Community Southwark

Sample Confidentiality Policy

Below is a simple template for a confidentiality policy: depending on your organisation you may want to flesh it out further – please see the resources at the end for more information.

***Please note**: This information is intended to offer assistance and provide information where appropriate and Community Southwark is not liable for action taken, or not taken, as a result of reading this guide.*

ORGANISATION Confidentiality Policy

1. General principles

1.1. ORGANISATION recognises that colleagues (employees, volunteers, trustees, secondees and students) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from your line manager.

1.2. Colleagues are able to share information with their line manager in order to discuss issues and seek advice.

1.3. Colleagues will avoid exchanging personal information or comments about individuals with whom they have a professional relationship.

1.4. Talking about the private life of a colleague is to be avoided at all times, unless the colleague in question has instigated the conversation.

1.5. Colleagues will avoid talking about organisations or individuals in social settings.

1.6. Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.

1.7. There may be circumstances where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. The organisation's consent must be sought before discussing the situation, unless the colleague is convinced beyond doubt that the organisation would not object to this. Alternatively, a discussion may take place with names or identifying information remaining confidential.

1.8. Where there is a legal duty on ORGANISATION to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

2. Why information is held

2.1. Most information held by ORGANISATION relates to individuals, voluntary and community organisations, self-help groups, volunteers, students, employees, trustees or services which support or fund them.

2.2. Information is kept to enable ORGANISATION colleagues to understand the history and activities of individuals or organisations in order to deliver the most appropriate services.

2.3. ORGANISATION has a role in putting people in touch with voluntary and community organisations and keeps contact details which are passed on to any enquirer, except where the group or organisation expressly requests that the details remain confidential.

2.4. Information about students is given to the training organisation and the college, but to no one else.

2.5. Information about ethnicity and disability of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

3. Access to information

3.1. Information is confidential to ORGANISATION as an organisation and may be passed to colleagues, line managers or trustees to ensure the best quality service for users.

3.2. Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.

3.3. Colleagues will not withhold information from their line manager unless it is purely personal.

3.4. Users may have sight of ORGANISATION records held in their name or that of their organisation. The request must be in writing to the Chief Officer giving 14 days' notice and be signed by the individual, or in the case of an organisation's records, by the Chair or Executive Officer. Sensitive information as outlined in para 3.2 will only be made available to the person or organisation named on the file.

3.5. Employees may have sight of their personnel records by giving 14 days' notice in writing to the Chief Officer.

3.6. When photocopying or working on confidential documents, colleagues must ensure people passing do not see them. This also applies to information on computer screens.

4. Storing information

4.1. General non-confidential information about organisations is kept in unlocked filing cabinets and in computer files with open access to all ORGANISATION colleagues.

4.2. Personnel information on employees, volunteers, students and other individuals working within ORGANISATION will be kept in lockable filing cabinets by line managers and will be accessible to the Chief Officer.

4.3. Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.

4.4. In an emergency situation, the Chief Officer may authorise access to files by other people.

5. Duty to disclose information

5.1. There is a legal duty to disclose some information including:

5.1.1. Child abuse will be reported to the Social Services Department

5.1.2. Drug trafficking, money laundering or acts of terrorism will be disclosed to the police.

5.2. In addition colleagues believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the Chief Officer who will report it to the appropriate authorities.

5.3. Users should be informed of this disclosure.

6. Disclosures

6.1 ORGANISATION complies fully with the DBS Code of practice (E File) regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

6.2 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a **criminal offence** to pass this information to anyone who is not entitled to receive it.

6.3 Documents will be kept for a year and then destroyed by secure means. Photocopies will not be kept. However, ORGANISATION may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

7. Data Protection Act

7.1. Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles.

These are that personal data must be:

- Obtained and processed fairly and lawfully.
- Held only for specified purposes.
- Adequate, relevant and not excessive.

- Accurate and up to date.
- Not kept longer than necessary.
- Processed in accordance with the Act.
- Kept secure and protected.
- Not transferred out of Europe.

8. Breach of confidentiality

8.1. Employees who are dissatisfied with the conduct or actions of other colleagues or ORGANISATION should raise this with their line manager using the grievance procedure, if necessary, and not discuss their dissatisfaction outside ORGANISATION

8.2. Colleagues accessing unauthorised files or breaching confidentially may face disciplinary action.

9. Whistle blowing

Where the Finance Worker has concerns about the use of ORGANISATION funds, he or she may refer directly to the Chair or Treasurer outside the usual grievance procedure.

All colleagues hold the right to inform either his or her manager or one of the trustees if they believe that ORGANISATION is being brought into disrepute by the actions of another colleague or trustee.

Resources

The following resources are useful in keeping your policies and procedures up-to-date:

- Acas: Privacy Policy
- Acas: Data Protection
- Gateshead Carers: Confidentiality Policy
- Gov.UK: Non-disclosure agreements
- Voluntary Action Islington: Policies, Resources & Toolkits

Support

If you would like any support with policies and procedures or any other issues facing your organisation, please contact the Development Team at Community Southwark: development@communitysouthwark.org.uk or 020 7358 7020.