PRA BRANCHES DATA PROTECTION Dos and don'ts of looking after information

As a Trustee/Committee Member we all have a duty to ensure that any personal and sensitive information we hear or see is kept confidential, safe and secure. Personal data is anything from a persons name, address, email and phone number and sensitive data is about their health and family.

Getting this wrong can be distressing for the people whose information we have. It can also be unlawful, cost hundreds of thousands of pounds in fines and put you as an Trustee/Committee Member at risk of disciplinary action. This short checklist is aimed at helping you remember the important points when you handle information: -

Do:

- Do ensure that personal information is accurate and up to date and only keep it for as long as is necessary, for the purpose it was collected.
- Do review what you keep regularly to make sure it is still accurate, up to date and needed.
- Do ensure that anyone providing personal information understands what it will be used for through your privacy policy and data protection policy.
- Do avoid using any USB sticks or ensure to encrypt any information on a USB stick and delete it as soon as you have finished using it.
- Do dispose of personal/sensitive information on manual files or print outs as confidential waste.
- Do delete emails (including inbox, sent and deleted items), documents with personal information in them as soon as no longer needed. Do complete an annual review.
- Do check that computers and other equipment, including disks and memory sticks, do not have personal information on the hard drive before they are decommissioned
- Do remember that all personal information needs to be kept secure:
    - manual files must be securely locked up, not left on desks overnight.
    - ensure that any electronic files holding personal information are password protected.
    - computers should not be left logged on and unattended unless you have a password-protected screensaver.
    - comply with specific rules about security if you take personal information out of the office: it is your responsibility to make sure that it is kept safe and no one else can access it.

- Do be aware that the individual about whom the information relates has a right to see all the information that is held about them. Therefore inserting personal remarks/notes on files should be avoided, this includes emails.
- Do be aware that any breach of the provisions of the GDPR could attract personal criminal liability. This may arise if you knowingly or recklessly, obtain or disclose personal information to another source.
- Do pass all requests by individuals to see the information we hold on them to the Data Protection Officer/Branch Chairman ASAP as these are "Subject Access Requests".
- Do report any losses or potential losses of information to the Branch Chairman asap.
- All communications sent electronically which contains personal data, especially sensitive personal data should always be encrypted.
- Be safe; if you're not sure ask for advice.

Don't:

- Don’t use information for a different purpose than that for which it was obtained without the consent of the person who gave it or advice from Data Protection Advisor.
- Don’t disclose information to other family/friends/volunteers
- Don’t leave any personal identifying data, confidential information on printers, desks, computer screens.
- Don’t store or send personal data on removable media, such as a USB pen drive as these are easily lost or stolen.
- Don’t put information about individuals on the Internet, without written permission.
- Don’t write passwords down and ensure you change them at least every 60 days.
- Don’t send confidential communications by email if possible but at the very least such communications should be encrypted.
- Don’t ignore software security updates on devices. Failure to do so can leave devices open to hackers and cyber-theft.
- Don’t give out personal information over the phone or in person:
    - do not include any sensitive personal information in any email message.
    - do not forward email messages containing personal information without the sender’s consent.
- Don’t pass on personal data to a third party without consent.
- Don’t assume that data protection doesn’t matter – IT DOES.

Remember to keep all personal data secure, confidential and treat it as if it were your own. If you have any concerns or queries then contact the Data Protection Advisor for further guidance.