1.1.1.3 Data Protection and Privacy Policy

Purpose

This policy defines SESP's commitment to safeguarding all personal and confidential information obtained, processed, and stored in the course of its training, administrative, and support operations.
It ensures that personal data are handled lawfully, transparently, and securely in compliance with applicable data-protection laws, including the EU General Data Protection Regulation (GDPR) and the Saudi Arabian Personal Data Protection Law (PDPL).

Scope

This policy applies to all personnel, contractors, learners, and third-party service providers who collect, access, use, or manage personal data on behalf of SESP.
It covers all formats and media – electronic, paper, image, and audio – and applies to:

- Staff and trainee records;
- Financial and administrative information;
- Partner, employer, and supplier data;
- Learning-management and IT systems operated by SESP.

Policy Statement

SESP recognizes the right of every individual to privacy and the protection of personal data.
The organization shall:

1. Collect and process personal data only for legitimate business, educational, or regulatory purposes;
2. Obtain data lawfully and fairly, with informed consent where required;
3. Limit data collection to what is necessary and relevant;
4. Keep personal data accurate, up to date, and retained only for as long as required by law or internal policy;
5. Protect data through appropriate technical and organizational controls;
6. Respect the rights of data subjects to access, correct, restrict, or request deletion of their personal data; and
7. Report and investigate any suspected data breach promptly and transparently.

Definitions

- Personal Data: Any information relating to an identified or identifiable natural person.
- Processing: Any operation performed on personal data (collection, recording, storage, retrieval, disclosure, or deletion).
- Data Subject: An individual whose personal data are processed by SESP.

- Data Controller: SESP, which determines the purpose and means of data processing.
- Data Processor: Any third party processing data on SESP's behalf.

Responsibilities

Role	Responsibility
Executive Officer (OEO)	Ensures organizational compliance and approves the policy.
Quality Unit (QUU)	Oversees integration of data-protection controls within the QMS and monitors compliance audits.
IT & Educational Technology (SSD _ITE)	Implements technical safeguards, access controls, encryption, and system-security measures.
Human Resources (SSD _HRA)	Manages employee and trainee records in compliance with retention and privacy requirements.
All Employees and Trainers	Handle personal data responsibly and report any suspected breach or unauthorized access immediately.

Data Protection Principles

SESP applies the following core principles to all processing activities:

1. Lawfulness, Fairness, and Transparency – personal data processed for legitimate purposes with clear communication to data subjects.
2. Purpose Limitation – used only for the purpose originally collected.
3. Data Minimization – limited to data necessary for the stated purpose.
4. Accuracy – maintained and updated as necessary.
5. Storage Limitation – retained only as long as required by policy or law.
6. Integrity and Confidentiality – protected against unauthorized access, loss, or destruction through technical and procedural safeguards.
7. Accountability – SESP demonstrates compliance through records, training, and continual review.

Access and Security Controls

- Access to personal data is restricted by role and authorized credentials.
- All electronic systems use password protection, multi-factor authentication, and regular backups.
- Physical files are secured in locked cabinets or restricted areas.
- Data transfers to external parties require written agreements ensuring equivalent protection levels.
- Portable media and devices must be encrypted when containing personal data.

Data Retention and Disposal

Data are retained in accordance with the Records Retention Procedure (SSD_HRA-PRO-003) and statutory requirements.
At the end of the retention period, records are securely destroyed or anonymized.
Destruction is documented and verified by authorized personnel.

Incident Reporting and Breach Response

Any suspected data breach must be reported immediately to the IT Department and Quality Unit.
A breach investigation will determine scope, impact, and remedial actions.
Where required, affected individuals and regulatory authorities will be notified within applicable legal timeframes.

Training and Awareness

All employees receive data-protection and information-security awareness training at induction and periodically thereafter.
Specialized training is provided to personnel handling sensitive or high-risk information.

Review and Audit

This policy is reviewed annually or following major regulatory, organizational, or technological changes.
Compliance with this policy is verified through internal audits conducted by the Quality Unit (QUU).