Highland Senior Citizens Network

HSCN

HIGHLAND SENIOR CITIZENS NETWORK
DATA PROTECTION AND PRIVACY POLICY

1. Introduction

The Highland Senior Citizens Network needs to collect and use certain types of information about the individuals and groups who come into contact with the Network in order to carry on our work. This personal information must be collected and dealt with appropriately whether collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 2018.

2. Data Protection Officer

A Data Protection Officer (DPO), with the Trustees, determines what purposes personal information held will be used for. The DPO takes responsibility for Data Protection compliance.

3. Disclosure

This information is held only for the purpose of providing individual/group members with information about Highland Senior Citizens Network and other information that we think would be of interest to older people in Highland.

We will only disclose information with your consent or where it is authorised under the Data Protection Act.

The Network regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

4. Data Protection Act 2018

To this end, the Network will adhere to the Principles of Data Protection, as detailed in the above Act 2018. Specifically, the Principles require that personal information shall be:

a) processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
b) obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
c) adequate, relevant and not excessive in relation to that/those purpose(s),
d) accurate and, where necessary, kept up to date,
e) kept for no longer than is necessary,
f) processed in accordance with the rights of data subjects under the Act,

g) kept secure by the appropriate person who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information and
h) untransferrable to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal information.

The Network will, through appropriate management and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information,
- meet its legal obligations to specify the purposes for which information is used,
- collect and process appropriate information and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- ensure the quality of information used,
- ensure that the rights of people about whom information is held can be fully exercised under the Act. These include the right to:

    - be informed that processing is being undertaken,
    - access to one's personal information,
    - prevent processing in certain circumstances, and
    - correct, rectify, block or erase information which is regarded as wrong information

- take appropriate technical and organisational security measures to safeguard personal information,
- ensure that personal information is not transferred abroad without suitable safeguards,
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information, and
- set out clear procedures for responding to requests for information.

5. Data Collection

Informed consent is when:

- an individual or group clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data, and
- then gives their consent.

The Network will ensure that data is collected within the boundaries defined in this Policy. This applies to data that is collected in person or by completing a form. When collecting data, the Network will ensure that the individual/group:

a) clearly understands why the information is needed,

b) understands what it will be used for and what the consequences are should the individual decide not to give consent to processing,
c) as far as reasonably possible grants explicit consent, either written or verbal, for data to be processed,
d) is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress and
e) has received sufficient information on why their data is needed and how it will be used.

6. Data Storage

Information and records, including disclosure checks, relating to individuals/groups will be stored securely in the Highland Senior Citizens Network locked filing cabinet in accordance with the principles of the Data Protection Act 2018 and will only be accessible to nominated Trustees and employees.

Such information may be requested in writing by the individual/group member at no charge allowing the organisation one month to fulfil this request and the information may be rectified/deleted as instructed by the member.

Information will be stored for only as long as it is needed, required by statute or as long as you wish to remain a member and it will be disposed of appropriately. This will be a minimum seven years for financial records and six years for members, staff/HR information.

It is the Network's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

7. Data Access and Accuracy

All individuals have the right to access the information the Network holds about them. Data will be verified on an annual basis by asking members if their contact data needs updating by including a mailing with the Spring Newsletter, by their preferred method of contact.

In addition, the Network will ensure that:

- it has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection
- everyone processing personal information understands that they are contractually responsible for following good data protection practice
- it deals promptly and courteously with any enquiries about handling personal information
- it describes clearly how it handles personal information
- it will regularly review and audit the way it holds, manages and uses personal information
- it regularly assesses and evaluates its methods and performance in relation to handling personal information
- any breach of the Data Protection and Privacy Policy will be reported as soon as possible to the Information Commissioner's Office within 72 hours of

becoming aware of the breach, where feasible, even if full details are not yet available
- all staff and Trustees are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

In the case of any queries or questions in relation to this policy please contact the Data Protection Officer at:

Highland Senior Citizens Network
Box 301
8 Church Street
Inverness IV1 1EA
Telephone: 07716 884989
Email: hscn@hotmail.co.uk

Glossary of Terms

Data Protection Act 2018 – the UK legislation which provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that the Network follows its Data Protection and Privacy Policy and complies with the Data Protection Act 2018.

Individual/Group – the person or groups whose information is being held or processed by the Network.

Explicit Consent – is a freely given, specific and informed agreement by an individual/group in the processing of personal information about them. Explicit consent is needed for processing sensitive data.

June 2018