Confidentiality Policy

1. Overview

All persons contacting SHC have a reasonable right to assume that any disclosure of information they make will be treated in confidence within the organisation and will not be passed on without their consent. Any such disclosure, unless required by law, is a misuse and abuse of privacy. Personal information, in accordance with SHC's Privacy Policy, will only be shared with individuals whose role is appropriate.

As a volunteer (Project Team Member) at SHC you may have access to or be entrusted with information that SHC has deemed as confidential or should be considered as such through the good judgement of the individual. For example, you may collect email addresses for mailing list opt-ins or process photos where consent has been given. If you have any concerns regarding this matter, or the Confidentiality Policy in general speak to a Trustee.

Information acquired about individuals is particularly sensitive and has a higher confidentiality rating than other charity related issues.

2. Rights & responsibilities

The principles of confidentiality apply to all volunteers of SHC.

Everyone should read, understand and abide by our Data Protection Policy. In essence, people's information can only be used with their permission and for the purpose they provide their permission for.

However, information which contravenes the law or where people may be at risk will have to be passed on.

If you request it, you may have access to all records which name you. All volunteers have the right to receive ongoing support and supervision which is undertaken in confidence. Information which is subsequently divulged should be anonymous.

All volunteers are responsible for:

- Reading and abiding by this policy
- Declaring any conflict of interest between their role at SHC and their role in another capacity (as detailed in our Conflict of Interest policy)
- Respecting confidential agenda items in meetings
- Keeping minutes, records and other internal documents secure

3. Government Rules on Sharing Confidential Information

SHC will abide by the Government's seven golden rules to sharing information (see below)

The seven golden rules to sharing information (as per UK Government)

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up- to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

4. Use and Storage of Confidential Information

At SHC everyone must ensure that confidential information is dealt with appropriately and confidential discussions are held in closed rooms.

If you are working on confidential data (such as mailing lists) on screen and have to step away from your desk, you must lock the computer in your absence.

If you are working on hard copy of confidential documents and have to step away from your desk, you must lock away or cover the documents.

You must ensure that confidential information which is no longer required is shredded or deleted when no longer required.

5. Membership Records

Personal information should be kept in a locked cabinet with restricted access or in soft copy in folders which have restricted access.

Membership records will be kept for 6 months after the member leaves SHC and will then be destroyed.

NOTE: individual funding requirements may include asking for documents to be retained beyond the statutory minimums.

6. Monitoring

The effectiveness of this policy will be monitored on a regular basis by the Trustees through:

- Recording and reporting all complaints about breaches of confidentiality
- Addressing any issues of poor behaviour/performance
- Discussing such issues at team meetings

7. Breaches of Confidentiality

Any instance of breaching confidentiality by a volunteer will be investigated by the Trustees of SHC. If volunteers have any concerns regarding this speak to a Trustee.

Policy Review

This policy will be reviewed regularly to reflect best practice in response to changes in relevant legislation or an identified failing in the policy's effectiveness.

SHC Version 1.1, August 2019 - Date last Reviewed August 2019 – Next review date August 2020