

DATA PROTECTION

## Aims of this Policy

1. Healthwatch Isles of Scilly needs to keep certain information on its service users, members, employees and directors to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

1. This policy covers employees, directors and other volunteers.
2. This policy should be read in conjunction with the Healthwatch Isles of Scilly policy on Information Governance - representation, confidentiality and communications.
3. **The key requirements of the Data Protection Act**
4. In line with the Data Protection Act 1998 principles, Healthwatch Isles of Scilly will ensure that personal data will:
* be obtained fairly and lawfully and shall not be processed unless certain conditions are met;
* be obtained for a specific and lawful purpose;
* be adequate, relevant but not excessive;
* be accurate and kept up to date;
* not be held longer than necessary;
* be processed in accordance with the rights of data subjects;
* be subject to appropriate security measures;
* not to be transferred outside the European Economic Area (EEA).

The definition of ‘Processing’ is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

1. The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. Healthwatch Isles of Scilly will seek to abide by this code in relation to all the personal data it processes, i.e.
* **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
* **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
* **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA’s eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject’s consent should be explicitly obtained.
* **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
* **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.
1. **Policy Implementation**
2. To meet our responsibilities, all staff, directors and other volunteers will:
* ensure any personal or confidential information is collected in a fair and lawful way;
* explain why it is needed at the start;
* ensure that only the minimum amount of information needed is collected and used;
* ensure the information used is up to date and accurate;
* review the length of time information is held;
* ensure it is kept safely;
* ensure the rights people have in relation to their personal data can be exercised.

 We will ensure that:

* everyone managing and handling personal or confidential information is trained to do so;
* anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
* any disclosure of personal data will be in line with our procedures;
* queries about handling personal information will be dealt with swiftly and politely.
1. Training and maintaining awareness about the Data Protection Act and how it is followed in the organisation will take the following forms:
* staff and directors who handle and process personal information will have the relevant policies given and explained to them:
	+ data protection policy
	+ information governance policy
* staff, directors and other volunteers who may receive personal or confidential information will have the relevant policies given and explained to them:
	+ information governance policy
	+ procedure for managing direct feedback
1. Regular reminders about procedures will be given to staff in supervision meetings.
2. All policies will be reviewed biannually by the Board of Directors.
3. **Responsibilities**
4. Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of Healthwatch Isles of Scilly, this is the Board of Directors.

 The governing body delegates responsibility to the Manager. The Manager is responsible for:

* understanding and communicating obligations under the Act;
* identifying potential problem areas or risks;
* producing clear and effective procedures;
* supervision of all staff who process information.
1. All employees and volunteers who process personal or sensitive information must ensure they not only understand but also act in line with this policy and the data protection principles.
2. **Breaches of this policy**
3. Anyone who suspects that a breach of data protection or confidentiality has occurred may use the Healthwatch Isles of Scilly Complaints Procedure.
4. Any unauthorised disclosure made by an employee will result in disciplinary proceedings.

Any unauthorised disclosure made by a director or other volunteer may result in the termination of the volunteering agreement.

A breach of this policy by any employee, director or other volunteer will be reported and attended to by the Manager and Chair, in the first instance.

If the matter concerns the Chair, it will be reported and attended to by another Director.

1. **Type of information processed**
2. Healthwatch Isles of Scilly processes the following personal information:
* members’ contact details;
* service users’ contact details, where they have given permission;
* information about individual directors necessary for records held at Companies House;
* information about employees in accordance with normal employment requirements and processes;
* information about job applicants, during the recruitment process only. All personal information pertaining to unsuccessful applicants will be securely destroyed at the end of the recruitment process.
1. The organisation also collects confidential information in the form of community feedback about people’s experiences of health and social care. All such information is recorded anonymously, or where the individual has given permission to be contacted, by a coded reference system.

Healthwatch Isles of Scilly may also receive confidential information about services during the course of its work.

The way that confidential and sensitive information is processed is set out in part 7 of this policy and in the Healthwatch Isles of Scilly policy on Information Governance - representation, confidentiality and communications.

1. **Gathering and checking information**
2. Before personal information is collected, we will consider:
* what details are necessary for our purposes;
* how long we are likely to need this information.

We will inform people whose information is gathered about the following:

* why the information is being gathered;
* what the information will be used for;
* who will have access to their information (including third parties) and in what form.
1. We will ask members and volunteers to check the contact details we hold for them from time to time.
2. Personal sensitive information will not be used apart from the exact purpose for which permission was given.
3. **Data Security**

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

* personal and confidential information on paper will be securely stored in a lockable filing system;
* personal and confidential information in digital form will be stored on password protected computers;
* personal and attributable confidential information will not be taken off site, unless on a password protected device;
* back up data which is held off site will be stored on a password protected device.
1. **Subject Access Requests**
2. Anyone whose personal information we process has the right to know:
* what information we hold and process on them;
* how to gain access to this information;
* how to keep it up to date;
* what we are doing to comply with the Act.
1. They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.
2. Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to:

The Manager
Healthwatch Isles of Scilly, Gleaner House, Porthcressa, St Marys, Isles of Scilly TR21 0HW
01720 423037
contact@healthwatchislesofscilly.co.uk

1. **Review**

This policy will be reviewed at intervals of 2 years to ensure it remains up to date and compliant with the law.

**Declaration**

I confirm I have read and understood Healthwatch Isles of Scilly’s Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

* Member of staff
* Director
* Volunteer

Signature:

Print name:

Date:

Please return this form to the Manager, Healthwatch Isles of Scilly.