Information Governance and Management
Incorporating Data Protection Policy and GDPR (May 2018)

Information	
Creation:	05/07/2013
Amended/Reviewed	4/11/2014; 25/07/2014; 08/12/2017; scheduled for 18/07/18
Signed: Chairman	

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

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

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 work. Having accurate relevant information available at the time and place where it is needed, is critical in all areas of our work and plays a key part in corporate governance, strategic risk, organisational planning and performance management.

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

- 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.

- 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.

- The majority of information about Healthwatch Lincolnshire LTD should be open for public scrutiny via the website although some, which is commercially sensitive, may need to be safeguarded.

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

- Integrated Governance
- Risk Management
- Research Governance
- Financial Governance
- Information Governance

This policy must be read in conjunction with other related policies, eg Confidentiality, Data Retention procedure and Privacy Statement.

Information Governance covers all information held by our organisation (for example; staff, financial, 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.

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.

Information Governance (IG) is considered under 7 themes:

- Information Governance Management
- Data Protection
- Confidentiality Code of Conduct
- Service User Records Management
- Corporate Records Management
- Information Quality Assurance
- Information Security.

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

- Their personal records, applications, records of advice given are accurate, fit for purpose, held securely and remain confidential

- Other records required to be kept to protect their safety and wellbeing are maintained and held securely where required.

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

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

- Held securely and confidentially
- Obtained fairly and efficiently.
- Recorded accurately and reliably.
- Used effectively and ethically.
- Shared appropriately and lawfully.

There are five interlinked principles which guide this strategy:

- Openness.
- Legal Compliance.
- Information Security.
- Quality Assurance.
- Proactive Use of Information.

In developing this policy, the organisation recognises and supports:

- The need for an appropriate balance between openness and confidentiality in the management and use of information.

- 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.

- 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.

- 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.

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

DATA PROTECTION ACT 1998

Policy Statement
Healthwatch Lincolnshire LTD (HWL) complies with the requirements of the Data Protection Act 1998 (as amended 2003) in accessing and processing personal data.

Background
HWL has in place the following procedures in order to respond to requests for information by clients or employees, and to meet the requirements of the Data Protection legislation. It is essential that members of staff are aware of all aspects of the procedures for Subject Access to Information together with the guidelines for Employees.

PROCEDURES

Data Controller. Under the Act HWL and the Directors/Trustees are ultimately responsible for its implementation. However, the designated Data Protection Coordinator dealing with day-to-day matters will be an appointed staff member agreed by the Board. Current management responsibility lead is Chief Executive Officer.

Data Protection Principles. Data controllers and all staff must abide by the following principles when processing personal data:

- Personal data shall be processed fairly and lawfully.
- 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 purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.
- Personal data shall be processed in accordance with the rights of data subjects.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
- Personal data shall not be transferred to a country outside the European Economic Area unless adequate levels of protection exist.

A data subject, meaning an individual who is the subject of personal data who presents a written request can obtain a copy of any personal data held about them on computer or in a file.

GDPR (May 2018)

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

The GDPR sets out seven key principles which lie at the heart of our organisations way of handling data:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

To ensure compliance we will refer to the Information Commissioners document: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Data Protection Officer DPO

Under the new regulations organisations must be able to sensitively and transparently deal with any potential data breaches and to do this they must have an independent Data Protection Officer. Healthwatch Lincolnshire Research, Data and Communications Officer has been identified as our designated DPO. However, in order for us to comply with legislation requirements ie our DPO not to be responsible for investigating our own potential data breach, we have partnered with Healthwatch Derbyshire and Northamptonshire to provide a 3 way DPO support service. Should any data breach be reported in Lincolnshire, Derbyshire or Northamptonshire, we will collaborate to agree which is the most appropriate DPO to handle any investigation and reporting to ICO.

DPO's in our consortium are:
Northamptonshire/Rutland DPO is Jo Spenceley, PhD, Senior Healthwatch Officer – Research, Reporting and Intelligence
Lincolnshire DPO is Dean Odell, MSc, Research, Data and Communications Officer
Derbyshire DPO is Karen Richie, CEO

Asset Register and Impact Assessment

We have in place a Healthwatch Lincolnshire Information Asset Register which a member of the public can request a copy. In addition, to comply with new GDPR requirements Healthwatch Lincolnshire have completed a Data Protection Impact Assessment and made necessary changes to our information storage and reporting systems (IMP) as a result.

Privacy statement

Our Privacy Statement sets out the data processing practices carried out by Healthwatch Lincolnshire. We retain and use personal data (information that relates to and identifies living people) to help us carry out our role as the local independent champion for people who use health and social care services.

We will always make sure that your information is protected and treated securely. Any information that you give will be held in accordance with:

- Data Protection Act 1998
- As of 25 May 2018, the new data protection legislation introduced under the General Data Protection Regulation (GDPR) and Data Protection Bill.

To complement this Data Protection and GDPR Policy, we recommend reading our full Privacy Statement document which can be accessed by using this link http://www.healthwatchlincolnshire.co.uk/data-protection/

Responsibility of Staff.

If, as part of their responsibilities, staff collect information about other people they must comply with the guidelines included in these and our privacy statement procedures. Everyone handling personal data is expected to keep personal information confidential. Personal data must only be used to assist with carrying out HWL business.

Staff guidelines for processing information are available and staff receive training to support their role and understanding of the need to comply. A standard confidentiality statement, is to be displayed in all public areas within HWL's premises. This statement is also to be brought to the attention of all clients when HWL's staff visit them.

Data Security. All staff are responsible for ensuring that:

- Any information that they manage for HWL in connection with their employment is accurate and up to date.
- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

Staff must note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information must be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected; or

- Kept only on an electronic device that is secure and password protected.

Publication of Information about HWL.
Information that is already in the public domain is exempt from the Act. It is HWL's policy to make as much information public as possible and, in particular, the following information will be available to the public for inspection:

- Names of HWL Directors/Trustees, Register of interests of Directors/Trustees and senior staff with significant financial responsibilities (for inspection during office hours only).
- List of staff.
- Photographs of key staff.
- Please note, HWL's internal phone list will **not** be a public document.

Any individual who has good reason to obtain details contained in the above should contact the Chief Executive Officer.

Requests for Information.
If requests for information are received, the name and address of the applicant are to be forwarded to the Chief Executive Officer who will deal with the request. Unless the request is received in writing the Chief Executive Officer must arrange for an application form to be sent to the enquirer to enable them, or someone on their behalf, to make the necessary written request for information. Further verification of identity may be necessary but it is hoped that this procedure will help to ensure that the applicant is in fact the data subject or has the authority to act on behalf of the data subject. Once this application form is completed, and verified by the Chief Executive Officer, the member of staff responsible for maintaining the data will be asked by the Chief Executive Officer to search for and extract the information from HWL's electronic files or the structured manual filing system and send a copy of that information to the Chief Executive Officer will coordinate HWL's response to the enquirer.

The Chief Executive Officer is to verify the identity of the applicant and contact third parties where appropriate to seek their agreement. The Chief Executive Officer will check the information to determine which material is to be excluded in line with agreed procedures and that the consent of third parties has been obtained. Appropriate arrangements will be made (on request) if literacy problems exist or transcription into a more suitable format (eg Braille, large print, audio tape) is required. The application may be given copies of material if required, but files may not be removed from HWL's premises.

Access to requested data may in some instances be refused. In such cases the Chief Executive Officer will write to the applicant giving the reasons.

Routine Enquiries. Staff who use computer-held personal data on a day-to-day basis should be able to distinguish a routine enquiry from a formal subject access request under the Act. Routine requests for information are usually concerned with individual items of data held on electronic systems or with information held on manual files. Enquiries of this nature are not subject to access requests, as defined by the Act. Only if the enquirer quotes the Act or asks for **all** the personal data held about them, are they making a formal request for access – only then should these formal procedures be invoked.

Provision of Information. It will be necessary for personal data to be despatched to the data subject within the 40-day period allowed by the Act. It is illegal to alter the data because of an access request being received.

Charging Fees. In line with GDPR requirements HWL will make no charge for dealing with a request for information. Staff will not to be charged for access to their pay or personal data.

Exemptions.
Special exemption orders apply to personal data held for social work or health purposes. These enable access to be refused in the following circumstances but only where the practice of social work or health care would be prejudiced:

- Where access to the information by the data subject would be likely to result in serious harm to him/her or some other person.

- Where access to the information might enable the data subject to know or deduce the identity of another person (other than an employee) or identify that other person as the source of the information. In this instance a judgement will be made by the Chief Executive Officer on the duty of confidentiality to the third party by disclosing information without their consent, after weighing up such factors as the steps necessary to inform them of the disclosure and what is reasonable in the circumstances.

Appeals. Where HWL and the data subject eg service user or authorised agent, are unable to reach agreement in connection with the right of access, accessing information or the classified nature of a document, an appeal can be made to the Chief Executive Officer, details of which are available on request.

Follow-up Queries and Complaints. The Chief Executive Officer will deal with any such queries or complaints that a data subject might make following inspection of the data held by HWL about them.

Amendment of Data Following Data Subject Access. In general, the subject's records will be willingly amended within 21 working days if the data is found to be inaccurate. Details of the material in dispute must be made known to the Chief Executive Officer.

Retention and Disposal of Data. HWL will keep some forms of information for longer than others. HWL archiving guidelines and retention times are set out in our Data Retention plan (copy of the plan can be downloaded from our website page http://www.healthwatchlincolnshire.co.uk/data-protection/ which is accessed within our Governance process documentation. When disposing of any document containing personal data care is taken to ensure that the document is shredded before consigning to the waste collection.

Sharing of data with other agencies – statement included in all reports

'To comply with Healthwatch Lincolnshire Data Protection Policy requirements, all information received from members of the general public, health and care providers or other stakeholders will be treated as strictly confidential at all times. Healthwatch Lincolnshire gathers and retains information via various methods eg Survey Monkey, survey forms, on-line quick polls. To comply with Healthwatch national requirements and data protection laws, we will not share our stored data in any format with any other organisation and will refuse any requests to do so unless the work has been carried out on behalf of or collaboratively with the requesting organisation'.