Policy Owner: Data Protection Officer	
Version: 4.00	**Relevant to:** All ONSIDE Staff, Volunteers, and data concerning service users.
Approval Date: 31.07.2026	**Approved By:** Director of People
Date Effective From: 01.08.2026	**Next Review Date:** 01.08.2028
Related Policies: SFROM03 - Privacy Policy SFRSD18 - Adults Safeguarding SFRSD14 - Children's Safeguarding	
Resources: https://www.gov.uk/data-protection	
Policy Amendments/Updates: Clarity on third party confidentiality	

Data Protection and Confidentiality Policy

1. General Policy Statement

1.1 ONSIDE is fully committed to compliance with the requirements of the Data Protection Act 2018 and UK General Data Protection Regulation (UKGDPR). The organisation will therefore follow procedures that aim to ensure that all ONSIDE representatives which includes and is not limited to, employees, volunteers and trustees; along with contractors, agents, consultants, partners or others acting on its behalf; who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under this policy and code of practice.

1.2 In order to operate efficiently, ONSIDE has to collect and use information about people with whom it works. These may include members of the public; service users; current, past and prospective employees, volunteers and trustees; freelance workers; student placements and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used; whether it is on paper, in computer records or recorded by any other means; in accordance with the safeguards set out within this policy and the Act.

1.3 ONSIDE representatives may also have access to confidential information about the organisations with which ONSIDE works and the internal business affairs of ONSIDE,

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.

1.4 ONSIDE regards the lawful, responsible, and correct treatment of personal and/or confidential information as very important to its successful operation and to maintaining confidence between the organisation and those with whom it works. ONSIDE will also ensure that it treats personal and confidential information lawfully and correctly.

2. Purpose

2.1 The purpose of this policy is to set out the organisation's commitment and procedures for protecting personal data and dealing with confidential information held by the organisation.

2.2 The objectives of this policy are to:

- Put in place effective controls and ensure appropriate records are kept.
- Meet its legal obligations under UK General Data Protection Regulation and other appropriate legislation.
- Prevent inappropriate use of data held and harm to individuals whose data is held.
- Meet its contractual obligations and the requirements of funders.
- Demonstrate good data protection management, respect for confidentiality, and meet relevant quality assurance systems.

3. Scope

3.1 This policy applies to all ONSIDE representatives. It also applies to all contractors, agents, consultants, partners, or others acting on its behalf, who have access to any personal data or confidential information held by or on behalf of the organisation.

3.2 ONSIDE has a range of policies and procedures, which deal with good practice standards and information processing; these include:

- Equality and Diversity
- Governance
- Financial Controls
- Safe Recruitment
- Safeguarding
- Whistle Blowing

3.3 This policy needs to be read in conjunction with these other policies. ONSIDE representatives are encouraged to use the provisions of these policies and procedures when appropriate.

4. General Principals

4.1 ONSIDE recognises that its representatives gain information about individuals and organisations during the course of their work. This may involve dealing with information such as names/addresses/telephone numbers and, in certain areas of work, information on the health and criminal records of service users; as well as being told or overhearing other sensitive information about the work of ONSIDE.

4.2 UKGDPR gives specific guidance on how this information should be dealt with by organisations. In essence, to comply with the law, personal information must be collected, used fairly, stored securely, not disclosed to any other person unlawfully and then disposed of securely.

4.3 ONSIDE representatives must assume that information is confidential unless they know that it is intended to be made public by ONSIDE; this includes passing information to another organisation. In most cases information will not be stated as confidential and ONSIDE representatives will have to exercise common sense and discretion in identifying whether information is expected to be confidential. Where uncertain, advice should be sought from the line manager.

4.4 ONSIDE representatives should avoid exchanging personal or confidential information or comments (gossip) about individuals and/or organisations with whom they have a professional relationship and should avoid talking about organisations or individuals in social settings.

4.5 ONSIDE representatives are able to share information with their line manager and/or Senior Leadership Team in order to share information, discuss issues and seek advice. In circumstances where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem, they should do so with names or identifying information remaining confidential. Where the circumstances have legal implications for either the organisation in question and/or for ONSIDE, employees should have a confidential discussion with the Senior Management Team to ascertain an appropriate course of action and/or advice.

4.6 ONSIDE representatives must not compromise or seek to evade security measures designed to protect personal and/or confidential information.

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

4.8 Any decision to override the duty of confidentiality and the rationale for this decision should be recorded by the data protection officer and stored securely and with limited access except where this relates to a criminal act or abuse of a child or vulnerable adult. In such cases information will be stored securely and with limited access in line with ONSIDE's risk management and safeguarding procedures. (See Section 12 Duty to Disclose Information).

4.9 ONSIDE representatives' obligations to use and respect personal and confidential information continue to apply after they have stopped working or volunteering for ONSIDE.

5. Legislation

5.1 Information about individuals; whether on paper, in computer records or recorded by any other means; falls within the scope of the UKGDPR and must comply with the data protection principles. Anyone processing personal data (i.e., information about identifiable, living individuals) must ensure that personal information is obtained and stored according to these principles:

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

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

5.2 ONSIDE representatives who process or use any personal information in the course of their duties must ensure that these principles are followed at all times.

5.3 Members of the public may request certain information from a public sector agency under the **Freedom of Information Act 2000**. The Act does not therefore apply to ONSIDE. 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.

6. Responsibilities

6.1 All ONSIDE representatives; along with contractors, agents, consultants, partners or others acting on behalf of ONSIDE are to be made fully aware of this Policy and of their duties, responsibilities and contractual obligations under the Act.

6.2 All ONSIDE representatives will be required to sign a Confidentiality Statement within employment contracts before commencing work with ONSIDE.

6.3 In relation to data protection and confidentiality issues, specific responsibilities are as follows:

6.4 **Chief Executive** - The Chief Executive will act as the 'Data Controller' and is the 'person' legally responsible for complying with the Data Protection Act. The Chief

Executive will designate lead responsibility for data protection in the organisation to the Head of Quality, Compliance & Business Development.

6.5 **Data Protection Officer** - The role of 'Data Protection Officer' is delegated to IG Health, 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 Senior Leadership Team and/or Trustee Board as necessary
- The provision of data protection training as required
- The development of practice guidelines and procedures
- Advising, in conjunction with the Head of Quality, Compliance & Business Development, other employees and volunteers on difficult or uncertain data protection issues
- Developing information sharing protocols between ONSIDE and its contractors, agents, consultants, partners, or others acting on its behalf.

6.6 – Head of Quality & Compliance -

The Head of Quality & Compliance will determine the policy, taking into account legal requirements, and ensure that it is properly implemented and adequately resourced. The Head of Quality& Compliance will also exercise control over the following matters, in consultation with the Chief Executive and/or with the assistance of the Data Protection Officer:

- Handling subject access requests
- Handling freedom of information act requests in line with section 5.3
- Approving requests for the transfer of data to other agencies (other than established procedures already approved)
- 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.

7. Personal Data

7.1 The Regulation makes a distinction between *personal data* and *"sensitive" personal data*.

7.2 **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.

7.3 ONSIDE usually obtains holds and processes the following personal data in respect of individuals:

- Names
- Addresses
- Telephone numbers

- Email addresses
- Financial circumstances
- Medical information
- Family circumstances

7.4 **Sensitive personal data** is defined by GDPR 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
- Sexual life
- Gender

7.5 ONSIDE may obtain, hold, and process any of the above sensitive personal data in respect of individuals for specific purposes, dependent upon the area of work.

7.6 This data is obtained, stored and processed solely to assist staff within the organisation in the efficient running of the service requested by the service user or to verify a service user's access to services (e.g. to a funder).

7.7 Personal data supplied by service users is not used to send marketing material or newsletters unless permission has been granted by the service user.

8. Handling Personal and Sensitive Information

8.1 ONSIDE will, through appropriate management and the use of controls:

- Provide and implement a Code of Practice on Data Protection and Confidentiality
- Fully observe conditions regarding the fair collection and use of personal information
- Meet its 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 of 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.

8.2 In addition, ONSIDE 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.

8.3 All ONSIDE representatives 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 or is stored on databases with limited access, agreed with IT specialists.
- Contractors, agents, consultants, partners, or others acting on behalf of ONSIDE are made aware of this policy and follow defined procedures to comply with their responsibilities under UKGDPR.

8.4 All contractors, agents, consultants, partners, or others acting on behalf of ONSIDE will be made aware of this Policy and required to follow defined procedures to comply with their responsibilities under UKGDPR. Any breach of UKGDPR will be deemed as being a breach of any contract between the organisation and that individual, company, partner or firm. Independent contractors will indemnify ONSIDE against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

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

9. Monitoring & Review

9.1 This policy takes account of UKGDPR and other guidance available from relevant agencies.

9.2 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 Data Protection Officer, who can also advise colleagues on any aspect of this policy.

9.3 The effectiveness of this policy, and its procedures, will be monitored and amended as and when necessary. The Head of Quality & Compliance may make minor changes to office procedures. Significant changes will require the approval of the Trustee Board. The policy will also be reviewed every three years; or following any significant change in legislation; or an investigation following non-compliance; and as part of a continuing review of organisational policies.

10. Document Status

10.1 This is a controlled document. Whilst this document may be printed, the electronic version saved on the SharePoint Drive and posted on the Intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Intranet.

Data Protection and Confidentiality Code of Practice

1. Introduction

1.1 ONSIDE is fully committed to compliance with the requirements of UKGDPR and has therefore developed a policy and this Code of Practice to ensure that all ONSIDE representatives; along with contractors, agents, consultants, partners or others acting on its behalf; who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under the Act.

2. Obtaining Personal Information by Consent

2.1 The purpose for which personal data is held varies with each area of work, each of which has clearly identified purposes related to every service user (see section 3).

2.2 When collecting personal data, it is important that we inform the data subject:

- Who is collecting the data (or on whose behalf it is being collected)
- What purpose(s) the data is being collected for
- Who the data might be passed on to (and who it will not be passed to)
- How to contact us if they want to stop us from using the data or to check what we are doing with it or to change what we use the data for (for example, opting in or out of mailings or other purposes).

2.3 People being asked to supply personal data must, where appropriate, be given options on how their data will be used. They must be given a choice over direct marketing and whether their information can appear on websites. It is important that we are clear about what choices are offered, record them carefully and ensure they are acted upon.

2.4 People may also be given options on what data they provide, for example through a statement about the optional nature of a question or a 'prefer not to say' tick box when asking whether someone has a disability.

2.5 Where a service user needs support to communicate, ONSIDE may use an appropriate third party such as a community language interpreter, British Sign Language interpreter, communication professional, or a family member or friend chosen by the service user. Before any personal or confidential information is shared in the presence of that third party, the service user must be told what information may need to be discussed, who will hear it, why the third party is being involved, and that the third party must treat the information as confidential. The service user's consent must be sought and recorded in the case record, including the name and role of the third party, the date consent was given, any limits placed on what may be shared, and whether consent was given verbally, in writing, or by another accessible method. If the service user does not consent, staff and volunteers must not use that third party unless there is a legal duty to disclose information or a safeguarding reason that justifies disclosure under this policy.

2.6 When a referral is made via a third party (for example: a relative or friend, another service user or a partner organisation), wherever practicable, contact must be made with the potential service user to ensure that permission has been granted to store and process their personal data.

2.7 To enable service users to understand how we use the information we collect from them; brief explanations are included in forms used to collect personal data and also in the ONSIDE and You agreement. Information on how we use information is also available on our website.

3. Working with People Who May Lack Capacity

3.1 When working with service users it may become apparent that they do not have sufficient understanding to provide consent to disclose or obtain confidential information about themselves. In those circumstances staff and volunteers must take steps they consider necessary in the best interests of that person and work within ONSIDE's Non-Instructed Advocacy guidance and framework. In arriving at this decision and determining what may be in the person's best interests a line manager should be consulted and they should ensure appropriate supervision and guidance is provided to the advocate. At all times accurate records should be kept of any determination to work within a non-instructed advocacy framework and actions taken.

In making a best interest decision the following factors should be taken into account:

3.1.1 The ascertainable past and present wishes and feeling of the person and the factors the person would consider if able to do so.

3.1.2 The need to permit and encourage the person to participate or to improve their ability to participate as fully as possible in decisions affecting them.

3.1.3 The view of other people who it is appropriate and practicable to consult about the persons wishes and feelings and what would be in their best interests.

3.1.4 Whether the purpose for which any action or decision is required can be as effectively achieved in a manner less restrictive of their freedom.

3.1.5 Staff and volunteers should be alert to differences of opinion between those consulted and the possibility of conflicts of interest between the service users and relatives, carers etc.

4. Information Held on Service Users for Specific Purposes

4.1 The purpose for which personal data is held varies with each area of work. Those purposes are reviewed and approved by the relevant line manager. Each area of work has clearly identified those purposes to every service user.

4.2 Most information relates to support being provided on a one-to-one basis to those using our services.

4.3 ONSIDE has a role in helping people to access a range of services and other agencies and keeps contact details which are passed on to any enquirer, except where the group or organisation expressly requests that the details remain confidential.

4.4 Information about organisations worked with (but not the detailed nature of the advice provided) may be passed to funders for the purposes of verifying work undertaken.

4.5 Information about the gender, age, ethnicity, disability, employment status, qualifications and lone parent status of service users is kept for the purposes of monitoring our Equality and Diversity Policy and may also be reported to funders.

4.6 Information relating to trainees/students on placement within ONSIDE and its enterprises in order to provide appropriate support and meet health and safety risk assessment requirements

5. Information Held on Employees, Volunteers and Trustees For Specific Purposes

5.1 Information relating to a prospective employee's, volunteer's or Trustee's home address, telephone numbers and email address, along with application forms, references and in some cases other details such as identification papers, qualifications, DBS checks and driving documents is held so that ONSIDE can assess the suitability of an applicant for a specified role; set up and maintain relevant personnel records; send written communications to a home address or contact them by telephone in connection with the organisation's recruitment and selection processes and, in the case of prospective employees, meet its obligations under employment law.

5.2 Information relating to an employee's, volunteer's or Trustee's home address, telephone numbers and email address is held so that ONSIDE can set up and maintain relevant personnel and training records, send written communications to a home address or contact them by telephone in connection with the organisation's business

activities and, in the case of employees, meet its obligations under employment law or, in the case of trustees, meet its obligations under company and/or charity law.

5.3 Information relating to an employee's or volunteer's home address, telephone numbers and those of designated contacts is held so that ONSIDE can make contact with them or some other designated person in the event of an emergency (for example changes to travel arrangements or closure of business premises). In the event of the employee or volunteer being taken ill, or involved in an accident or other emergency, there may be a need for the Senior Leadership Team or another member of staff to contact a friend or relative (a designated contact) of the employee or volunteer to inform them of the situation.

5.4 Where employees, volunteers or Trustees have designated responsibility for premises, information relating their home address and/or telephone numbers is held so that ONSIDE can make arrangements to contact them in the event of an 'out of hours' emergency (such as a break-in, fire or false alarm). This information is also made available to our alarm and cleaning services providers who will use it to contact designated individuals in the event of an emergency.

5.5 Information relating to an employee's or volunteer's home address, telephone numbers and email address is held so that colleagues can reasonably contact them at home in connection with work matters. Where a member of staff exercises an option to work at home, this data will be shared with colleagues but must not be given out to service users.

5.6 Information relating to an employee's home address, personal bank account, vehicle registration and National Insurance number is held so that ONSIDE can make arrangements to pay their salary and travel expenses. This information is also made available to our payroll services provider who will use it to make salary payments, provide the employee with a payslip and to meet HM Revenue & Customs regulations.

5.7 Information relating to an employee's name, the job they are undertaking, relevant experience for the job, relevant qualifications and professional memberships, and business contact details is held so that ONSIDE can release information to the public (for example business cards, emails, correspondence, organisational literature or on the website).

5.8 An employee's or volunteer's photograph is held, with their consent, so that ONSIDE can use it in reception, on its website, in organisational literature and on an identity card (in the case of an employee or volunteer meeting service users away from our main premises).

5.9 Information about the gender, age, ethnicity, disability and employment status of employees, volunteers and trustees is kept for the purposes of monitoring our equal opportunities policy and may also be reported to funders.

6. Access to Information and the Sharing of Personal Data

6.1 Work-related telephone numbers (including issued mobiles) and email addresses are freely available to all enquirers.

6.2 *Personal data*, which includes names and contact details, and *sensitive personal data* such as health and criminal records supplied by service users must only be shared within the organisation where necessary. *Sensitive personal data* should remain within the service area of work.

6.3 Only employees and volunteers within ONSIDE will normally have access to service users' personal data.

6.4 Personal, and especially sensitive, information should never be given to anyone outside of ONSIDE, including partner organisations, other service users, interpreters, communication support workers, family members, friends, or other people supporting communication, without explicit consent from the service user, employee, volunteer, or trustee unless there is a legal duty of disclosure under other legislation in which case a Director of ONSIDE will be consulted (see section 12). Where a third party is used to support communication, staff and volunteers must record who was present, why they were involved, what consent was given, and any limits on what information may be shared. Where colleagues believe that a user is at risk of harming themselves or others, this will be reported to ONSIDE's Safeguarding and Professional Guidance Manager and/or local authority in line with ONSIDE's safeguarding policies and procedures.

6.5 If information is issued without the necessary consent the data user must ask their line manager or the Data Protection Officer for advice.

7. Confidentiality

7.1 Where a third party is present to support communication, staff and volunteers must explain confidentiality in plain language before the discussion begins. Professional interpreters or communication professionals should be used where practicable and must be subject to an appropriate confidentiality obligation, either through their professional standards, contract, or service agreement. If the service user asks for a family member, friend, or other informal supporter to assist, staff and volunteers must explain that the person may hear personal or sensitive information, that they are expected to keep it confidential, and that ONSIDE cannot guarantee the same level of confidentiality as with a professional interpreter. The discussion, the explanation given, and the service user's consent must be recorded.

7.2 Where information is sensitive, such as where it involves disputes or legal issues, it will be confidential to the employee dealing with the case and their line manager and/or Senior Leadership Team. 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.

7.3 When printing, photocopying, or working on confidential documents, data users must ensure they are not seen by people in passing. This also applies to information on computer screens.

7.4 Personal contact details, such as home and mobile telephone numbers, and emergency contacts of employees, volunteers and Trustees are only made available to colleagues within ONSIDE with their explicit consent. Employees who elect to work from home must be prepared to be contacted at home by colleagues who will have access to their home and personal telephone numbers, email and home addresses. This information is strictly confidential and must not, under any circumstances, be passed on to anyone outside of the organisation (for example a service user or partner organisation).

7.5 This information will be stored in the Emergency Contacts database held on the restricted access HR System. In an emergency the senior member of staff present may access this information. The Director of People is responsible for keeping this information up-to-date and for reviewing it as appropriate.

7.6 All employees, volunteers and Trustees are made aware of the organisation's Confidentiality and Data Protection Policy and their obligation not to disclose personal data to anyone who is not authorised to have it. All employees, volunteers and Trustees will be required to sign a copy of the organisations Data Protection and Confidentiality policy to confirm they have understood and accepted the requirement to work within its framework at all times.

8. Requests to View Records

8.1 Individual service users may request and be supplied with a copy of any personal data held by ONSIDE. Ideally, requests should be made in writing, but they may also be made orally or through an accessible communication method. Where a service user uses an interpreter, communication professional, family member, friend, or other third party to make or understand a request, staff and volunteers must confirm and record the service user's consent for that person to assist and must only share information with the third party to the extent consented to or otherwise permitted under this policy. We have one calendar month to provide the information from when the request is received.

8.2 Organisations may have sight of ONSIDE's records held in the name of their organisation. The request must be in writing from the Chairperson or Chief Executive Officer of the organisation concerned. Sensitive information, as outlined in paragraph 6.1, will only be made available to the person or organisation named on the file.

8.3 Employees may request and have sight of their personnel records by submitting a subject access request.

9. Withholding Information from a Service User

9.1 There is a general duty to disclose to the service user complete details of all communications concerning them. However, there may be exceptional circumstances in which this would not be in the service users' best interests. Any decision to withhold information must be justifiable as being in the best interest of the service user. It should always be discussed with a line manager at the time of the decision or as soon after as possible. Any decision to withhold information must be justifiable on any of the following grounds:

9.1.1 Providing such information would have, or has the realistic potential to be detrimental to the physical or emotional wellbeing of the person concerned or

9.1.2 Providing such information would have, or have the realistic potential of being detrimental to the physical wellbeing of a third party or

9.1.3 Providing such information would or has the realistic potential if interfering with the fair and proper investigation or adjudication of an allegation or complaint.

9.2 The intention is to prevent serious harm or unjustified interference in to a proper investigation. It should not provide a rationale to deny service users access to information other than in highly exceptional circumstances.

9.3 At all times staff and volunteers should make every effort to ensure that third parties do not disclose information to them they do not wish to be disclosed to service users.

10. Accuracy and Longevity of Personal Information

10.1 When recording information in case records it is important that only relevant data is recorded and that, where possible, facts are checked with the individual, a colleague or through authoritative documents. Where opinions are recorded it is important to quote the evidence on which opinions are based or to make it clear that an assumption has been made (i.e. not a checked fact).

10.2 When recording personal information in service user, organisational or personnel records it is important to ask the right questions and to explain why data is required. Systems for recording data must facilitate accurate data entry and these systems need to be synchronised regularly (where it is unavoidable to have someone's records on different systems). Data subjects must also be given the opportunity to inform us of changes to, and to check and update, their records.

10.3 ONSIDE representatives must inform the Director of People of changes to their contact details so that personal data within their personnel record can be kept up to date, accurate and corrections made in a timely manner.

10.4 ONSIDE will take reasonable steps to keep all personal data held by the organisation up to date and accurate and to make corrections in a timely manner.

10.5 The personal data of service users in receipt of services will be retained for a period of seven years from the close of the funded project or last contact with service user.

This retention period is because much of this work is externally funded and may be subject to audit within that period.

10.6 Personal data relating to employees, volunteers and Trustees will be stored for as long as the individual is working for ONSIDE and for five years after they have left in the case of employees and two years in the case of volunteers and trustees. Once this period has elapsed, all personal data held by ONSIDE on the individual will be destroyed.

10.7 Personal data relating to unsuccessful job applicants will be destroyed 12 months after the relevant appointment is made.

11. Security and Storage of Personal and Confidential Information

11.1 General non-confidential information about organisations is kept in filing cabinets, on bookshelves and desks, or on the computer system with open access to all ONSIDE colleagues.

11.2 Personal information about service users, volunteers and other individuals is kept in lockable filing cabinets or desks or cupboards, or on the computer system by the employee or volunteer directly responsible. They must ensure that their line manager knows how to gain access.

11.3 In order to prevent unauthorised access and accidental loss or damage to personal information held on paper, employees and volunteers should take good care of files used in the course of their work. Where files containing personal data or confidential information are required to be used outside of the organisation's main premises, additional care must be taken to ensure that they are not left unattended, stolen or lost.

11.4 Financial information relating to the activities of ONSIDE is accessible by, and is confidential to, the Senior Leadership Team, the Director of Finance, the Trustees, the Treasurer, and the Auditor. Financial information required by employees for the purposes of ordering goods and services may be provided on the authority of their line manager. Financial information required by trustees for the purposes of overseeing the organisation's finances and for authorising expenditure may be provided by the Senior Leadership Team and Director of Finance. Financial information required by funders for the purposes of an application, tender, claim or audit may be provided on the authority of the Chief Executive.

11.5 Computerised records are maintained on a server at ONSIDE's main office. Where computerised records containing personal data are required to be kept on PCs or laptop computers for use outside of the organisation's main premises, access to computer records, networks and databases must be password protected. Employees and volunteers using laptop computers for such purposes must take additional care to ensure that equipment is not left unattended, stolen, or lost.

11.6 Personal data relating to ONSIDE representatives will be stored in paper filing systems and kept in a locked filing cabinet when not in use. Contact details and birthdays will also be kept as a computerised record, which is only available to other employees. Contact details for the Chief Executive may also be passed to and stored by Trustees.

11.7 Files containing confidential information should be labelled 'confidential'.

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

12. Duty to Disclose Information

12.1 There is a legal duty to disclose some information including:

- Child abuse and the abuse of vulnerable adults will be reported to the local authority Social Services Department and/or the police.
- Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.

12.2 In addition, colleagues believing an illegal act has taken place, must report this to a Director who will report it to the appropriate authorities. Colleagues believing that a user is at risk of harming themselves or others, would raise a safeguarding concern in line with ONSIDE's safeguarding policies and procedures.

12.3 Users should be informed of this disclosure. Unless to do so carries further risk.

13. Disclosures

13.1 ONSIDE complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

13.2 Documents will be kept for as long as the individual concerned is working at ONSIDE and then destroyed by secure means. Photocopies will not be kept. However, ONSIDE 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.

14. Unlawful Disclosure of personal Information

14.1 It is a criminal offence if anyone working for ONSIDE discloses personal information 'knowingly or recklessly' to anyone who is not supposed to have this information. ONSIDE representatives must therefore be careful if, for example, there are members of the public or staff from partner organisations in the office for any reason. They should also ensure that conversations are kept as private as possible and be aware that conversations containing personal or sensitive information may be overheard by people who should not have access to it.

15. Use of Photographs

15.1 When taking photographs at events, workshops or within other settings, ONSIDE will display a notice advising participants that photographs are being taken and that they should indicate to the photographer or the event organiser if they do not wish to be photographed.

15.2 Where practicable, ONSIDE will seek consent of service users before displaying photographs in which they appear. A form for obtaining permission for photographs to be published can be found on the office computer network. If consent is not possible (for example a large group photo) ONSIDE will remove any photograph if a service user or a relative/friend of the service user makes such a request. This policy also applies to photographs published on the internet.

16. Email Addresses

16.1 Outlook and Outlook Express address books are covered by the Act. Email addresses are not released without the addressee's permission. The 'BCC or blind carbon copy' facility is used for email addresses of recipients of group emails.

16.2 When forwarding emails, consideration should be given as to whether it is appropriate to share both content and contact details contained within the original message more widely with extended recipients.

17. Disposal of Personal and Confidential Information

17.1 ONSIDE representatives must be aware that names/addresses/telephone numbers and possibly details of an enquiry written on scrap paper are also considered to be confidential. Please ensure they are shredded before disposal. Similarly, information relating to financial transactions of the organisation is also considered to be confidential and should be shredded if no longer required.

18. Breach of Confidentiality

18.1 Employees who are dissatisfied with the conduct or actions of other colleagues or ONSIDE should raise this with their line manager and/or Senior Leadership Team using the grievance or whistle blowing procedure.

18.2 ONSIDE representatives accessing unauthorised files or breaching confidentially may face disciplinary action under the terms of the appropriate policy. Former employees breaching confidentiality may face legal action.

19. Further Information & Advice

19.1 ONSIDE representatives needing further information, advice, or training on any aspect of this Policy and Code of Practice should contact their line manager or the Head of Quality & Compliance, or the Data Protection Officer.