Data Protection – Quick Guidance and Do's & Don'ts

This short guidance relates to how to treat people's personal data, whether a colleague, a member, a customer or any other person whose personal data we may process in our day-to-day jobs. Under data protection law, we have a number of obligations about this, and we must ensure we comply.

Colleagues should ensure they are familiar with other Society's policies and procedures in relation to the processing of people's personal data – these can be found on Colleagues Connect: https://colleaguesconnect.midcounties.coop/working-here/data-protection/.

1. Collecting, Storing and Disposing of Personal Data

1.1. We collect personal data from or members, colleagues, customers, third party partners, agency workers etc. because we need it in order to provide them with services, but we must ensure we let them know how, for how long and why their personal data will be processed.

1.2. All personal data we process must be **accurate and up to date**. Our databases, cabinets, folders and files should be regularly reviewed to ensure out-of-date information is either updated or deleted if we no longer need it.

1.3. Data should only be **held for as long as it is needed** for the purpose, we collected it. For example, if we collect customers' details to enter them in a competition, their data should be deleted once the competition is over. Equally, we collect personal data from members for the purpose of providing them with services in relation to their membership, but when they cancel their membership, we cannot retain their details forever. The point is, personal data cannot be kept "just in case" we may need it in future.

2. Keeping data secure and confidential

2.1. Personal data must be **kept secure at all times**. The table below gives a quick overview of important do's and don'ts about keeping data secure.

3. People's rights over their personal data

3.1. If you receive a request, either in writing or by telephone, about someone's personal data, for example a former colleague asking for copies of their past payroll and wage details; or a member asking for information relating to their share account, or bond; or a parent asking information about their children's

progress charts; **you must tell your DPCs immediately**, as we have a deadline to comply with such requests, which are known as **Subject Access Requests**.

3.2. Personal data of any individual should **never be disclosed to their friends or relatives (including a spouse)** without that individual's specific written consent.

3.3. Sometimes, instead of a Subject Access Request, you may receive a request from a public organisation or any authority, ie. the Police, HMRC, a City or County Council etc. asking us to disclose information relating to, for example, a colleague, a customer or a member. These requests are sometimes known as **official disclosure requests,** and you should immediately let your DPCs know so that the request can be dealt with timely and efficiently.

4. Data breaches

4.1. If you become aware of any personal data being used inappropriately, or simply something doesn't feel quite right about the way people's data is being processed, you must **immediately report your concerns to your business group's DPCs**, so that the incident can be dealt with timely and efficiently. Examples of personal data breaches include:

- access to someone's personal data by an unauthorised colleague, or third party working for us;
- sending personal data to an incorrect recipient;
- computers/laptops/mobile devices containing personal data being lost or stolen;
- amending personal data without permission;
- loss of availability (system failures, hacking etc.) of someone's personal data.

5. Communication by email

5.1. Chain emails should be avoided where possible. You should **always check before sending your email**, to ensure that:

a) all the people you are sending it to are relevant to the message
b) all email addresses are correct; and
c) you have deleted any unnecessary trail history eg. previous emails in the conversation.

REMEMBER! Chain emails are one of our biggest risks, as they can lead to inappropriate disclosure of people's personal data to unintended recipients.

6. Who to contact?

6.1. If you have any queries, please contact your business group's **Data Protection Champions ("DPCs")** – the contact list is available on Colleagues Connect: https://colleaguesconnect.midcounties.coop/working-here/data-protection/

6.2. Alternatively, you can contact the **Society's Data Protection Manager ("DPM")**[1] by telephone: 01926 516 064 or by email: data-protection@midcounties.coop

[1] For Healthcare, Energy and Phone Co-op: Data Protection Officer ("DPO").

version control: August 2020

DATA PROTECTION DO'S & DON'TS

- limit access to computers and files containing personal data strictly to those who need to know
- keep personal data stored on laptops and other portable devices to a minimum
- lock manual filing cabinets containing personal data and ensure only authorised personnel can access them
- ensure that personal data is always transmitted or transferred in a secure way (eg. password-protected, recorded delivery etc.)
- dispose of personal data securely, ie. by shredding, placing in confidential waste bags or securely deleting electronic files
- ensure personal data stored on portable devices such as laptops, mobile phones, memory sticks or tablets is kept secure at all times
- report data breaches (e.g. personal data is lost, stolen or disclosed to the wrong person) immediately
- keep passwords confidential and change them regularly. Sharing passwords is in breach of Society's policy.
- lock your computer screen if you leave your desk for any length of time

- leave personal data unattended e.g. on desks, fax machines, printers, in a vehicle, on a train etc.
- leave papers or electronic devices containing, or able to access, personal data, lying around unattended
- put papers containing personal data in regular paper baskets. Use appropriate disposal means
- send personal data to external third parties by email unless you have adequately protected it eg. with a password
- talk about confidential matters when others can hear you, for example on trains, or in coffee shops and airport lounges
- remove personal data from the office unless you are authorised to do so. The use of memory sticks and other memory devices is in breach of Society's policy (unless authorised by the Society's DPM)
- send people's personal data to your private email address to work from home – use appropriate tools (VPN, encrypted memory storage devices etc.) approved by the Society
- delay to report any loss or theft of electronic equipment, ie. laptops, mobile phones, tablets etc. or soft copies of documents containing personal data
- disclose your passwords or log in credentials to anyone – sharing this information is against Society's policy