AMNESTY INTERNATIONAL UK SECTION

DATA PROTECTION GUIDANCE FOR GROUPS

DATA PROTECTION COMPLIANCE

Quick Check List

DO	DON'T
DO Ask someone for their consent before sharing their personal data with another organisation	DON'T Share someone's personal data with another organisation without explicit consent
DO Ask one person if you can forward their details to the other (or ask both in advance)	DON'T Copy two people into an email who do not already have each other's email addresses
DO Email your group putting everyone in the 'bcc' and then write in the body who the email has gone to eg all of your local group members	DON'T Email your group with email addresses in the 'to' or 'cc' fields
DO Make it clear in any statement if the personal data is staying with the group or being passed to an Amnesty UK office	DON'T Pass personal data to the Amnesty UK offices without consent
DO Ask everyone in your group who accesses or keeps personal data to read these guidelines and confirm they've read and understood them	DON'T Pass personal data to anyone in your group who has not be trained, or read and understood these guidelines
DO Ensure every device that you open or keep personal data on is password protected with a strong password, and documents are always filed away or shredded after use	DON'T Leave lists of data on the train, on a table in the pub or open on a screen for anyone to see. Or leave computer terminals unattended while logged in
DO Encrypt and password-protect any documents containing personal data and send the password in a different medium, eg text message	DON'T Email personal data in an open document
DO Check emails have the correct file and recipients before hitting send	DON'T Hit send on an email with an attachment without double-checking everything
DO Dispose of out-of-date personal data securely, eg shred them	DON'T Keep out-of-date paper or electronic records of personal data
DO Regularly review those who can access personal data on a cloud system and remove those who no longer need to access it	DON'T Store personal data in a cloud system without checking its security, adding a password and that only appropriate people can access it