Data Protection and Confidentiality Policy

Reviewed: May 2015 Next Review: May 2017 Responsible: Trustee Board

Introduction

We're fully committed to complying with the requirements of the Data Protection Act 1998. We follow procedures that aim to ensure that all staff, volunteers, trustees, contractors, agents, consultants, partner organisations, and others acting on our behalf, who have access to any personal information held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under the Act.

We have to collect and use personal information about people with whom we work in order to operate efficiently. The information we collect and use may be about members of the public; service users; current, past and prospective staff; volunteers and trustees; or suppliers. The information must be handled and dealt with properly however it is collected, recorded and used, and must be done so in accordance with the safeguards set out within this policy and the Act. This applies to information recorded on paper, in computer records or recorded by any other means.

Staff, volunteers and trustees may also have access to confidential information about our partner organisations and about the internal business affairs of our organisation including: payroll data, contracts and tenders, and other information considered 'commercially sensitive'. Access to such information is on a 'need to know' and properly authorised basis. It must only be used for the purpose(s) for which it has been authorised.

We regard the lawful and correct treatment of personal and/or confidential information as very important to being successful in our operations and to maintaining confidence between the organisation and those with whom we work. We will ensure that we treat personal and/or confidential information lawfully and correctly.

Purpose

The policy sets out our commitment to and procedures for protecting personal information and for dealing with confidential information. The objectives of this policy are to:

- put in place effective controls and ensure appropriate records are kept
- meet our legal obligations under the Data Protection Act 1998 and other legislation
- prevent inappropriate use of information held by us
- prevent harm to individuals whose information is held by us
- meet our contractual obligations and the requirements of our funders
- demonstrate good data protection management, respect for confidentiality and meet relevant quality assurance systems

Scope
This policy applies to all our staff, volunteers and trustees. It also applies to all contractors, agents, consultants, partner organisations, and others acting on our behalf, who have access to any personal and/or confidential information held by or on behalf of the organisation.

We have a range of policies and procedures which deal with good practice standards and information processing which should be read in conjunction with this policy, including:

- Equal Opportunities and Diversity
- Financial Policy and Procedure
- Recruitment Policy
- Safeguarding Policy
- Whistleblowing

General principles
We recognise that we gain personal and/or confidential information about individuals and organisations during the course of our work. This may include dealing with information such as names/addresses/telephone numbers, information on the health and criminal records of service users, as well as being told or overhearing sensitive information about our work.

The Data Protection Act 1998 gives specific guidance on how this information should be dealt with. To comply with the law personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

Staff, volunteers and trustees should:

- assume that information is confidential unless they know that it is intended to be made public by Community Works, this includes passing information to another organisation
- exercise common sense and discretion in identifying whether information is expected to be confidential. In most cases information will not be explicitly stated as being confidential
- avoid exchanging personal or confidential information or comments (eg gossip) about individuals and organisations with which they have a professional relationship
- avoid talking about organisations or individuals in social settings
- not disclose to anyone, other than to colleagues, their line-manager, or the CEO, any information considered sensitive, personal, financial or private without the prior knowledge and consent of the individual or the organisation concerned
- share information sensitively if they need to discuss issues and seek advice with their line-manager and/or CEO only
- seek the consent of an individual or organisation before discussing difficult situations with other colleagues to gain a wider perspective on how to approach a problem, unless it is beyond doubt that the organisation would not object to this. Alternatively, a discussion may take place with names and identifying information anonymised. Where the situation may have legal implications for either the individual, organisation or for Community Works, you should have a confidential discussion with the CEO to ascertain the appropriate course of action and/or advice

- not compromise or seek to evade security measures designed to protect personal data and/or confidential information
- where we have a legal duty to disclose information, inform the person or organisation wo whom confidentiality is owed that disclose has or will be made
- note that their obligations to use and respect personal data and confidential information continues to apply after they have ceased working or volunteering for us

Legislation
Information about individuals (whether on paper, in computer records or recorded by any other means) falls within the scope of the Data Protection Act 1998 and must comply with the data protection principles.

The data protection principles are that anyone processing personal data (ie information about identifiable, living individuals) must ensure that personal data is:
- obtained and processed fairly and lawfully
- obtained and used only for specified purposes
- adequate, relevant and not excessive in relation to the purpose(s) for which it is kept
- accurate and, where necessary, kept up to date
- not to be kept for longer than is necessary
- processed in a way that respects the rights of data subjects
- kept secure and protected from unauthorised or unlawful processing, accidental loss or destruction, or damage

In addition, there are also special rules that apply to transfers abroad (including publication over the Internet).

Staff, volunteers and trustees who process or use any personal data in the course of their duties must ensure that these principles are followed at all times.

Members of the public may request certain information from a public sector agency under the Freedom of Information Act 2000. The Act does not apply to us as we are not a public sector agency. However, given that we undertake the delivery of services under contracts with public sector agencies, we may be required to assist that agency to meet a Freedom of Information Act request where we hold information on their behalf.

Responsibilities
All staff, volunteers and trustees, along with contractors, agents, consultants, partner organisations, and others acting on our behalf are to be made fully aware of this Policy and of their duties, responsibilities and contractual obligations under the Act.

All staff, volunteers and trustees will be required to sign a Confidentiality Statement before commencing work or volunteering with us.

Specific responsibilities
In relation to data protection and confidentiality issues, specific responsibilities also include:

The Trustee Board will act as the 'Data Controller' and is the 'person' legally responsible for complying with the Data Protection Act. The Trustee Board will determine the policy, taking into account legal requirements, and ensure that it is properly implemented and adequately resourced. The Trustee Board will designate lead responsibility for data protection in the organisation to the Central Services Manager.

The role of 'Data Protection Officer' is delegated to the Central Services Manager, who will be responsible for ensuring that this policy is implemented. The 'Data Protection Officer' will also have overall responsibility for:

- undertaking risk assessments and taking steps to ensure that risks are mitigated, reporting to the CEO and/or Trustee Board as necessary
- the provision of data protection training for all staff and volunteers
- the development of practice guidelines and procedures
- advising other staff and volunteers on difficult or uncertain data protection issues
- developing information sharing protocols between the organisation and its contractors, agents, consultants, partner organisations, and others acting on our behalf.

The CEO will exercise control over the following matters, in consultation and/or with the assistance of the Central Services Manager:

- handling subject access requests
- handing Freedom of Information Act requests
- approving requests for the transfer of data to other agencies (where established procedures are not in place)
- approving unusual or controversial disclosures of personal information
- approving information sharing protocols and contracts with data processors
- carrying out compliance checks to ensure adherence to the Act and this policy

Personal data

The Data Protection Act 1998 makes a distinction between personal data and 'sensitive' personal data. Personal data is defined as data relating to a living individual who can be identified from the data held and other information which is in the possession of the data controller. This includes any expression of opinion about the individual and any indication of intentions in respect of the individual.

We usually obtain, hold and process the following personal data in respect of individuals:

- names
- addresses
- telephone numbers
- email addresses

We may obtain, hold and process any sensitive personal data in respect of individuals for specific purposes, dependant upon the area of work. Sensitive personal data is defined as personal data consisting of information as to their:

- racial or ethnic origin
- political opinion

- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexuality
- criminal proceedings or convictions

This data is obtained, stored and processed solely to assist staff in the efficient running of a service requested by the service user or to verify a service user's access to services (eg to a funder). Personal data supplied by service users is not used to send marketing material or newsletters unless permission has been granted to do so, by the service user.

Handling personal and sensitive information
We will, through appropriate management and the use of controls:

- provide and implement a Code of Practice on Data Protection and Confidentiality (as attached to this Policy)
- fully observe conditions regarding the fair collection and use of personal information
- meet our legal obligations to specify the purpose for which information is used
- collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of information used
- apply checks to determine the length of time information is held
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the people about whom the information is held can fully exercise the right to:
    - be informed that processing is being undertaken
    - have access to one's personal information within the statutory 40 days
    - prevent processing in certain circumstances
    - correct, rectify, block or erase information regarded as wrong information.

In addition, we will ensure that:
- everyone managing and handling personal information understands that they are responsible for following good data protection practice
- everyone managing and handling personal information is appropriately trained to do so, and supervised
- procedures are in place to respond to anyone wanting to make enquiries about handling personal information
- queries about handling personal information are promptly and courteously dealt with
- performance in handling personal information is regularly reviewed and evaluated
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing

All staff, volunteers and trustees within the organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- paper files and other records or documents containing personal/sensitive data are kept in a secure environment
- personal data held on computers and computer systems is protected by the use of secure passwords, agreed with the Central Services Manager;
- contractors, agents, consultants, partner organisations and others acting on our are made aware of this Policy and follow defined procedures to comply with their responsibilities under the Act

All contractors, agents, consultants, partner organisations and others acting on our behalf will be made aware of this Policy and are required to follow defined procedures to comply with their responsibilities under the Act. Any breach of the Act will be deemed as being a breach of any contract between the organisation and that individual, company, partner or firm.

Independent contractors will indemnify us against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by us will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the organisation.

Monitoring and review

This policy takes account of the Data Protection Act 1998 and other guidance available **from** relevant agencies.

Day to day responsibility for ensuring that the organisation keeps up-to-date with data protection issues and for compliance with this policy rests with the Central Services Manager, who can also advise colleagues on any aspect of this policy.

The effectiveness of this policy, and its procedures, will be monitored and amended as and when necessary. The CEO may make minor changes to this policy as required. Significant changes will require the approval of the Trustee Board. The policy will also be reviewed every two years as part of a continuing review of organisational policies.

Data protection and confidentiality code of practice

We also have a data protection and confidentiality code of practice which all our staff and trustees follow. However, due to the content of the code of practice being confidential we cannot make it publically available.