DATA PROTECTION POLICY

SAMARITANS OF EALING, HAMMERSMITH AND HOUNSLOW /
SAMARITANS EALING BRANCH

("Ealing Samaritans")

Date of adoption: 24th May 2017

Date of next review: May 2018

This policy is an internal document that should be drawn on in the event of queries from callers, volunteers or the Information Commissioner's Office.

This policy is subject to regular change and continuous review. There is a note on compliance at the end of the policy.

Introduction

1. Samaritans is committed to compliance with all relevant legislation in respect of personal data, and to protecting the rights and privacy of individuals whose information Samaritans collects in accordance with the Data Protection Act 1998 (DPA).

2. **This data protection policy applies to Samaritans of Ealing, Hammersmith and Hounslow**, **hereafter called 'Ealing Samaritans',** a branch of Samaritans providing confidential emotional support to people who are struggling to cope.

3. **Data protection is the responsibility of the Committee, which has appointed a volunteer as Data Protection Coordinator to make sure that the branch is and remains compliant.** This policy has been approved by the Committee and it will be reviewed at least annually, and whenever the branch changes the way it processes personal data.

4. **All volunteers are responsible for ensuring that this policy is observed.** If anyone considers that the policy has not been followed, they should raise this matter with the Data Protection Coordinator. The co-ordinator can be reached at dpo.ealingsams@gmail.com.

The Data Protection Act 1998

5. **The DPA established a framework of rights and duties** which are designed to safeguard personal data. It places legal obligations on organisations which handle personal data about individuals.

6. **The DPA applies to all electronic records, including CCTV images and also to some paper-based records** if they form part of a "relevant filing system". In practice this relates to filing systems which are organised in a manner where documents relating to a living individual can be found easily – for example where files are ordered by name and alphabetically.

Definitions used by Samaritans (drawn from the DPA where applicable)

Data Controller	Any person or organisation that makes decisions with regard to particular personal data including decisions regarding the purposes for, and the way in which, personal data is processed.
Data Subject	Any living individual who is the subject of personal information held by an organisation.
Personal Data	Data relating to a living individual can be identified from that data such as name, telephone number, email address. It also includes • Information that enables volunteers to "recognise" an individual such as accents, key phrases or situations. • Data that is likely to come into the possession of Samaritans. • Any expression of opinion about the individual or any indication of the intentions of Samaritans in respect of the individual.

Sensitive Personal Data	The DPA also classifies certain types of personal data as "sensitive". The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. Sensitive personal data is defined as personal data consisting of information as to: • Racial or ethnic origins • Political opinions • Religious beliefs or other beliefs of a similar nature • Trade Union membership • Physical or mental health or condition • Sexual life • The commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed
Data Processing	Processing, in relation to personal data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.
Subject Access Request	A request from a caller, volunteer, staff member, etc to see any personal data that the branch holds on him/her
Data Protection Co-ordinator	Volunteer appointed by the Committee to make sure that the branch is and remains compliant.

7. **Ealing Samaritans processes personal data relating to callers, volunteers, and donors**. Its procedures are designed to comply with the Data Protection Principles which can be found in Appendix A.

8. **Ealing Samaritans has audited its operations** and documented how each area is compliant with data protection legislation. All changes to services and processes are assessed for data protection implications. Where there is concern that the principles are not being complied with, this should be raised with the Data Protection Co-ordinator.

Registration with the Information Commissioner's Office

9. **Ealing Samaritans is an independent charitable organisation and is registered as a data controller** with the Information Commissioner's Office (ICO) as required by the DPA. This registration sets out the purposes for which Samaritans may process personal data.

Processing Caller Personal Data

10. **Ealing Samaritans provides confidential emotional support** for people who are struggling to cope primarily through a telephone support line, but also through email, SMS, face-to-face and outreach in the community.

11. **The branch processes personal data relating to callers, using an electronic call logging system and some strictly short-term paper records**, for the following purposes:

    - Providing statistical data
    - Providing ongoing support to callers
    - Third party referrals
    - Managing abuse of the service

12. **Our volunteers do not generally have sight of caller telephone numbers or email addresses**, although the central charity processes encrypted telephone data relating to callers, as well as caller email addresses and mobile numbers associated with the email and SMS services.

13. **Much of the data relating to callers that is processed by the branch is anonymous and not personal data as described by the Act**. However in the course of delivering the service volunteers collect certain caller data that enables individual callers to be "recognised" in a Samaritans context, even though the actual identity of the caller is not known. As decisions relating to caller support may be based on this "anonymous personal data",

Samaritans takes a cautious approach and implements data protection practices on the basis that the organisation as a whole is processing personal data.

Use of CCTV

14. **The branch has installed CCTV which does not record images.** The branch uses CCTV equipment to help ensure volunteer safety.

Processing Volunteer Data

15. **Ealing Samaritans processes personal data (in some cases sensitive personal data) about volunteers** for the following purposes:

    - Recruiting and selecting volunteers
    - Coordinating criminal record disclosures
    - Training volunteers
    - Volunteer management
    - Volunteer support
    - Volunteer communication
    - Volunteer expenses
    - Managing the Listener Scheme

16. **The branch uses the 3rings system to manage the rota and share information.** This includes volunteer contact details so that volunteers can communicate on branch matters such as swapping shifts. The system can be accessed remotely and each volunteer is allocated a user name and password which should not be shared with any other person. The branch is responsible for ensuring that volunteers are removed from the system when they leave the branch.

17. **Personal data relating to volunteers is not minuted in official records** such as minutes of committee, leader or Directorate meetings.

Processing Donor Data

18. **Ealing Samaritans processes personal data relating to donors** for the following purposes:

    - Recording gifts from donors to the branch
    - Recording direct debit details where appropriate
    - Processing gift aid declarations in relation to donations made to the branch

Legal Basis for Processing Personal Data

19. **Wherever possible Ealing Samaritans obtains consent to process personal data.** Where it is not possible to ask for consent, the branch relies on the condition that processing of personal data is necessary for the purposes of legitimate interests of Samaritans.

20. **Given the nature of the confidential emotional support service offered by Samaritans, volunteers are trained to assess and record the level of emotional distress and suicidal ideation of callers.** Volunteers may also process personal data relating to mental and/or physical health, sexual life and criminal activity. In the vast majority of cases this caller information will not be deemed to be "sensitive personal data" as defined by the DPA because it is not identifiable. However in some cases the information held is likely to be considered sensitive personal data because we are able to "recognise" the caller in a Samaritans' context. This is likely to be in relation to callers who use the service regularly.

21. **In a very small number of cases the data relating to callers may be identifiable.** This is usually where additional information has come into the possession of the branch.

22. **Wherever possible Ealing Samaritans obtains explicit consent to hold sensitive personal data. This may not be possible in relation to the support service**. In these cases Samaritans relies on the Confidential Counselling condition (as set out in paragraph 4 to the Schedule of the Data Protection (Processing of Sensitive Personal Data) Order 2000), which allows processing of sensitive personal data without explicit consent of the data subject as long as certain conditions are met.

Privacy Notices

23. **Ealing Samaritans ensures that all documentation used to collect personal data with regard to callers, volunteers, donors and staff meets the "fair collection" requirements of the DPA.** A privacy statement is available on Samaritans website (www.samaritans.org). This also explains our use of "cookies".

24. **Samaritans considers it to be impractical and potentially detrimental to callers to make a formal fair collection notice to callers to the emotional support service at point of access.** This is because callers are often in great distress when they first contact the service and it is inappropriate for volunteers to make such a statement at the beginning of contact. Nor does Samaritans consider the use of recorded messages in this context appropriate. It therefore relies on the privacy statement on the central charity's website to make callers aware of how Samaritans processes personal data.

Information Sharing

25. **In line with our policy on confidentiality, Samaritans does not share caller information with other organisations, other than in exceptional circumstances.** Exemptions to our confidentiality policy are clearly stated in our *Confidentiality Policy* on the central charity website.

26. **Ealing Samaritans shares information about callers with other branches in the London Region, with the Regional Caller Support Officer and the Organisation-wide Caller Support team.** From time to time the charity may share CCTV images of callers across the organisation. This is where there is a pattern of physical or verbal abuse or harassment of volunteers.

27. **Ealing Samaritans may in specific cases share volunteer personal data with the central charity** particularly in relation to the charity's *Volunteer Problem Solving and Safeguarding Procedures*.

28. **SamaritansNet (the organisation-wide intranet) is the major vehicle for sharing information about callers (including the caller support forum, caller support plans) and volunteers (branch directory).** It is hosted by the central charity and access is restricted to volunteers. Ealing Samaritans is responsible for ensuring that access to the intranet is suspended when volunteers leave the organisation.

29. **Ealing Samaritans has read and subscribes to the *Information Sharing Statement*** which sets out how information is shared across the organisation. The statement is hosted on this page: https://www.samaritansnet.org/pages/viewpage.action?pageId=62817797

Data Retention

30. Ealing Samaritans has established a *data retention schedule* (see Appendix B) which identifies retention periods for different categories of personal data held**.**

31. It has also set up a system for ensuring that the relevant retention limit is observed in practice, and for documenting and reviewing the retention policy. Personal data will be disposed of in a secure manner.

The Rights of Subject Access

32. Ealing Samaritans has a separate policy and procedure for *Dealing with Subject Access Requests* (see Appendix C). In summary:

    - Subject access requests must generally be put in writing
    - Data subjects must provide proof of identity including full name and postal address
    - A fee of £10 is charged
    - The response will be sent to the data subject by registered mail to a postal address within 40 days of receipt of the subject access.
    - Where the subject access request is from a caller, Samaritans will take steps to protect the anonymity of its volunteers except where there has been direct interaction between the volunteer and the caller. It will also ensure the confidentiality of other callers.

33. Where the subject access request is from a caller and involves contacts with a number of Samaritans branches, the branch will forward the subject access request to the Head of Planning & Governance at General Office immediately upon receipt.

Data Security

34. Due to the confidential nature of the service provided, Samaritans understands the need to keep personal data secure. As a result the charity has developed security measures which ensure that data is held securely. These are set out as Appendix D.

35. In most cases personal data should not be removed from the branch. In specific cases, permission must be obtained from the Director. Guidance on the importance of keeping personal data secure has been issued to volunteers.

36. One of the largest risks relating to data protection relates to the amount of personal data which is kept on volunteer laptops and computers and other electronic media. Samaritans has reviewed the ICO's guidance on *Bring Your Own Device* and issued guidance to all branch volunteers holding positions that involve processing personal data.

37. A copy of the *Computer Use Policy* is issued to each volunteer as part of the induction process. This is attached as Appendix E.

Training and Education

38. **Ealing Samaritans is responsible for ensuring that all volunteers are trained in and understand the basic principles of data protection.** Separate guidance is issued to branch volunteers holding key roles within the branch.

Appendices

Appendix A: The Eight Data Protection Principles

Appendix B: Data Retention Schedule

Appendix C: Subject Access Request Procedures

Appendix D: Branch Security Measures

Appendix E: Use of Branch Computer Policy

Appendix A: The Eight Data Protection Principles

The DPA establishes eight data protection principles which govern the processing of personal data. These state that personal data must be:

1. Processed fairly and lawfully
2. Obtained for one or more specified and lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Not kept for longer than is necessary
6. Processed in accordance with the rights of data subjects
7. Kept securely
8. Not transferred out of the European Economic Area without adequate protection

Appendix B - Data Retention Policy

One of the key principles of the Data Protection Act 1998 is that Personal Data[1] shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. As such, personal data should only be stored for as long as is necessary for the purposes for which it is held.

Samaritans Central Office has key responsibilities regarding breaches of data security and Subject Access Requests[2]. Samaritans Central Charity branches can play their part in enabling the SCC to remain compliant by adhering to the data retention periods summarised below. It is also recommended that affiliate branches adhere to these timescales in order to carry out best practice.

It's still important to remember that you can only use the data for the purpose that it was collected for regardless of how long it is retained. For more guidance on managing personal data you can access branch data protection guidance and checklists on this section of the Branch Hub.

Volunteering: Recruitment and Training DDs

Data source	Basis for processing	Purpose of processing	Retention Period
Potential volunteer contact details and diversity details	Consent	Needed to register interest as volunteer Equal opportunities monitoring	6 months or until volunteer application form is completed whichever is sooner
Volunteer application form	Consent	Needed to enable branches to contact volunteers and support them in process of becoming a volunteer.	Application form should be destroyed if volunteer does not become a volunteer /is not selected/withdraws from selection

[1] Personal Data means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or likely to come into the possession of, the Data Controller (Samaritans)

[2] Individuals have a right to make Subject Access Requests in order to be provided with a copy of the information an organisation holds about them

			process Otherwise application form should be deleted once the volunteer leaves the branch.
Volunteer references	Consent	To assess suitability of candidate	Until a volunteer becomes a full member of the branch; Where a volunteer does not join the branch, documents should be shredded within 30 days of the decision being made
Criminal record checks (different procedures across the 5 jurisdictions)	Consent	To assess suitability of candidate	Branches keep record of volunteer name, date form submitted, date received from DBS, date renewal needed. Delete once volunteer leaves
Volunteer – Selection notes	Consent/Legitimate interests	To assess suitability to join SIT course	For volunteers that continue to SIT: keep until a volunteer becomes a full member of the branch For a volunteer that does not continue to SIT: securely dispose of 30 days after selection decision given to volunteer

Volunteer – SIT notes	Consent/Legitimate interests	To assess suitability to become a volunteer	Until a volunteer becomes a full member of the branch; For a volunteer who leaves before becoming a full member of the branch: keep for 1 month after date of leaving branch
Volunteer file front sheet	Consent/Legitimate interests	To enable branches to have a register of who volunteers at branch and contact details for them. Data is transferred from application form once Volunteer has commenced training.	If volunteer does not become a full member of branch or complete SIT then forms deleted after 1 month. For volunteers who do become full members then sheet is kept for duration of their volunteering and then should be destroyed once volunteer leaves.
Membership form	Legitimate interests	To have a record of volunteers who become full members of the branch	To be destroyed within 1 month of leaving

Branch Management

Data source	Basis for processing	Purpose of processing	Retention Period
Branch contact list [this may be within an electronic rota management package]	Legitimate interests	To enable branch to contact volunteers about shifts and other branch matters	Until the volunteer resigns; need to obtain further consent if branch wants to stay in touch with volunteer after they leave
Samaritans Accounts	Legitimate interests	To authenticate volunteers access rights to Samaritans systems	Samaritans Account should be disabled within 1 month of volunteer leaving the branch
Next of kin data	Legitimate interests/consent	For emergency purposes if a volunteer falls ill on shift	Until the volunteer resigns
Expense claim forms	Legitimate interests	Accounting requirements	Destroy after 7 years

Caller Information – DD CALLER CARE. The following contains examples of some of the most common reasons for processing caller data. A more complete list is at the bottom of appendix B.

Data source	Basis for processing	Purpose of processing	Retention Period
Basic data (elog)	Legitimate interests and confidential counselling	Provision of service and (anonymised) statistical information	Anonymised after 4 months
Volunteer concerns (elog for caller support)	Legitimate interests and confidential counselling	Provision of service	Anonymised after 4 months
Volunteer concerns (Branch monitoring caller characteristics for caller support	Legitimate interests and confidential counselling	Provision of service	Typically, 6-8 weeks based on branch's own assessment
Caller contact details (if assigned to group of branches)	Consent	Provision of service	Assigned group support is normally reviewed and rotated to a different group of branches after 12 weeks
Emergency call log forms	Legitimate interests	Providing statistical information on service?	Shred on inputting data onto elog
Notes from outreach work[3]	Consent?	Providing statistical information on service / To assist in developing caller support plan	On adding details to elog. If other requirements, in line with specific data protection assessment

[3] These notes should be anonymised where possible, but have been included in case it is absolutely necessary to take these details. In this instance a data protection assessment should be carried out

Supporter Information

Data source	Basis for processing	Purpose of processing	Retention Period
Donor details	Consent	To keep donor up to date with work Fundraising	Remove details on request of donor or when donation details are removed (see below)
Donation details	Legitimate interest	Accounting records	Destroy after 7 years

APPENDIX B CONT'D: DATA RETENTION SCHEDULE FOR CALLER SUPPORT DATA

Personal data set	Location	Maximum Retention Period (where branch is responsible)	Responsible for disposal	Who has access?	Remote Access	Can data be removed from office?	Notes
Green caller care book, including written notes to caller support team about caller concerns	Branch	3 months	Caller Support team	All volunteers on shift	No	No	Must be locked away when the branch is closed. Old pages must be shredded.
Electronic logs, including electronic flags to caller support team (We only use e-log, not our own logs)	E-logging	N/A	Caller Support team	All volunteers on shift plus additional access for CSDD & Teams and Director	No	No	Logged data is the responsibility of Samaritans Central Office.
Call backs book, signposting book	Branch	3 months	Caller support team	All volunteers	No	No	Books should be locked away when the branch is closed.
Caller support forums	Samsnet	N/A	Regional Caller support officer and GO	Caller Support volunteers (deputies and CS teams)plus Branch Director, RCSO, DRCSO, RD, RPSO, GO staff	Yes	N/A	Data should not be downloaded to home computers; Ideally data should not be printed out, access for meetings should be through laptops/tablets.
Caller contact details for follow up calls and 3rd party referrals (post-it notes in diary)	Branch	Destroyed as soon as actioned	Volunteers	All volunteers on shift	No	No	All post-it notes are put in the diary. Volunteers should check regularly that old post-its are destroyed.

Personal data set	Location	Maximum Retention Period (where branch is responsible)	Responsible for disposal	Who has access?	Remote Access	Can data be removed from office?	Notes
Caller emails	Central server; accessed in branch only	60 days	Caller support team destroy hard copy printout; Emails cleared from server after 30 days	Caller support reviews hard copy email responses GO can access emails via the server	No	No	Hard copies must be shredded. We would like to aim for 30 days in future.
Caller SMS	Central server; accessed in branch only	N/A	Texts cleared from server after 30 days	GO can access via the server	No	No	No print outs of SMS messages
SMS case notes	Central server	N/A	N/A	All volunteers	Case note editors only	No	Case notes are attached to caller ID rather than message ID. Case note editors are selected and trained to review and edit
Support Plans	Available on Samsnet; Hard copy in branch ("Pink folders")	3 months	Caller Support Team	All volunteers and various GO staff	Caller Support volunteers only	No	***RCSO's to specify what format data may be brought to caller support meetings*** We reprint every 3 months and shred old copies.

Personal data set	Location	Maximum Retention Period (where branch is responsible)	Responsible for disposal	Who has access?	Remote Access	Can data be removed from office?	Notes
Assigned callers	Branch	3 months	Caller Support Team	All Volunteers	No	No	**(Currently we don't have any assigned callers. When we do, we will liaise with RCSO)** Assigned support should be reviewed and rotated to a different group of branches after 24 weeks; the outgoing group should shred records once the RCSO has been updated.
Assignment of email and text callers	GO	The assignment is removed if there has been no contact for 3 months	GO	GO	Yes various GO staff and volunteers	No	**(Ditto)** Actioned by request from CSDD (via RCSO) for both assignment and removal of assignment.
No call back list	Available on Samsnet, hard copy in branch	3 months	Caller Support team	All Volunteers various GO staff	No	No	GO maintains and updates the list We print our list approximately every 3 months and destroy the old version.
Service withdrawn list	Available on Samsnet, hard copy in branch	3 months	Caller Support team responsible for destroying hard copies.				We print our list approximately every 3 months and destroy the old version.

Personal data set	Location	Maximum Retention Period (where branch is responsible)	Responsible for disposal	Who has access?	Remote Access	Can data be removed from office?	Notes
Hotlist	Available on Samsnet, hard copy in branch	3 months	Caller Support team responsible for destroying hard copies.	All Volunteers various GO staff	Yes	No	We print our list approximately every 3 months and destroy the old version.
List of Order Plans	Available on Samsnet, hard copy in branch	3 months	Caller Support team responsible for destroying hard copies.	All Volunteers and various GO staff	Yes	No	We print our list approximately every 3 months and destroy the old version.

Appendix C

Procedure for Dealing with Subject Access Requests

Under the Data Protection Act (DPA) any anyone can ask to see whatever data we have kept on them, at any time – this is known as a Subject Access Request (SAR). Requests may come from callers, volunteers (including potential volunteers, ex-volunteers, and Listeners), donors and staff.

The Samaritans Central Office (SCO) will handle the following Subject Access Requests:

- All requests addressed to an SCC branch
- Any request from a caller (requests from face to face callers will be considered on a case by case basis depending on whether the caller is also using other access channels and whether a support plan is in place for the caller)
- Requests from volunteers who are appealing a Problem Solving decision or a decision by the Safeguarding Referral Panel

The important part: What do I do if I am asked for a Subject Access Request?

- **If a phone caller makes a subject access request, first suggest that they put the request in writing to dataprotection@samaritans.org or to the Data Protection Officer, Samaritans, The Upper Mill, Kingston Road, Ewell, KT17 2AF.**
- **If the caller is unwilling to put a request in writing, they can call SCO on 020 8394 8322 and ask to speak to the Head of Risk & Compliance.**
- **If a caller is unwilling to call the SCO, you can take the details of the request and pass them on to the SCO using the branch hub service desk at this link https://servicedesk.samaritansnet.org/servicedesk/customer/portal/9/create/116 You will need to have a telephone number for the caller so that the SCO can contact them.**
- **If a request comes in by email or SMS service it counts as a written request. Acknowledge the request and offer support as appropriate. Following the call please raise an issue via the Branch Hub Risk & Data Protection Service Desk at this link https://servicedesk.samaritansnet.org/servicedesk/customer/portal/9/create/116 Include the caller ID, message ID and your branch.**

- **If (as an affiliate branch) we would like support in responding to a subject access request from volunteers (current, ex and potential), listeners or donors, we should raise an issue here https://servicedesk.samaritansnet.org/servicedesk/customer/portal/9/create/116**
- **Please be aware that support can only be provided if resource is available. Requests from face to face callers will be reviewed on a case by case basis depending on the factors involved.**

*** In addition to all the above, please let our Data Protection Officer know by email: dpo.ealingsams@gmail.com**

What happens next?

When it receives a subject access request, the SCO will advise any branches involved. This advice will include the name of the person making the request, the nature of the request and the deadline for responding. This information will be relayed by telephone to the branch director.

The SCO will take steps to verify the identity of the person making a subject access request (data subject). Where the data subject is a face to face caller, volunteer, branch employee or branch donor, the SCO will contact the branch for help in this process. Where the request is from a caller, it may not be possible to validate the identity of the caller and in this case the caller will be informed that we cannot comply with the subject access request.

The branch will be asked to start a search for any documents that contain personal data relating to the data subject. In addition to formal files this will include a check of minutes of meetings and emails of any branch officers or other volunteers involved by the scope of the request.

Subject Access Requests from callers: the SCO has access to much of the caller data that is likely to exist – eLog, caller support forums, caller support plans, SMS case notes, etc. However the branch will be asked to check whether it has any additional data including volunteer comment books, CCTV images, etc.

Once we have had an opportunity to review all the documents submitted, we may contact the branch to clarify issues raised. For instance there may be reference to emails or documents that have not been provided.

Can the branch refuse to provide the data?

No. Under the law the Data Controller is required to respond to subject access requests and to explain what data is being processed and for what purpose.

There may be circumstances where we cannot identify the data subject from the information that has been given. In this case we still have to respond explaining the situation.

There are also cases where we might not disclose certain documents or we might provide them in a redacted format. For example if a third party refuses consent for their personal data to be disclosed as part of a response, we would consider whether it would be reasonable to override this refusal and provide the data in redacted form.

What will happen to the data the branch provides to the SCO?

A caller has the right to see the data held on them so you should assume that as long as it is possible to identify the caller from the data provided, the data will be passed on to the caller. You should therefore only pass on data that you are sure relates to the caller in question; if the caller has called anonymously or under a variety of names this should not be included; but you should advise the SCO that you believe this has happened.

If the identity of the caller is validated, the data provided will be redacted where it relates to other callers. In most cases we will also redact volunteer names. The exception to this would be where a volunteer has talked to the caller about the support provided by the branch. This is because the caller will know the name of the person they spoke to about their support and the content of the conversation. In this case the caller could reasonably expect to see full record of the contact.

Personal data identified as relating to a volunteer subject access request will be reviewed and an assessment will be made as to whether each document falls within the scope of the request. We will also consider whether the document contains personal data relating to any other volunteers.

What if the documents refer to third parties?

The document search will often include documents which contain third party information – this is particularly likely where the subject access request is from a volunteer. There may be complaints raised by other volunteers or other volunteers may have been interviewed as part of an investigation.

In each case the SCO will attempt to get consent from the third party for the document to be included in full. We will ask the branch for help in contacting any volunteers who are named in the disclosure and we will send a consent form to be signed and returned. Third parties may refuse consent, however the consent form makes it clear that there may be circumstances when refusal will be overridden.

Why would the SCO override refusal to consent?

In deciding whether to include a document that contains third party data we have to consider whether third party's right to privacy outweighs the data subject's right of access. This has to be considered on a case by case basis and the ICO guidance provides a framework to help organisations do this. Factors to be considered include:

- The expectation of confidentiality by the third party
- Whether it is possible to redact a document so that the identity of the third party is concealed
- Whether the information already known to the data subject
- Whether the views expressed by the third party had a material effect on the data subject.

The SCO would advise a third party if it decided to disclose personal data without their consent.

Will the SCO give the branch a copy of the data that is sent to the data subject?

We will not give the branch a copy of the full subject access request, but we will give you a copy of the accompanying letter. We will let the branch know in advance if we think that the subject access request has highlighted any issues that we think the branch should be aware of. We will also let the branch know if there are any follow up issues once the data subject has received the disclosure pack.

Is there anything I can do to prepare for a subject access request?

- Ensure that the branch is aware of the right of the caller to access their data
- Do not keep records you would not want a caller to see
- Regularly review records held, make sure they are up to date
- Maintain a data retention schedule and dispose of records in line with the schedule

APPENDIX D – BRANCH SECURITY MEASURES

The branch takes all reasonable steps to prevent unauthorised access to the premises and any personal data stored on the premises.

This includes:

Computer passwords, coded door entry passnumbers and keysafe passnumbers

We never share passwords/codes for branch-based systems or coded door entry with anyone outside the branch. If a volunteer believes that a password /code may have been compromised, they should change this immediately and inform the Branch Director.

Security Measures

- We secure personal data (paper files and computers) whenever the branch closes.
- We make sure that personal data is not accessible to anyone visiting the branch.
- We make sure that old files/care plans/log sheets are destroyed in a secure manner. As soon as personal data records are no longer required, we render them anonymous and/or shred them. We do not allow piles of shredding to build up.
- We determine what personal data (caller/volunteer/donor) can be taken out of the branch. If it is necessary to take personal data to meetings (whether hard or soft copies) for discussion purposes, we make sure that it is kept with us at all times. If the meeting room is vacated for breaks and confidential papers are left in the room, we ensure that the room is locked.
- We ensure that volunteers understand that branch computers should not be used for personal purposes and that no one should install software that has not been approved by the branch committee and the branch IT volunteer.
- The branch IT volunteer will make sure that firewalls and security software is up to date on branch computers.
- If we send emails to a number of recipients, we make sure that everyone on the list is happy for their email address to be visible; if necessary we use the blind copy function to maintain privacy.

- We do not leave laptops, memory sticks and other portable media unattended at any time. Where possible laptops and other mobile devices should be encrypted and password protected.
- We ensure that volunteers understand the importance of keeping data safe both inside and outside of the branch.

Locked filing cabinets

We keep files in a secure cabinet at the branch and access to this file should be restricted to the branch director and those nominated by the branch director.

We may keep some personal data on spreadsheets. These should only be on branch computers and must be password protected.

CCTV

We do not record CCTV images. Live CCTV images are used to help identify visitors in order to protect volunteer safety.

APPENDIX E – USE OF BRANCH COMPUTERS POLICY

1. **We don't use branch computers or printers for personal reasons.**
2. **Only designated IT volunteers can download or update software on branch computers.**
3. **We don't attach personal computers or devices to the branch wifi network or router without the permission of the Director.**
4. **We don't remove or access personal data without the permission of the Director:**
    a. Personal data will not be kept indefinitely at home and should be returned to the branch or safely destroyed once the use for it has expired
    b. Personal data will be stored securely when off the branch premises
    c. When attending meetings hard copies containing any caller data will be kept with you at all times and will be returned to the branch as soon as possible and not kept at home
    d. Volunteers will ensure that operating system, firewall and anti-virus software on home computers is up to date
    e. Volunteers will ensure that personal computers and mobile devices can only be accessed using a password and are configured to automatically lock after a period (e.g. 15 minutes) of inactivity.
    f. Personal data for callers or volunteers must not be held on mobile devices unless this has been approved by the branch. Any mobile devices used for the storage of personal data should be encrypted
    g. Any personal data that is downloaded to a personal computer or other mobile device is to be removed as soon as practical