

## AGE UK BROMLEY & GREENWICH

### PROCEDURES MANUAL

<b>BS EN ISO 9001 REFERENCE</b>	<b>:</b>	<b>505</b>
<b>TITLE</b>	<b>:</b>	<b>Confidentiality Policy &amp; Procedure</b>
<b>RESPONSIBILITY</b>	<b>:</b>	<b>Management Board, all Staff &amp; Time Bank Volunteers</b>
<b>SCOPE</b>	<b>:</b>	<b>Applies to all services and Activities. <u>This policy &amp; procedure should be implemented in conjunction with the Data Protection Act (DPA) Policy</u></b>

### PROCEDURES

This Confidentiality Policy has been drawn up to meet the needs of the organisation, its Management Board members, staff, Time Bank Volunteers and service users. Confidentiality should be maintained to protect all parties.

The object of the policy is to detail basic standards that Management Board members, staff and Time Bank Volunteers should adhere to and which are incorporated as part of normal working practice.

The most common situation, where issues of confidentiality may arise, will be matters relating to an individual user's personal problems. However, principles of confidentiality also relate to personnel records, addresses of Management Board Members, staff, Time Bank Volunteers and information concerning organisations within and outside Age UK Bromley & Greenwich, including Age UK Bromley & Greenwich itself. The policy is designed to cover all aspects.

Management Board members, staff and Time Bank Volunteers will be made aware of this policy when first joining the organisation and will be bound by it through the acceptance of the Terms and Conditions of Employment or the Time Bank Volunteers Record.

#### 1. Practical Aspects

##### 1.1. Information and Advice - Enquirers

Age UK Bromley & Greenwich offers to users a confidential, information and advice service. It is implicit therefore that such confidentiality is respected.

Information and advice inquiries should be referred to the Information and Advice Manager or Advice Desk. For clients unable to use the lift to access the office, the interview room off the main entrance may be used. Staff and Time Bank Volunteers working in other service areas should only give leaflets stocked by Age UK Bromley & Greenwich and information about organisations in Age UK Bromley & Greenwich's Annotated Guide to Services for Older People, or the Age UK Fact sheets

An enquirer's approach is to the organisation rather than to an individual employee or Time Bank Volunteer, discussion of information in order to serve best the needs of the user does not breach the policy if such discussion is with another member of staff/Time Bank Volunteers.

- 2.1 In no circumstances should details of a client be discussed by anyone outside the organisation in such a manner that it is possible to identify the client.

Client cases should only be discussed with your line manager or other senior colleagues and not discussed in general with other members of staff or Time Bank Volunteers.

- 2.2 Age UK Bromley & Greenwich aims to provide a service to users but a user may choose to waive confidentiality if it is in his/her own interest to do so, in which case there is no problem in passing on information to a third party. A Consent Form is used for this purpose.

Where a user requests that information is not divulged to a third party this wish should normally be respected (see Safeguarding Adult's Policy).

### **3. Procedures to be followed – All Services**

- 3.1 Any member of Staff/Time Bank Volunteer faced with a decision relating to confidentiality, must consult their line manager, informing them of the position, first advising the user that this action is necessary.

- 3.2 Under no circumstances should details, which enable an individual to be identified, be made public or passed to a third party without the user's informed consent in writing using the correct consent form.

Such consent is valid only for the purpose for which it was given. If information is to be re-used in a different context, permission should be sought again.

If an individual is not in a fit state mentally or physically to give permission it should be sought from their carer, relative or advocate and only with the consent of the Chief Executive or Deputy Chief Executive.

### **3.3 Person-centred care, support and treatment services:**

Age UK Bromley & Greenwich will ensure that all people using the service, and those lawfully acting on their behalf, have given consent before any, service, care or treatment is provided. The organisation must make sure that they obtain the consent lawfully and that the person who obtains the consent has the necessary knowledge and understanding of the care and/or treatment that they are asking consent for. Consent is an important aspect of providing care and treatment, but in some cases, acting strictly in accordance with consent will mean that some of the other regulations cannot be met. For example, this might apply with regard to nutrition and person-centred care. However, the organisation must not provide unsafe or inappropriate care just because someone has consented to care or treatment that would be unsafe.

The organisation must take into account people's capacity and ability to consent, and that either they, or a person lawfully acting on their behalf, must be involved in the planning, management and review of their care, support or treatment plans. The organisation must make sure that decisions are made by those with the legal authority or responsibility to do so, and must work within the requirements of the Mental Capacity Act 2005, which includes the duty to consult others such as carers, families and/or advocates where appropriate.

- Relevant person "relevant person" means the person using a service and/or any person who must be consulted when providing person-centred care to a person using a service. Where an adult who uses our services lacks the capacity to make a decision about their care, this would include any person acting lawfully on their behalf under the Mental Capacity Act 2005, such as with authority given by an advance decision to refuse treatment, Lasting Powers of Attorney for health and welfare containing the relevant clauses, or a Court appointed Deputy. Where a person using a service is subject to the Mental Health Act 1983, it would include any person with the authority to determine care. Where a person using a service is under 16 and not competent to make a decision about their care, this would include any person with parental responsibility or other legal authority (such as a local authority having a care order), or other recognised family member, carer or advocate.

#### **4. Enquiries involving Third Parties**

- 4.1 Correspondence from Age UK Bromley & Greenwich on behalf of a service user should make it clear that the reply will be shown to the user. In the event of a response being received from a third party, which would in the opinion of Age UK Bromley & Greenwich, damage relations or negotiations with the user, Age UK Bromley & Greenwich should check with the other agency that the answer could be shown to the user.
- 4.2 The situation often arises where an enquiry is made on behalf of someone else (third party), e.g. by a relative, friend, neighbour for an older person.

- 4.3 Confidentiality is not broken if information is given to be passed on, but whenever possible this should be backed up with a relevant leaflet, fact sheet or hand out, to ensure that the information ultimately received by the third party is accurate.
- 4.4 In cases where it would be helpful for Age UK Bromley & Greenwich to contact an outside agency, the third party should be telephoned for permission or written to before further action is taken. Without this permission there is a breach of confidentiality as action would be taken without the knowledge or consent of the third party and may not be in accordance with their wishes or in their best interests.
- 4.5 In cases where an enquirer acting on behalf of someone else is in possession of documents suggesting that he/she is acting with full knowledge and consent of the third party, great care should be taken and the employee/Time Bank Volunteer should consult the Chief Executive or Deputy Chief Executive if in any doubt that the confidentiality rule could be breached.

## **5. Keeping and Safeguarding Records**

- 5.1 Records relating to service users are only available to staff/Time Bank Volunteers who have undergone selection and training and only those who have - signed the statement on confidentiality.
- 5.2 Care must be taken at all times to ensure that all records are handled with discretion and are secured when the premises are not staffed. Correspondence and other records, minutes, files, card index systems pertaining to an individual or organisation should not be left on desks and notes should be shredded once case files/database records have been compiled.
- 5.3 All enquiry records should be kept in lockable cabinets with access limited to relevant staff.
- 5.4 Personal files for employees/Time Bank Volunteers should be stored in locked cabinets with access limited to relevant staff. In the case of employees, the Chief Executive should keep personal files.
- 5.5 Old records and files must be regularly monitored and information shredded when it is no longer necessary to keep it. Any files, papers, records containing names and addresses should, when no longer needed, be shredded.
- 5.6 The same principles should be applied to confidential information in memos, briefing papers and minutes of meetings.
- 5.7 Age UK Bromley & Greenwich is registered under the Data Protection Act and complies with the requirements. The act gives protection against possible

dangers arising from the use and storage of recorded information on computer or organised paper filing systems.

The Data Protection Act 1998 specifically states that, from 23<sup>rd</sup> October 2001, explicit consent must be obtained from a client to record 'sensitive' personal data. 'Sensitive' includes health; religious beliefs; race or ethnic origin, political opinions etc., and therefore applies to many Information and Advice cases. This means clients must sign a consent form.

*UK data protection law will change on 25 May 2018, when the new EU General Data Protection Regulation takes effect. Age UK Bromley & Greenwich will update this policy when more information becomes available - between now and 25 May 2018 - . See [Provisional publishing schedule: Employment for more information](#)*

See the Data Protection Act (DPA) Policy for more information on Compliance with the Act.

5.8 To protect the confidentiality of records held electronically, only authorised persons should access it. Computer screens should be locked when staff are away from their desk and passwords should not be shared with other staff members. Staff passwords are changed on a regular basis and known only by the staff member. The passwords must be at least 11 characters long and contain a mix of alphanumeric, capitals and special characters.

## **6. Use of the Telephone & Fax**

6.1 It is important that care should be taken over the use of the telephone. The 'hold' facility should be used at all times when conversation with a service user needs to be interrupted. Where two or more conversations are simultaneously taking place on telephones, staff/Time Bank Volunteers should be aware of the nature of these and ensure that confidentiality is not breached.

It should also be remembered that no personal caller should be able to hear (witness) a conversation with another service user. The interview room or another private area should be used for the appointment, or for callers to the office.

When calling a person back staff/Time Bank Volunteers should check that the person they want is the person they are speaking to before saying they are from Age UK Bromley & Greenwich.

6.2 Confidential information should not normally be sent by fax. If it is necessary to do so, the first page must indicate clearly that the material is confidential and who should receive it. Prior arrangements should be made with the recipient to ensure that confidentiality is not breached.

## **7 Guidance on sharing personal and confidential Information via email**

- 7.1 Your writing style should be courteous, business like and brief. Emails can be made available to the general public under Freedom of Information legislation (unless they contain personally identifiable information about service users). Service users could also request these under Access to Records policies.
- 7.2 When using email to send personal or sensitive information you have a duty of care to preserve the confidentiality of personal information. You are responsible for ensuring the information is communicated in a way which protects the privacy of the service user.
- 7.3 When using email you are expected to ensure that the intended recipient has a legitimate need to know the information and the identity of the person to whom it refers.
- 7.4 It is good practice when sending personal or confidential information via email to anonymise it, you should not put the person's name or reference number in the email title.
- 7.5 When titling the email mark it "Confidential- addressee only". You should make sure the email has been addressed only to the intended recipient, double check the address is correct before sending. Avoid use of the "reply all" option when responding to emails, especially when you need to send personal or confidential information. You may inadvertently send this to larger groups of people who may have no legitimate reason for accessing it. Check who was copied into the original email and delete the name of anyone who doesn't need to see the information you are replying with.
- 7.6 If forwarding on an email check the contents of the "email chain" within the body of the email, is there personal/confidential information which some of the recipients do not need to see? Delete anything which should not be shared.
- 7.7 If you wish to ensure the email has been received, you can choose to receive a delivery and/or read receipt for the email. You can do this when creating an email by going into "options" on the toolbar of a new email message.
- 7.8 Email systems should not be used as a permanent record store for significant documents and information. Emails that form part of a decision/audit trail or service user record should be archived to suitable electronic or physical places of storage. For example, you can copy and paste an email message and save it in a Word document in a folder on Charitylog or the clients' electronic file.

## **8 Sending documents securely via email**

When sending personal or confidential information via email you should put this into a Word document which you attach to your email rather than in the actual body of the email itself.

These are the instructions for creating a document in Word and password protecting it:

To password protect a Word document:

- ✓ From Word,
- ✓ Go to file
- ✓ from the Info toolbar go to Protect Document and from the drop down list select **encrypt with password**
- ✓ You will be prompted to type a password and to confirm the password – make a note of the password, otherwise you/the recipient will not be able to access the document.
- ✓ Go to File, Save as, and save the document
- ✓ In Outlook, go to the paperclip on the toolbar, it allows you to browse and insert your encrypted document into your mail message, and send it to the intended recipient.
- ✓ Send a separate email to the recipient with the password

## **9. Removal of Information from the Premises**

- 9.1 It is sometimes necessary for staff to carry with them on home visits or when attending meetings or case conference, information relating to individuals. Staff are expected to exercise due care and attention to ensure that such material is kept to a minimum, is safe and in their possession at all times. Particular care should be taken with diaries where appointments indicate the name and address of a service user. No such material/information should be left unattended in a vehicle.
- 9.2 If staff and volunteers have to take home with them information related to service users after home visits or outreach sessions, they must ensure that the information is kept in a locked filing cabinet/bag in a secured room. Age UK Bromley & Greenwich will ensure that all relevant staff and volunteers have access to lockable cabinets/bags at home, and if required the organisation will facilitate the purchase of appropriate lockable bags.
- 9.2 Papers relating to individuals must, when no longer needed, be returned to the office for shredding.

## **10. Information from Other Organisations**

- 10.1 Staff/Time Bank Volunteers may receive confidential or sensitive information relating to Age UK Organisations/Groups or other organisations. The same standards of confidentiality should be adhered to, as is the case with individuals approaching Age UK Bromley & Greenwich. Such information should only be divulged to a colleague or third party within the organisation, and never to anyone outside without consultation with the Chief Executive or Deputy Chief Executive.
- 10.2 When in doubt about how to handle any information received staff/Time Bank Volunteer should contact their line manager and inform them of the position.

## **11. Management Board Responsibilities**

- 11.1 Management Board members will be expected to make themselves aware of this policy.
- 11.2 In respect of confidential agenda items at meetings and confidential minutes, Board members will be expected to adhere to the policy and guard against any breaches intentional or unintentional.

Where there may be a conflict of interest between providers who are members of the Board, some matters will remain confidential and the procedure at meetings, may therefore exclude individuals who seem to 'have an interest'.

**All files will be destroyed after 6 years of discharge from the program, however there are exceptions to this rule, please see the Data Protection Act (DPA) Policy for more information on Compliance with the Data Protection Act 1998**