Storing, sharing and deleting information

How to recognise when information should be treated as confidential

See also the separate page on identifying personal, sensitive and confidential information. All personal data should be treated as confidential.

Note that all data within Petra is classed as confidential, apart from simple statistics which cannot identify clients. See Petra and data security.

Storage and mobile working

Data / action	Not confidential	Confidential	Further guidance
Information stored on paper, CDs, DVDs, laptops and memory sticks	Normal office procedure	Should be locked away when not in use or unattended to avoid the risk of unauthorised persons gaining access. Laptops and memory sticks should be encrypted if they hold personal information. Think about what data needs to be stored and try to minimise the amount of confidential data stored. Do not store confidential data on CDs or DVDs.	Golden rules Encryption
Removing information from the office	Allowed	Information should be carried in appropriate container, briefcase, rucksack etc. It should not be left unattended in public and should not be entrusted to a member of the public, for example in a hotel safe. Working on such material in public (e.g. on public transport) is discouraged; if it is absolutely necessary then great care should be taken (particularly with laptops and smart phones) to make sure information is not inadvertently seen.	Golden rules

Data / action	Not confidential	Confidential	Further guidance
		The safest method of working with such material is to view remotely via a VPN connection. If you plan to take high-level risk information away from the office, manager or information asset owner should give approval.	
Exchange of information within CAB offices	No special measures required	Information should be hand delivered to the recipient. If the recipient is not available the material should be locked in secure storage. It should not be left in work trays or unoccupied offices. Emails – think about the information contained within the email and ensure it is marked appropriately, addressed to only the relevant people and encrypted if necessary.	
Sharing data with local and national archives	No special measures required	Follow the BMIS guidance.	Sharing client data with local or national archive services

Transmitting information

- Always log transfers of confidential information.
- For regular or large transfer of information see guidance on data sharing.

Data / action	Not confidential	Confidential	Further guidance
Letters / paper documentation	No special protective measures	Moderately confidential, such as a single client record: • Normal post, recorded delivery or hand delivered. High risk confidential or large amounts of data: • Recorded delivery.	Golden rules

Data / action	Not confidential	Confidential	Further guidance
Fax	No special protective measures	Permitted but with appropriate safeguards. • Ensure a trusted person is at the recipient fax machine to receive fax. • Use a cover sheet (including appropriate protective marking). • Check fax number is correct. • Use pre-programmed fax numbers where possible. • Confirm receipt of fax via telephone / email.	Golden rules
Email within the Citizens Advice network. i.e. from a Citizens Advice email or Cabnet address	No special protective measures	No special protective measures required, but think about the information contained within the email and ensure it is marked appropriately, addressed to only the relevant people.	Encryption Golden rules
Email transmission to external parties over public networks (i.e. the internet)	No special protective measures	Confidential data should be encrypted or contained in a password-protected attachment. Password must not be transmitted via email. The email should be marked Confidential. Do not copy or forward confidential emails unless there's an essential business need.	Encryption Golden rules
Use of telephone equipment (desktop, mobile, BlackBerry, smart phone, iPad)	No special restrictive measures required	Take care if communicating in a public space where the conversation may be overheard or in the office if unauthorised persons are present and might overhear. Avoid discussing when one or both partners are overseas.	Encryption Golden rules
Leaving information on answer phones or voicemail systems	No special restrictive measures	The conditions on the use of telephone equipment apply.	

Data / action	Not confidential	Confidential	Further guidance
		There is the additional risk that the recipient's setup is not secure and messages may be accessed by others.	
Video conferencing	No special protective measures	Must not be established in a public place where the conference might be overheard / overseen. Should avoid when one or both parties are overseas.	
Instant messaging	No special protective measures	Avoid sending any personal information via instant messaging.	ICT acceptable use policy
Email advice	Information allowed	Avoid giving advice which uses personal details unless using encrypted email.	Digital advice services: information assurance issues
Web chat	Information allowed	Avoid giving advice which uses personal details.	Digital advice services: information assurance issues

Disposal

Data / action	Not confidential	Confidential	Further guidance
Disposal of paper documentation	Allowed	Paper must be disposed of by a secure method such as cross-shredding or confidential waste disposal facilities.	Planning for disposal of confidential information
Disposal of files on magnetic media – CDs, DVD etc.	No special protective measures required	CDs and DVDs should be destroyed.	CABlink: IT equipment disposal Planning for disposal of confidential information
Disposal of IT systems back-up tapes and hard drive disk systems	Must be disposed of in a secure manner to ensure the re-constitution of data is unlikely.		CABlink: IT equipment disposal Planning for disposal of confidential information

Data / action	Not confidential	Confidential	Further guidance
Disposal of photocopier / multi-function devices	Check if existing equipment is capable of storing data. If the equipment can store data, contact suppliers / maintainance company for instructions on securely deleting the user data area. New equipment which has the capability of storing data: ensure that instructions for securely deleting the user data area are supplied.		CABlink: IT equipment disposal Planning for disposal of confidential information
Photocopying and printing of information	No special protective measures required	Keep to a minimum and only for essential business requirements.	

Cloud based file sharing and storage

See the guidance on working with information that is stored in the cloud.

Marking personal and sensitive information

See information about how to mark documents and files that contain confidential information.