to ensure its security and confidentiality.

This policy ensures that SSEF:

- Complies with data protection laws.
- Protects the rights of individuals whose personal data we hold.
- Is transparent in how personal data is collected, stored, and processed.
- Reduces the risk of data breaches.

Definitions:

- Personal Data: Any information relating to an identifiable person (e.g., name, address, date of birth).
- Special Category Data: Sensitive data such as health, religion, or ethnicity.
- Processing: Any operation performed on data (e.g., collection, storage, use, destruction).
- Data Controller: SSEF, which determines how and why personal data is processed.
- Data Processor: Third parties processing data on behalf of the Data Controller.

SSEF adheres to the GDPR's data protection principles:

- Data must be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specific and lawful purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- Personal data shall be accurate and where necessary kept up to date.
- Personal data processed for any purpose(s) shall not be kept for longer than is necessary for operational purposes. Personal data no longer required is deleted or destroyed.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data is not to be transferred outside the UK unless the destination ensures an adequate level of protection.

Data Collection and Processing:

ProEd collects and processes data for the following purposes:

- Staff employment and payroll.
- Student registration and records.
- Marketing and communications.
- Health and safety compliance.

ProEd Obligations:

- Computers which hold the databases are protected with 2-factor authentication.
- Access to personal data is limited to authorised personnel only.
- SSEF ensures that any third-party organisations and systems are GDPR-compliant. SSEF only shares personal data if it is necessary for legitimate operational purposes.
- All breaches must be reported immediately to the CEO.
- Individuals can object to data processing for specific purposes.
- Individuals with concerns about data handling can contact the CEO.