**Information Management:**

**Working Away from the Office**

**Dos and Don’ts**

## Do:

Do keep information safe and secure at all times.

Do lock paperwork, computers and devices away when not in use.

Do ensure conversations discussing personal information are not overheard.

Do record what information you are removing from the office, and record when it is returned.

Do ensure your home Wi-Fi/network/devices are all secure, password protected with current antivirus.

Do swiftly report any known or suspected data breaches to line managers and [databreach@moray.gov.uk](mailto:databreach@moray.gov.uk).

Do remember that data subjects can request all information that identifies and relates to them; ensure that the personal information you keep is proportionate.

Do ensure you have completed mandatory Data Protection training on LearnPro(CLIVE).

Do remember it is the responsibility of all staff to ensure the safety and security of all personal information and devices in their charge.

## Don’t:

Don’t use personal email addresses or telephones for work purposes. If using a personal phone for work purposes cannot be helped then remember to withhold your number.

Don’t leave information on the kitchen table, car seat or anywhere it can be seen.

Don’t share information with those around you; brainstorming with others can be productive but ensure you don’t discuss confidential or personal information with unauthorised personnel.

Don’t input personal information in to websites that have not been through the Data Protection Impact Assessment (DPIA) process.

Don’t put paperwork with personal or confidential information on into your home recycling.

Don’t use work equipment for personal use, including accessing personal emails or social media accounts.

Don’t store information where it is not secure, i.e. only use encrypted password protected USBs.

Don’t take unnecessary paperwork out of the office, don’t go to extra locations or dawdle when travelling between locations.