HemingfordHub
Good neighbour scheme

HemingfordHub Confidentiality and Data Protection Policy 18.09.20

What information does HemingfordHub hold ?

- HemingfordHub needs to hold Information relating to its volunteers, and the people we help (our residents), to enable the Hub to offer appropriate services to our residents.
- We need to keep data relevant to our residents' needs which may include age, gender, ethnicity, disability, as well as name and contact details
- In addition we need to hold this data for the purposes of monitoring our equal opportunities policy and for measuring performance.

All volunteers and residents shall be informed that we need to hold information about them on a computer database and that they have the right to be provided with a printout of the data stored about them if they request it.

How we store and restrict access to information

- We will store data relating to volunteers and residents on the HH database. This information can only be accessed by the Working Group and our IT Support person. We will store the database (including a back-up) on a password-protected computer at all times, using Dropbox.
- If the Hub Working Group members need to use the database information they must make a copy of the information on their personal computer and delete the copy as soon as the task is complete.
- The Hub will hold all confidential data electronically; confidential data on paper shall be at a minimum. Any committee member holding paper copies of confidential data will destroy the information as soon as it is no longer required to deliver the Hub services to our residents.

Resident related information – PARTICULARLY IMPORTANT FOR Volunteers

- We will only discuss information that will identify a resident or a resident's affairs when necessary for the efficient delivery of Hub services.
- At no time will we discuss resident information with other residents, volunteers, friends or family without the resident's permission (See GDPR Permission Form). General gossip should be avoided at all times.
- The Hub Working Group may share information with each other and a Designated Safeguarding Person in order to discuss issues and seek advice. No GDPR Permission Form is required for this.
- Where the Hub has a legal duty to disclose information (for example, where abuse is suspected), the individual will be informed that disclosure has or will be made. No GDPR Permission Form is required for this.
- Any personal data held about a resident who stops receiving support permanently from the Hub will be deleted when all support finishes.

Volunteer Related Information

- If the HemingfordHub Working Group uses other members of the Hub to interview potential volunteers, these representatives will have access to Volunteer Application Forms at the time of the interview. Following these interviews any Volunteer Application forms will be forwarded to the Working Group and not held by the interviewer.
- The Hub will keep a record of the following information relating to a volunteer:
    - Application Form
    - References
    - Confidentiality and data protection agreement
    - Completion of Safeguarding training certificate
    - DBS date of issue, name of the subject, unique reference number of the Disclosure
    - Photograph for ID card
    - Confirmation of reading Hub Handbook and all attached policies
- Only the Hub Working Group will have access to volunteer related data including DBS information (In accordance with section 124 of the Police Act 1977**). Disclosure information shall only be used for the specific purpose for which it was requested and for which an applicant's full consent has been given.**
- We will delete all data relating to volunteers who have permanently resigned from the Hub
- If a Working Group member resigns they will no longer have access to Dropbox, the database and other Hub Committee papers. They should return all sensitive paperwork to the group.

Duty to disclose information

The Hub has a legal duty to disclose Abuse of Adults to the Social Services Department (following any notification of abuse (see HH Safeguarding Adults Policy).

Breach of confidentiality and Data Protection policy

HemingfordHub requires every volunteer to sign a Confidentiality and Data Protection Agreement indicating that they understand this Confidentiality and Data Protection Policy. Any committee member or volunteer who breaches any of the conditions within this policy will be dismissed from HemingfordHub.

The HemingfordHub Working Group will review this policy and related good practice annually.

Chairman's Signature: *Tish Peek*

Adopted by the HemingfordHub Working Group on: 23/02/2021 Latest Review Date: 23/02/2022