Data & Information Protection Policy

OnThisROC

BUILDING COMMUNITY
ON A FIRM FOUNDATION

June 2015

1. General principles

1.1. OnThisROC recognises that OnThisROC employees, volunteers, trustees, secondees and students use information about individuals and organisations during the course of their work or activities. In most cases information will not be stated as confidential and it will be necessary to use common sense and discretion in deciding whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from OnThisROC.

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

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

1.4. It is not appropriate to discuss a person's sexuality without their prior consent.

1.5. Colleagues should 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. If it is necessary 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 personal information enters into the discussion, unless it is 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 OnThisROC 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 OnThisROC relates to organisations or individuals which support or fund them etc.

2.2. OnThisROC 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.

2.3. Information about volunteers is given to known groups or statutory agencies which request volunteers, but is not disclosed to anyone else.

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 OnThisROC 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 OnThisROC records held in their name or that of their organisation. The request must be in writing to the Director 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 paragraph 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 Director.

3.6. When photocopying or working on confidential documents, colleagues must ensure they are not accidentally seen by others. 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 with open access to all OnThisROC colleagues.

4.2. Information about volunteers, students and other individuals will be kept in filing cabinets by the colleague directly responsible. These colleagues must ensure line managers know how to gain access.

4.3. Employees' personnel information will be kept in lockable filing cabinets by line managers and will be accessible to the Director.

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

4.5. In an emergency situation, the Director 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, acts of terrorism or treason will be disclosed to the police.

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

5.3. Users should be informed of this disclosure.

6. Disclosures

6.1 When dealing with Disclosures and Disclosure information OnThisROC complies fully with the CRBS Code of practice.

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 criminal offence criminal offence 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, OnThisROC 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. OTR needs to collect and use certain types of information about citizens and other individuals who come into contact with OTR. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 1998.

7.2. OTR regards the lawful and correct treatment of personal information as very important and therefore ensures that personal information is treated lawfully and correctly. To this end OTR fully endorses and adheres to the Principles of Data Protection, as detailed in the Data Protection Act 1998. Specifically, the Principles require that personal information:

7.2.1. shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

7.2.2. shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;

7.2.3 shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

7.2.4. shall be accurate and, where necessary, kept up to date;

7.2.5. shall not be kept for longer than is necessary for that purpose or those purposes;

7.2.6. shall be processed in accordance with the rights of data subjects under the Act;

7.2.7. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

7.2.8. shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level

of protection for the rights and freedoms of data subjects in relation to the processing of personal data

7.3. OTR will, through appropriate management, strict application of criteria and controls

7.3.1. Observe fully conditions regarding the fair collection and use of information.

7.3.2. Meet its legal obligations to specify the purposes for which information is used.

7.3.3. 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.

7.3.4. Ensure the quality of information used.

7.3.5. Apply strict checks to determine the length of time information is held,

7.3.6 Ensure that the rights of people about whom information is held, can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information).

7.3.7. Take appropriate technical and organisational security measures to safeguard personal information.

7.3.8. Ensure that personal information is not transferred abroad without suitable safeguards.

7.3.9. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

7.3.10. Set out clear procedures for responding to requests for information.

7.4 In addition, OTR will ensure that:

7.4.1. There is someone with specific responsibility for Data Protection.

7.4.2. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.

7.4.3. Everyone managing and handling personal information is appropriately trained to do so.

7.4.4. Everyone managing and handling personal information is appropriately supervised.

7.4.5. Anybody wanting to make enquiries about handling personal information knows what to do.

7.4.6. Queries about handling personal information are promptly and courteously dealt with.

7.4.7. Methods of handling personal information are clearly described.

7.4.8. A regular review and audit is made of the way personal information is held, managed and used.

7.4.9. Methods of handling personal information are regularly assessed and evaluated.

7.4.10. Performance with handling personal information is regularly assessed and evaluated.

7.4.11. A breach of the rules and procedures identified in this policy by a member of staff may lead to disciplinary action being taken.

7.4.12. A breach of the rules and procedures identified in this policy by a Member is a potential breach of the Code of Conduct.

7.5. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

8. Acceptable use of ICT equipment

8.1. Use of the ICT equipment by employees of OnThisROC is permitted and encouraged where such use supports the goals and objectives of the business. However, OnThisROC has a policy for the use of the ICT equipment whereby employees must ensure that they:

8.1.1. comply with current legislation

8.1.2. use the internet in an acceptable way

8.1.3. do not create unnecessary business risk to the company by their misuse of the internet or other ICT equipment

8.2 Unacceptable behaviour - In particular the following is deemed unacceptable use or behaviour by employees:

8.2.1. visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material

8.2.2. using the computer to perpetrate any form of fraud, or software, film or music piracy

8.2.3. using the internet to send offensive or harassing material to other users

8.2.4. downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence hacking into unauthorised areas

8.2.5. publishing defamatory and/or knowingly false material about OnThisROC, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format

8.2.6. revealing confidential information about OnThisROC in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions

8.2.7. undertaking deliberate activities that waste staff effort or networked resources

8.2.8. introducing any form of malicious software into the corporate network

9. Company-owned information held on third-party websites

9.1. If you produce, collect and/or process business-related information in the course of your work, the information remains the property of OnThisROC. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

10. Monitoring

10.1. OnThisROC accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

10.2. All of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

11. Sanctions

11.1. Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

12. Agreement

12.1. All company employees, contractors or temporary staff who have been granted the right to use the company's internet access are required to sign a copy of this agreement confirming their understanding and acceptance of this policy.

13. Breach of confidentiality

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

13.2. Colleagues accessing unauthorised files or breaching confidentially may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

14. Whistle blowing

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