Confidentiality Policy Template

1. General principles

1.1 (Name of 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 must exercise common sense and discretion in identifying whether this information should be communicated to others. Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

1.2 Confidential information includes anything that contains the means to identify a person, e.g. name, address, post code, date of birth, National Insurance Number, passport and bank details. It includes information about sexual life, beliefs, commission or alleged commission of offences and other sensitive personal information as defined by the Data Protection Act. It also includes information about organisations such as confidential business plans, financial information, contracts, trade secrets and procurement information

1.3 Colleagues should seek advice from their line manager about confidentiality and sharing information as necessary

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

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

1.6 Colleagues will avoid discussing confidential information about organisations or individuals in social settings.

1.7 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.

1.8 Where there is a statutory duty on (NAME OF ORGANISATION) to disclose information, the person or people involved will usually be informed that disclosure has or will be made unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation. Details about disclosure of information and who has been informed will always be kept on record and stored securely with restricted access.

1.9 Confidential information will be stored securely. It will not le left on desks but locked away. On computer it will be stored in password protected folders.

2. Why information is held

2.1. Most information held by (NAME OF 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 (NAME OF ORGANISATION) colleagues to understand the history and activities of individuals or organisations in order to deliver the most appropriate services.

2.3. (NAME OF 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 protected equality characteristics 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 (NAME OF ORGANISATION) as an organisation and may be passed to colleagues, line managers or trustees on a need to know basis 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 any 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 (NAME 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 should 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 (NAME OF ORGANISATION) colleagues.

4.2. Personnel information on employees, volunteers, students and other individuals working within (NAME OF 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 and vulnerable adult abuse will be reported to the relevant statutory services

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 unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation. Details about disclosure of information and who has been informed will always be kept on record and stored securely with restricted access

6. Disclosures

6.1. (Name of 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, (NAME OF ORGANISATION) will 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:

7.1.1. Obtained and processed fairly and lawfully.

7.1.2. Held only for specified lawful purposes.

7.1.3. Adequate, relevant and not excessive.

7.1.4. Accurate and where necessary kept up to date.

7.1.5. Not kept longer than necessary, for the purpose(s) it is used

7.1.6. Processed in accordance with the rights of the data subject under the Act.

7.1.7. Appropriate technical and organisational measures are to be taken to guard against loss or destruction of, or damage to, personal data

7.1.8. Not transferred to countries outside the European Economic Area without an adequate level of protection in place.

8. Breach of confidentiality

8.1. Misuse of personal data and security incidents must be reported to line managers so that steps can be taken to rectify the problem and ensure that the same problem does not occur again. This includes unauthorised access to person-identifiable information where a member of staff, or third party, does not have a need to know. It also includes incidents of information lying around in a public area, theft and loss of information

Date:

Date to be reviewed: