

Introduction

1. The County Council records, keeps and uses large amounts of information including personal information about customers, service users, employees and others.
2. The Council therefore must comply with the Data Protection Act which requires under its seventh principle that:

“appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

“Personal data” means information about a living individual that allows you to identify them and tells the story about them

Example: name, address, telephone number, national insurance number, licence plate of a car, date of birth, or a photograph.

3. There is a particular risk of breaching this principle when Officers or Members take information about customers, service users or others away from Council premises. This might be in the form of a paper file, a laptop, loose documents, or some form of electronic removable media. Risks of loss, misuse or damage are greater because safety and security measures such as restricted access to buildings, lockable filing cabinets, security on laptops etc are not available once you leave the office.

Scope of this policy

4. This policy applies to any information in whatever format which includes personal data about a living individual including paper files, electronically on laptops, audio and video.

Responsibilities

5. The overall responsibility for legal compliance is with the Monitoring Officer.
6. Day to day responsibility for advice and compliance is with the Data Protection Officer.

7. All Members and Officers should familiarise themselves with this policy.
8. All Members and Officers who are likely to or who routinely take personal information about individual customers, service users, employees or others away from their designated County Council office or area of work must comply with this policy.
9. Failure to comply with this policy could have dire consequences for the County Council, by the release for example of highly sensitive client information which could lead to legal action against the County Council for compensation, possible adverse publicity and legal sanction by the Information Commissioner through court proceedings.

Relationship with other policies

10. This policy should not be read in isolation. It has a direct correlation to the County Council's management of records of its business activities including emails, its responsibilities to appropriately manage personal information generally. In Particular this policy should be read in conjunction with the Council's:

- a) Data Protection Policy
- b) Information Management Policy
- c) E-mail usage Policy
- e) Removable media Policy

Practical Measures to ensure appropriate information security and to minimise risks

11. There is an inherent risk in taking files, papers, laptops etc away from the office. Some Members and Officers have no choice but to take that risk, others have a degree of choice. The following are common sense pointers to reducing the risk to a minimum.
12. If you have to take personal information outside of the security of the office environment for work related reasons for example to attend a meeting, court hearing or to conduct a home visit please follow the steps set out below to reduce risks.
 - a) Consider whether there is any need to take personal information in the first place in view of the inherent risks. You may only need information of a general nature that does not refer to any particular person.
 - b) Only take that information which you need. Rather than take a full file which has client sensitive information just take a copy for example of a relevant report.

- c) Ensure that personal information is not physically visible to others when you are transporting it. Place it in a brief case or folder with no external markings.
- d) If you are travelling on public transport take proper care of personal information at all times in the same way you would with your personal belongings.
- e) If you are travelling in a car lock the personal information securely in the boot. Never leave it on display in the main body of the car.
- f) If a security breach occurs it is important to act quickly wherever possible. Thefts of personal information inside briefcases or laptops for example should be reported immediately to the police and to the Data Protection Officer. Loss or damage to personal information in other circumstances should be reported to the Data Protection Officer.

DRAFT