Information Security – Good Practice Guide

Document Owner's Name	Caroline Dodge Tel: 03000 416033 caroline.dodge@kent.gov.uk
Version	Version 2:1: April 2019

It is a key principle of the General Data Protection Regulation (GDPR) that protects personal privacy and upholds an individual's rights. The legislation refers to appropriate security measures being taken to protect unauthorised or illegal processing.

All personal data whether manual or electronic must be kept secure to prevent accidental loss, damage or destruction. The extent of the security measures required will depend on the sensitivity of the data.

Here are some basic Dos and Don'ts:

- Lock the office when leaving it unattended for any length of time to prevent unauthorised access to personal information.
- Manual records containing personal information should be locked away in a cabinet or drawer when not in use.
- When documents containing personal information have reached the end of their life dispose of them by shredding or use the confidential waste bins.
- Do not share your user ID or password with anyone.
- Ensure that your computer screen cannot be viewed by any unauthorised personnel.
- Do not send personal information by unsecured email (outside of the kent.gov email system) as its security cannot be guaranteed.
- If sending any email to multiple recipients outside of KCC, consider using blind copy facility so recipients can't view other recipients' email addresses (which, depending on the subject of the email, could constitute personal information)
- If you are required within the course of your duties to take personal data home (including laptops, videos, etc), do not leave the information unattended for any length of time, especially in a vehicle overnight.

If you are sending personal information by post, you must:

- confirm the name, department and address of the recipient;

- seal the information in a robust envelope;
- mark the envelope ‘Private and Confidential – To be opened by Addressee Only’ and place this inside a larger envelope with only the correct name and address on it - this adds an additional level of security as the package is not easily identifiable as ‘valuable’ and administrative staff should only open the outer envelope; and
- ensure that a return address is provided

If you are sending **sensitive** personal information by post, you must also:

- send the information by recorded, registered or 'signed for' delivery or by courier where appropriate;
- ask the recipient to confirm receipt; and
- record the disclosure on the service users file
- Registered post is the best way to send sensitive personal or confidential information

Different levels of security can be used depending on the information being sent:

- Reliable transport couriers should be used at all times. Consult with your organisation.
- Packaging must be adequate to protect the contents from damage during transit.

- Do not give out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the callers name and switchboard telephone number and verify their details before responding.
- Do not discuss other people’s personal business in public areas where conversations can be overheard by people with no right to know the details of the information.
- Remember - at all times treat people’s personal information as you would wish your own to be treated.

Further guidance can be found on the Information Governance portal on KNet:
http://knet/ourcouncil/Pages/information-governance.aspx