Group Data & Information Management Policy

Policy statement

SSE's policy is to collect and use all data responsibly and securely and to maximise the use of its data assets in an ethical and sustainable way to achieve a low cost, low carbon future for energy consumers.

Policy purpose

The purpose of this policy is to support SSE in meeting legal and regulatory requirements for data management, retention and reporting, and managing data assets in line with the strategic vision to be a "leading energy company in a low carbon world'.

This policy is owned by the General Counsel and is one of a suite of group-level policies that promote a healthy business culture, guide decisions and actions as expected by the company's stakeholders, and make SSE a responsible company that people want to invest in, buy from, work for and partner with.

Liz Tanner
General Counsel

Alistair Phillips-Davies
Chief Executive Officer

Doc Ref: PO-GRP-004
Version: 1.02
Effective Date: April 2022
Review Date: April 2023

POLICY PRINCIPLES

The following principles highlight how we expect the policy statement to be achieved, and should be used to guide behaviours, decision making and action:

Data Governance	• Data Governance shall be adopted to improve our Data Management capabilities and embed best practice data culture, accountability and strategic oversight through ownership, stewardship, policies, procedures, monitoring and reporting.
Data and Information Management	• SSE's Data Management approach is driven by business benefits and aims to reduce risk and improve profitability by actively managing the creation, use, storage and destruction of both digital and physical information and data in all its forms (documents, records, content) and knowledge. • Data Management practices shall be adopted to increase the prevalence and use of trusted data sources, including Data Quality Management and Metadata Management practices. • Data shall be classified and stored in a safe and secure manner. Access to data by employees, customers and suppliers shall be controlled to ensure confidentiality of Business Units and business separation is observed appropriately.
Data Sharing and Interoperability	• SSE recognises the drive to modernise energy data and the importance of this vision in the delivery of a net zero carbon future. SSE seeks to make key energy system data discoverable and accessible to stakeholders to promote transparency and innovation, whilst maintaining robust processes to prevent the dissemination and misuse of sensitive data.
Personal Data	• SSE is committed to collecting and using personal data responsibly, securely and fairly. We want people to understand how we use their data and to become a trusted partner with our customers; we protect the personal data of our employees to the same high standards. • Personal data shall be: o Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency') o Collected for specified, explicit and legitimate purposes ('purpose limitation')

	○ Adequate, relevant and limited to what is necessary ('data minimisation') ○ Accurate and, where necessary, kept up to date ('accuracy') ○ Kept for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation') ○ Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

ROLES AND RESPONSIBILITIES

This policy applies to all SSE employees, contingent workers and people contracted to provide services to the Company through third parties.

Business Unit MD's, BU Directors and Corporate Directors are responsible for the management of data and data-related resources relating to their business unit including the ownership, stewardship and operational controls to ensure that data is managed as an asset.

Managers are responsible for making sure that their teams understand and comply with the policy and supporting procedures as well as complete any relevant training.

All employees must comply with the policy and supporting procedures and complete all relevant training.

The **Data Management Team** report to the **Chief Data Officer** and act as a centre of excellence providing support to the business on best practice.

SSE's **Group Data Protection Officer** is supported in her tasks under Article 39 of the GDPR by designated **Data Protection Specialists** ('DPS's) within each Business Unit.

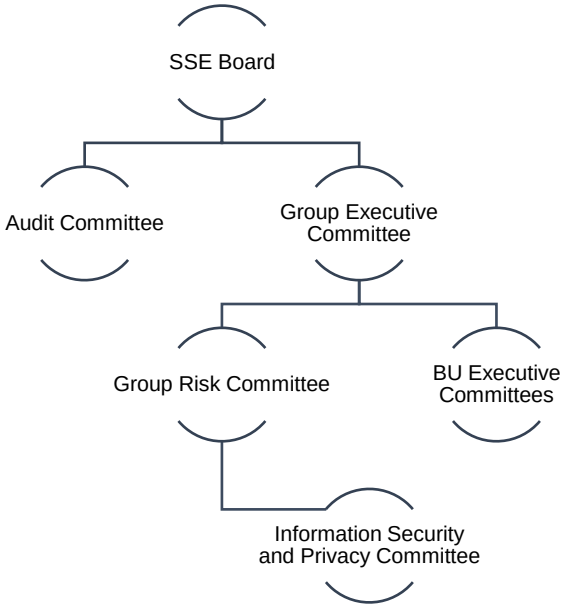
GOVERNANCE

The **SSE plc Board** and **Group Executive Committee** are responsible for the oversight for this policy including the approval of any changes to the policy. This policy is reviewed annually as part of an evaluation process.

The **Group Executive Committee** supports the Policy Owner and ensures that the policy is adhered to through awareness, training and monitoring of policy implementation. Incidents and breaches are reviewed and where appropriate opportunities for improvement are actioned.

Business Unit Executive Committees maintain oversight of BU data management activities to ensure they are aligned to overarching business strategies, goals and vision statements. In some BU's Data Governance Boards, under the delegated authority of the Business Unit Executive Committee, deliver the BU data strategy, coordinates and monitors data governance and data improvement activities.

SSE's **Group Data Protection Officer** monitors GDPR compliance and is required to be involved in all issues which related to the protection of personal data. She provides regular GDPR updates to SSE Board and the Group Executive Committee.



TRAINING

Annual GDPR training is a mandatory requirement for all SSE employees.

Data and information management incorporates a wide range of topics impacting numerous roles and therefore subject specific training is provided as required through relevant business units utilising both internal and external subject matter experts.

SPEAKING UP

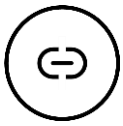
Any known loss of information should be reported and will be investigated accordingly.

All data protection incidents shall be reported via the Data Protection Incident Portal (DPIP), a group wide internal tool. Potential penalties include:

- Monetary penalty of up to 4% of the total worldwide annual turnover for SSE.
- Unlimited fines for an individual who unlawfully obtains or misuses personal data.

If you see or hear something that falls short of our expected high standards of ethical conduct and compliance you should be able to discuss it with your manager or a Speak Up Ambassador, but when that is not possible you are encouraged to raise issues with SafeCall through the following channels:

- Phone: 0800 915 1571 (UK) 1800 812 740 (Ireland)
- Email: sse@safecall.co.uk
- www.safecall.co.uk/report



SUPPORTING DOCUMENTS

Additional documents available to provide further guidance and support include:

- Information Classification Standard
- Data Protection
- Data Management
- Group Data Governance Framework

Further information can be found on SSEnet -

- DnA Intranet Page
- Data Protection Centre
- Data Directions Sharepoint

Complementary Policy:

- PO-GRP-003 Group Cyber Security Policy.

DEFINITIONS

Data Governance is a decision making, monitoring and enforcement body that has authority over Data Management.

Data Management is the control of data architecture, quality, security, policy, practices and procedures.

Data Assets. Data can be considered an asset when it is used to deliver economic value such as using data needed to perform core business functions to automate services e.g. through chatbots.

Personal data means any information relating to an identified or identifiable natural person ('data subject')

Metadata is data that describes other data, the underlying structure, meaning and relationships of data.

Comments and feedback on this policy and its application are welcome.

Please contact sheena.wilson@sse.com