

## Confidentiality and Data Protection Policy & Procedure

### 1. Background

Involvement in the work of Healthwatch Kingston (hereafter HWK) may mean that on occasions the Board of Trustees (hereafter trustees), staff and volunteers (affiliates and active affiliates) will see or hear information of a **confidential nature**, which could include personal information about individuals, commercially sensitive material or information exempt from public disclosure in accordance with the Local Government Act 1972. This policy is a statement of intent and will be implemented as a procedure.

### 2. Legal Framework

HWK shall act in accordance with the following legislation:

- Local Government Act 1972
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- The Public Disclosure Act 2012

The **Data Protection Act** gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. The Act works in two ways.

Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of Data Subjects
- Secure
- Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

### 3. Scope

For the purpose of this policy, HWK confidentiality extends to any sensitive information that HWK is party to in the course of its activities. This includes information passed on in writing and verbally. Data protection relates to the storage, access, and control of personal information held for HWK and with the permission of the person to whom those details relate.

This policy applies to the Board of Trustees, staff and volunteers of HWK. This policy will enable HWK to:

- Comply with the law in respect of the data it holds about individuals
- Follow good practise
- Protect clients, staff, volunteers and other individuals
- Protect the organisation from the consequences of a breach of its responsibilities

HWK will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

HWK recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. Information about the trustees, staff, volunteers and clients will be used fairly, securely and not disclosed to any person unlawfully. The Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, HWK will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Parkwood Healthcare (hereafter Parkwood) on behalf of HWK is the **Data Controller** and is registered under the Data Protection Act 1998. All processing of personal data will be undertaken in accordance with the data protection principles.

#### 4. Confidentiality

HWK's work is based upon the gathering of views and experiences of people about health and social care services. To do this HWK will be party to and record information that could be considered confidential. In relation to its work confidentiality can take two forms:

- **Sensitivity related confidentiality** (i.e. the type of information) - individuals, groups or communities may disclose to HWK information that is of a sensitive nature, and is passed on in confidence. Sensitive information may be passed on to HWK trustees, staff or volunteers to highlight a particular issue. This could include for example: details of treatment received for a medical condition to demonstrate an experience of accessing a service; or a service user might talk about personal circumstance, experiences of a personal nature, complaints made, cases of mistreatment or discrimination, or a combination of personal details which may allow them to be identified, such as their age or post code.
- **Safety related confidentiality** (i.e. the handling of information)- this is related to how confidential information given to HWK is stored. For example, how a person's contact details are recorded and protected so only those authorised to access them are able to and how data from surveys and interviews with service users is kept.

HWK is committed to ensuring confidential services to all individuals. The confidentiality is between the individual and HWK, NOT the member of staff or volunteer delivering a particular service.

Confidential information will not be sought from a client unless expressly in the interests of that client, i.e. to enable better service delivery.

Information will only be passed to another agency or to other individuals outside of HWK with the consent of the client, where possible this will be with written consent. If a member of staff or volunteer intends to get information from another agency to help the client or to refer them to another agency then this must be explained to the client and their permission given.

No personal information about trustees, staff, volunteers or users of HWK services will be given to any third party (including a member of their family), without their consent. Information will only be divulged on a “need to know” basis.

Any individual in contact with HWK is entitled to privacy and will be made aware that they can specifically request to be seen in private by a member of staff.

Information will be treated in confidence and will not be divulged to anyone outside HWK except where extenuating circumstances exist. These could include but are not limited to:

- That a person could cause danger to themselves or to others
- There is suspicion or hard evidence of abuse or a safeguarding incident
- Information is provided that indicates a crime has been committed
- Disclosure is required by law, for example, by the police

The decision on whether to break confidentiality will be decided on a case-by-case basis by the Chair of the Board of Trustees and the Manager of HWK.

## 5. Procedures

### 5.1 Definitions

5.1.1 The **Data Subject** is the individual whose personal data is being processed. Examples include:

- The Board of Trustees
- Employees - current and past
- Volunteers
- Job applicants
- Users
- Suppliers

Processing means the use made of personal data including:

- Obtaining and retrieving
- Holding and storing
- Making available within or outside the organisation
- Printing, sorting, matching, comparing, destroying

5.1.2 The **Data Controller** is the legal ‘person’, or organisation, that decides why and how personal data is to be processed. The data controller is responsible for complying with the Data Protection Act.

5.1.3 The **Data Processor** - the data controller may get another organisation to be their data processor, in other words to process the data on their behalf. Data processors are not subject to the Data Protection Act. The responsibility of what is processed and how remains with the data controller. There should be a written contract with the data processor who must have appropriate security.

5.1.4 The **Data Protection Officer** is the name given to the person in organisations who is the central point of contact for all data compliance issues.

## 5.2 Responsibilities

5.2.1 The Parkwood Management Team recognises its overall responsibility for ensuring that HWK complies with its legal obligations.

The Data Protection Officer has the following responsibilities:

- Briefing the Project Management Team on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Ensuring contracts with Data Processors have appropriate data protection clauses
- Electronic security
- Approving data protection-related statements on publicity materials and letters

5.2.2 Each trustee, member of staff or volunteer who handles personal data will comply with Parkwood's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed.

5.2.3 The trustees, staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

5.2.4 Significant breaches of this policy will be handled under the Code of Conduct for volunteers or in the case of staff under the Disciplinary Procedure

## 5.3 Security

5.3.1 Any recorded information on the trustees, volunteers and staff will be:

- Kept in locked cabinets
- Protected by the use of passwords if kept on computer
- Destroyed confidentially if it is no longer needed

5.3.2 Access to information on the main database is controlled by a password and only those needing access are given the password. Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display. Notes regarding personal data of clients should be shredded or destroyed.

## 5.4 Data Storage and Recording

5.4.1 HWK has a database holding basic information about the trustees and volunteers and HWK activities. The back-ups of data are kept off site in a secure data center managed by Parkwood.

## 5.5 Access to Data

5.5.1 Individuals have the right to access information stored about them. Further information can be found in the Freedom of Information Policy and Procedure.

## **5.6 Transparency**

5.6.1 HWK is committed to ensuring that in principle Data Subjects are aware that their data is being processed and for what purpose it is being processed:

- What types of disclosure are likely
- How to exercise their rights in relation to the data

5.6.2 Data Subjects will generally be informed in the following ways:

- Trustees - in their induction
- Staff - in their Terms and Conditions
- Volunteers - in their induction
- Clients - when they request (on paper, on line or by phone)

5.6.3 Standard statements will be provided to staff for use on forms where data is collected.

5.6.4 Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

## **5.7 Consent**

5.7.1 Consent will normally not be sought for most processing of information about staff.

5.7.2 Information about volunteers will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

5.7.3 Information about trustees will only be made public with their consent (this includes photographs). 'Sensitive' data about trustees (including health information) will be held only with the knowledge and consent of the individual. Consent should be given in writing, although for some services it is not always practicable to do so. In these cases verbal consent will always be sought to the storing and processing of data. In all cases it will be documented on the database that consent has been given.

5.7.4 HWK acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where there is no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

## **5.8 Training**

5.8.1 All staff who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including this Confidentiality & Data Protection Policy. All staff will be expected to adhere to all these policies and procedures.

5.8.2 Confidentiality and Data Protection will be included in the induction training for trustees and active affiliates. HWK will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

## 6. Document Control

Title of Document: <b>Confidentiality &amp; Data Protection Policy &amp; Procedure</b>	
Board Approval Date: December 2015	Review Date: December 2016