Information Governance Policy

There are six areas of activity that relate to Information Governance:

- Policy Implementation
- Awareness
- Monitoring and Assurance
- Records and Information Management
- Information Security
- Collection and Use of Personal Information

Policy Implementation:
Healthwatch Portsmouth will apply its Information Governance Policy to all of its activities. Healthwatch Portsmouth has a Privacy Statement which sets out our data processing activities.

Awareness:
Healthwatch Portsmouth will ensure that its staff and volunteers are made aware of the policy and procedures as set out by Learning Links through training offered to staff and volunteers.

Monitoring and Assurance:
Healthwatch Portsmouth will abide by the policies and procedures that have been developed by Learning Links, of which Healthwatch Portsmouth is a project, relating to information quality assurance and the effective management of records and data. Wherever possible information quality will be assured at the point of collection. Healthwatch Portsmouth undertakes an annual assessment of its information quality and records management arrangements.

Records and Information Management:
Healthwatch Portsmouth regards all identifiable personal information relating to individuals as confidential. Healthwatch Portsmouth has effective methods in place to manage our records and information. We know what information we hold and where it is stored so that we can retrieve information efficiently. Our information management system allows us to respond quickly to requests from individuals for information on what data is held on them, how it will be used, stored and disposed of. We publish information on our website about our activities and our Board meetings held in public to promote openness and transparency.

Information Security:
Healthwatch Portsmouth adheres to the policies and procedures set out by Learning Links for the effective and secure management of its information assets and resources. Healthwatch Portsmouth undertakes an annual assessment and audit of its information and IT security arrangements. Healthwatch Portsmouth follows the confidentiality, data and record management and security of information practices of Learning Links as set out in the staff policy and procedures handbook. Healthwatch Portsmouth will implement and maintain incident reporting procedures, monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.

Collection and Use of Personal Information:
Healthwatch Portsmouth will seek individuals' permission before using any personal information or any images in any publicity materials. Information that individuals have consented to provide to Healthwatch Portsmouth is held securely and used to:

- respond to the individual's correspondence
- send out information about health and social care, our newsletter or notices of meetings
- contact individuals to seek feedback on health and social care services or service reviews

Data Protection Policy extract from Learning Links Staff Handbook for Healthwatch Portsmouth

This policy is intended to assist Healthwatch Portsmouth in compliance with the General Data Protection Regulations and Data Protection Bill which become effective from 25th May 2018 and to establish good practice for handling personal data in the workplace.

Our Data Protection Policy classifies all personal data and handling of data as equally sensitive and subject to our security processes and current General Data Protection Regulation legislation.

Responsibilities

Healthwatch Portsmouth will adhere to the following principles in the course of its activities:

- That the Data is obtained and processed fairly and lawfully;
- That the Data is held for specific purposes only;
- That disclosure is compatible with the purposes and uses identified;
- That the Data is adequate, relevant and NOT excessive;
- That the Data is accurate and up to date;
- That the Data is held for no longer than necessary;
- That subject access is made in line with our policy and that corrections and erasures are carried out if requested;
- That the security principles are implemented: - keeping of the data is maintained i.e. storage facilities, back up disks;
- That accidental destruction or loss is prevented;
- That any passwords are kept confidential;

Employees must ensure that any files of a confidential nature should be in a lockable filing unit. Staff should report security loopholes, breaches and accidental loss or destruction of data immediately to a designated IT Security Monitor. Please refer to the Data Security Breach Policy.

No employees should disclose personal data outside our operational procedures, or use personal data held on others for their own purposes.

An employee disclosing personal data without the authority of a line manager may find himself/herself subject to disciplinary and/or legal proceedings.

Processing

Healthwatch will comply with the General Data Protection Regulations and Data Protection Bill which become effective from 25th May 2018 and applies to personal data that is subject to 'processing'. For the purposes of the Act, the term 'processing' applies to a comprehensive range of activities. It includes the initial obtaining of personal data, the keeping and use of, accessing and disclosing of data through to its final destruction.