| Policy/Procedure Title: | Information Governance |
|---|---|

| Domain | Information Governance | | |
|---|---|---|---|
| Number | IG 1 | | |
| Main author | CEO | Ratified by | The Board |
| Date Written | 03/05/2018 | Ratification date | 21/05/2018 |
| Date Distributed | 21/05/2018 | Review date | June 2019 |
| Responsible Group/person | CEO | Ratified by | |

| Version Number: | Date: | Supersedes Version No: |
|---|---|---|
| V1 | 21/03/2018 | |

These procedures are applicable to staff employed by and/or working for and/or delivering services to or on behalf of (whether directly or through sub-contract arrangements) Healthwatch Central West London.

These procedures apply to the following group(s) of staff:

| Staff Group | Yes |
|---|---|
| All staff | ✓ |
| Volunteers | ✓ |

Contents

## 1. Introduction

1.1 This strategy describes the development and implementation of a robust Information Governance (IG) framework needed for the effective management and protection of organisational and personal information.

1.2 Information Governance describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used in the organisation are sourced, held and used appropriately, securely and legally.

1.3 Information is a vital asset for the organisation supporting the effective function of the organisation. Therefore, it is essential in order to meet requirements that the entire organisation's information is managed effectively within a robust governance framework.

1.4 The organisation requires accurate, timely and relevant information to enable it to operate effectively as an organisation. It is the responsibility of all staff to ensure that information is accurate and up to date and that it is used proactively in its business. Having accurate relevant information available at the time and place where it is needed, is critical in all areas of the organisation's business and plays a key part in corporate governance, strategic risk, organisational planning and performance management.

1.5 The organisation carries a responsibility for handling and protecting information of many types:

1.5.1 Some information is confidential because it contains personal details of service users or staff. The organisation complies with legislation which regulates the holding and sharing of confidential personal information. It is important that relevant, timely and accurate information is available to those who are involved in the provision or information or care to service users, but it is also important that personal identifiable information is not shared more widely than is necessary, and deleted when no longer required for the purpose.

1.5.2 Some information is non-confidential and is for the benefit of the general public. Examples include information about the organisation's services, annual reports etc. The organisation and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.

1.5.3 The majority of information about the organisation and its business should be open for public scrutiny via the website although some, which is commercially sensitive, may need to be safeguarded.

## 2. Background

2.1 Information Governance is one of the main governance arrangements within the organisation, i.e.

2.1.1 Integrated Governance
2.1.2 Risk Management
2.1.3 Research Governance
2.1.4 Financial Governance
2.1.5 Information Governance

2.2 This strategy must be read in conjunction with any other related policies, eg Data Protection Policy, Confidentiality, Subject Access Request policy.

2.3 Information Governance covers all information held by the organisation (for example; clinical, staff, financial, estates, corporate, minutes, e-mails) and all information systems used to hold that information. These systems may be purely paper based or partially or

totally electronic. The information concerned may be owned or required for use by the organisation and so may be internal, e.g. created within the organisation such as staff communications, or external e.g. created by an external organisation such as contract tender submissions.

2.4 The governance requirements are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the organisation and ensuring that relevant information is available where and when it is needed.

2.5 Information Governance (IG) is considered under 7 themes:

- 2.5.1 Information Governance Management
- 2.5.2 Data Protection
- 2.5.3 Confidentiality Code of Conduct
- 2.5.4 Service User Records Management
- 2.5.5 Corporate Records Management
- 2.5.6 Information Quality Assurance
- 2.5.7 Information Security.

2.6 Information Governance contributes to ensure people who use services can be confident that:

- 2.6.1 Their personal records, applications, records of advice given are accurate, fit for purpose, held securely and remain confidential
- 2.6.2 Other records required to be kept to protect their safety and wellbeing are maintained and held securely where required.

2.7 The Information Governance arrangements will underpin the organisation's strategic goals and ensure that the information needed to support the organisation is readily available, accurate and understandable.

2.8 Implementation of robust Information Governance arrangements will deliver improvements in information handling ensuring information is:

- 2.8.1 Held securely and confidentially
- 2.8.2 Obtained fairly and efficiently.
- 2.8.3 Recorded accurately and reliably.
- 2.8.4 Used effectively and ethically.
- 2.8.5 Shared appropriately and lawfully.

## 3. Guiding Principles

3.1 There are five interlinked principles which guide this strategy:

- 3.1.1 Openness.
- 3.1.2 Legal Compliance.
- 3.1.3 Information Security.
- 3.1.4 Quality Assurance.
- 3.1.5 Proactive Use of Information.

3.2 In developing this IG strategy, the organisation recognises and supports:

- 3.2.1 The need for an appropriate balance between openness and confidentiality in the management and use of information.
- 3.2.2 The principles of corporate governance and public accountability and equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about organisations and people using our services, staff and commercially sensitive information.

3.2.3 The need to share service user information with other agencies in a controlled manner consistent with the interests of the service user and, in some circumstances, the public interest.

3.2.4 The principle that accurate, timely and relevant information is essential to deliver a high quality service and that it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision-making processes.

3.2.5 That robust Information Governance processes are essential for sustained public and organisational confidence in the way the organisation handles its data.

## 4 Strategic Objectives

4.1 To ensure openness, the organisation will:

4.1.1 Ensure non-confidential information about the organisation and its services is readily and easily available through a variety of media

4.1.2 Review policies in line with pre-agreed review dates and review arrangements for openness regularly

4.1.3 Ensure that the public have readily and easily available access to information relating to services available

4.1.4 Have clear procedures and arrangements for liaison with the press and broadcasting media, as outlined in the Scheme of Delegation.

4.1.5 Have clear procedures and arrangements for handling queries from service users and general public.

4.2 To ensure legal compliance, the organisation will:

4.2.1 Regard all identifiable personal information relating to organisations and people using our service and public as confidential.

4.2.2 Review compliance with legal requirements regularly.

4.2.3 Regard all identifiable personal information relating to staff as confidential, except where national policy on accountability and openness requires otherwise.

4.2.4 Establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act, Equality and Common Law Duty of Confidentiality and all associated guidance.

4.2.5 Establish and maintain policies for the controlled and appropriate sharing of service user information with other agencies taking account of relevant legislation.

4.3 To ensure that appropriate and legally compliant Information Systems Security exists, the organisation will:

4.3.1 Establish and maintain the Top Level IM&T Security Policy along with respective procedures for effective policing and secure management of all information assets, resources and IT systems.

4.3.2 Regularly review its information and IT security arrangements in line with the IT security policy.

4.3.3 Promote effective confidentiality and security practice to ensure all permanent/temporary contracted staff and third party associates of the organisation adhere to this via appropriate policies, procedures, training and documentation.

4.3.4 Establish and maintain appropriate policing, incident reporting procedures and investigations of all instances (actual and/or potential), along with any reported breeches of confidentiality and security.

4.4 To ensure Information Quality Assurance, the organisation will:

4.4.1 Establish and maintain policies and procedures for information quality assurance and the effective management of service user, staff and organisational records.

4.4.2 Regularly review its information quality and records management arrangements.

4.4.3 Ensure that key data is accurately recorded and maintained, including regular cross checking against source data.

4.4.4 Ensure that all staff are required to take ownership of and seek to improve the quality of information within their area and that information quality is assured at the point of collection.
4.4.5 Promote information quality and effective records management through policies, procedures, user manuals and training.

4.5 To ensure proactive use of information, the organisation will:
4.5.1 Ensure information systems hold the information required to support effective provision of services.
4.5.2 Develop information systems and reporting processes which support effective performance management and monitoring.
4.5.3 Develop information management awareness and training programmes to support staff.
4.5.4 Support integrated governance requirements including financial, corporate, and research governance.
4.5.5 Promote an information culture and expectation of informed, evidence-based decision making.
4.5.6 Ensure that, where appropriate and subject to confidentiality constraints, information is shared with other organisations in order to support organisations and people using our service and staff.

4.6 Implementation of this IG Strategy will ensure that the organisation and its staff (including contractors and temporary staff) handle and manage information in a consistent way. This is anticipated to lead to:
4.6.1 Improvements in information handling activities.
4.6.2 Reduction in numbers of IG incidents and complaints.
4.6.3 Increased organisational and public confidence in the way the organisation handles information.

4.7 Information Governance provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal and organisational information, ensuring:
4.7.1 Compliance with the law and professional standards.
4.7.2 Implementation of relevant advice and guidance.
4.7.3 Year on year improvements.

4.8 Through implementing this strategy, the organisation will:
4.8.1 Establish robust information governance processes
4.8.2 Ensure that all practices and procedures relating to handling and holding personal and corporate information are legal and confirm to best practice.
4.8.3 Ensure that clear advice is given to organisations and people using our service and staff about how their personal information is recorded, handled, stored and shared by the organisation. Guidance will be made available to explain individual's rights, how they can seek further information and how they can raise any concerns. This guidance will be made available in alternative formats should it be required.
4.8.4 Provide clear advice and guidance to staff and ensure they understand and apply the principles of Information Governance to their working practices in relation to protecting the confidentiality and security of personal information and to ensuring the safe keeping and handling of business/corporate information, ensuring compliance with appropriate legislation.
4.8.5 Maintain a clear reporting structure and ensure through management action and training that all staff understand IG requirements.
4.8.6 Undertake regular reviews of how information is recorded, held and used. The audits will be used to identify good practice and opportunities for improvement.
4.8.7 Ensure procedures are reviewed to monitor their effectiveness so that improvements or deterioration in information handling standards can be recognised and addressed.

4.8.8 Ensure that when service developments or modifications are undertaken/new services offered, a review of all aspects of IG arrangements is undertaken to ensure they are robust and effective.
4.8.9 Work to instil an IG culture in the organisation through increasing awareness and providing training on key issues.
4.8.10 Ensure there are robust procedures for notifying and learning from IG incidents in line with the organisation's risk management policy.
4.8.11 Assess the organisation's performance using the Data Security Awareness Level 1 Workbook and develop and implement action plans to ensure continued improvement.
4.8.12 Ensure that the Information Governance improvement programme is integrated with the Board and CEO.

## 5 Information Governance Roles and Responsibilities

5.1 The Information Governance structure consists of:
5.1.1 Information Governance Lead incorporating Risk.
5.1.2 CEO has overall responsibility for Information Governance.

5.2 Operational Information Governance responsibilities are performed as they arise and as part of an annual Information Governance audit.

5.3 The organisation's CEO is responsible for:
5.3.1 Approval of IG policies and procedures.
5.3.2 Ensuring all staff complete the Data Security Awareness Level 1 Workbook
5.3.3 To keep the Board up to date with Information Governance as part of organisational progress reports

## 6 Strategy Implementation

6.1 Ensure that we keep up to date with Information Governance, appropriate to our scale and risk, by:
6.1.1 Ensuring all new staff complete the Data Security Awareness Level 1 Workbook as part of their induction. This was developed by NHS Digital with the Department of Health and the Social Care Information Centre. It is based on information governance standards considered as good practice, and inter-links with other recommendations and standards such as those in the Data Protection Act etc.
6.1.2 All current staff will complete the Data Security Awareness Level 1 Workbook within the first six months of General Data Protection Regulation coming into effect.
6.1.3 Annual refresher training for all staff.
6.1.4 Information Governance will become part of the training staff provided to volunteers.

6.2 The CEO will:
6.2.1 Undertake annual assessments of the organisations current position in relation to IG standards, using the self-assessment toolkit.
6.2.2 Agree an annual work plan / programme to ensure a year on year improvement in performance.
6.2.3 Ensure regular review of strategies, policies, procedures etc. required for Information Governance.
6.2.4 Identify resources required for implementation.
6.2.5 Monitor progress made.
6.2.6 Report on progress, incidents and issues.

## 7. Conclusion

7.1 The implementation of the Information Governance strategy, infrastructure and action plans will ensure that all types of information is more effectively managed and proactively utilised by the organisation.

## 8. Amendments / Validity of Policy

8.1 The Board and CEO will review this strategy annually or in response to any significant changes to mandatory requirements or as a result of significant information governance breaches or incidents.