DATA PROTECTION POLICY

DOCUMENT VERSION CONTROL – GOVERNANCE SCHEME

Date	Author	Version	Status	Reason for Change
Oct 2006	SEStran	1.0	Policy created	Implementation
Oct 2017	SEStran	1.1	Adoption of version control	Implementation

A. **INTRODUCTION**

1. This is a statement of the Data protection Policy adopted by SEStran, the Regional Transport Partnership (RTP) for the South East of Scotland. This policy is applicable to all personal data held by the RTP. It applies to all employees and elected members of the RTP and to any contractors or agents performing work for or on behalf of the RTP and any other individuals with access to SEStran's information.

2. SEStran is a partnership of 8 councils; Edinburgh, Fife, Clackmannanshire, Scottish Borders, Falkirk, West Lothian, East Lothian, and Mid Lothian and provides a wide range of services not only within these boundaries but as part of a group of RTPs across Scotland.

3. SEStran needs to process certain types of data about people with whom it deals in order to operate ("personal data"). This includes current, past and prospective employees, suppliers, clients and customers, and others with whom it communicates.

4. In order to comply with the Data Protection Act 1998 SEStran must ensure that all personal data are securely stored and processed lawfully however it is collected, recorded and used. Safeguards are in place to observe the legislation of the Act, these are detailed below.

5. SEStran regards the safekeeping of all personal data as paramount to maintaining confidence between it and those with whom it deals. SEStran endeavours to fulfil all the requirements of the Act while remaining open and accessible by the public.

B. **SCOPE**

This policy is applicable to all personal data held by SEStran whether the information is held or accessed on SEStran premises or accessed remotely via mobile or home working or by using network access from partner organisations. Personal information held on removable devices and other portable media is also covered by this policy.

C. **THE DATA PROTECTION PRINCIPLES**

6. To that end, SEStran fully endorses and adheres to the eight Data Protection Principles set out in the Data Protection Act 1998 (the "Act").
7. These Principles can be summarised as follows:

- Personal data must be fairly and lawfully processed

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that or those purposes.
- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data must be accurate and up to date
- Personal data must be not kept longer than necessary
- Personal data must be processed in accordance with the individual's rights under the Act
- Personal data must be secure and appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to countries outside the European Economic area unless that country has adequate protection for the individual

WHAT SESTRAN WILL DO

8. To ensure compliance with the above data protection principles SEStran shall, through appropriate management and strict application of criteria and controls;
   - observe, fully, conditions regarding the fair collection and use of data;
   - meet its legal obligations to specify the purposes for which data is used;
   - collect and process appropriate data, and only to the extent that it is required to fulfill operational needs or to comply with any legal requirements;
   - ensure the quality of the data used;
   - apply strict checks to determine the length of time the data is held;
   - ensure that rights of people about whom data is held can be fully exercised under the Act. These include:

     (i) the right to be informed that processing is being undertaken;

     (ii) the right of access to one's personal data;

     (iii) the right to prevent processing in certain circumstances; and

     (iv) the right to correct, rectify, block or erase data which is regarded as wrong data;

Subject Access Requests

The Data Protection Act also allows people to find out what personal information is held by organisations about them by making a Subject Access Request. A SAR can include electronic information and paper records. The organisation must provide the information within 40 calendar days (there are some exceptions to this).

Data Subjects who wish to make a SAR to SEStran will need to provide evidence of their identity. There is no charge for the first SAR made by a data subject to SEStran. However repeat requests, particularly detailed requests or multiple requests made over a short period of time, may incur a small charge (£10). Fees will be applied on a case by case basis.

- take appropriate technical and organisation security measures to safeguard personal data;
- ensure that personal data is not transferred outside the European Economic area without suitable safeguards.

9. In addition SEStran will ensure that:

- there is someone with specific responsibility for data protection in the organisation;
- everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal data is appropriately trained do to so;
- everyone managing and handling personal data is appropriately supervised;
- anyone wishing to make enquiries about handling personal data knows what to do;
- queries about handling personal data are competently and courteously dealt with;
- methods of handling personal data are clearly described;
- a regular review and audit is made of the way personal data is managed;
- methods of handling personal data are regularly accessed and evaluated; and
- performance with handling personal data is regularly accessed and evaluated.

RESPONSIBILITIES

The Partnership Director has specific responsibility for data protection within SEStran.

The Partnership Director has responsibility for ensuring that the information under their control is collected, processed and held in accordance with this policy and the Data Protection Act 1998.

All employees and elected members of the RTP and any contractors or agents performing work for or on behalf of the RTP and any other individuals with access to SEStran's information have a responsibility to ensure that personal information is properly protected at all times. This requires continued compliance with the SEStran's information policies, procedures and other guidance.

All users have a responsibility to report any observed or suspected breach of this Data Protection Policy or related information procedures and guidance. This includes relevant legislation: Data Protection Act 1998, Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.

All incidents must be reported to [the Office Manager

GENERAL

10. This document states SEStran's primary, general policy with regard to Data Protection. SEStran also has policies, codes of practice, protocols and guidance, as appropriate, for specific types of data maintenance and data type. Additional data specific policies, codes, protocols and guidance will be adopted as and when necessary.

REVIEW

11. This policy will be reviewed annually, to take account of developments within SESTRAN and legislative requirements.