

## A QUICK REFERENCE GUIDE

## TO PROTECTING YOUR INFORMATION

	GENERAL	SENSITIVE	CONFIDENTIAL/ RESTRICTED
Marking documents	Having a marking system for documents, including emails, helps people to understand and follow correct procedures – like the ones set out in this checklist. If a document does not contain sensitive information, then you can either choose not to mark it or include 'general access' on the top of each page/email for example	When a document is sensitive or confidential, marking this in a header, footer or the top and bottom of the page will ensure that the document is handled correctly, from who sees it to how it is disposed of. You should also mark this on emails and envelopes too. Treat anything which contains customer, financial or contract details as RESTRICTED	
Storing sensitive/confidential information	n/a	Locked storage cabinet – see <a href="http://www.stop-idfraud.co.uk">www.stop-idfraud.co.uk</a> for further details	In secure storage area / safe - see <a href="http://www.stop-idfraud.co.uk">www.stop-idfraud.co.uk</a> for further details
Sending sensitive or confidential information by post	Standard post	Courier or Recorded Delivery TIP: try to use the same courier or delivery service. See <b>Royal Mail</b> website for more details	By hand if possible or by Recorded Delivery/Courier requiring recipient's signature. See <b>Royal Mail</b> website for more details
Sending sensitive or confidential information by email	Standard email (marked high importance if applicable) Never click on embedded URLs of unsolicited mails to ensure email stays protected from spyware	Public / Private key cryptography to encrypt or decrypt emails	Public / Private key cryptography plus digital signatures
Using the Internet	Always ensure anti-virus software and firewalls are maintained and up-to-date - both of these actions are essential. Always check for the lock button at the bottom of the screen when submitting sensitive or confidential information via a website. This ensures the information is encrypted		
Destruction and disposal of paper and CDs/DVDs	Shred all unwanted papers using a <b>cross cut shredder</b> . General information can be placed in boxes for shredding but <b>must</b> be shredded before you leave the office/department at the end of the day. You may find it easier and simpler to shred as and when you need to	Unwanted protectively marked or sensitive material <b>MUST</b> be disposed of properly – <b>DO NOT</b> put it in the recycling bins. Shred immediately using cross-cut shredder – this includes information held on CD or DVD ( <i>but check your shredder accepts them first</i> )	
Disposal of computer equipment and related information storage	Before disposing of, selling or donating an old computer or hard drive, the data on it should be fully erased from the hard disk. Simply deleting files isn't enough to permanently erase them. You need a special utility, such as <b>Evidence Eliminator</b> , <b>KillDisk</b> or <b>Eraser</b> , that will delete all traces of the file. There's a list of local computer recyclers and refurbishers on the <b>Waste Online</b> website. Your <b>local authority</b> will have more information about disposing and recycling rubbish. You may be able to sell your old equipment, but you can also considering donating them to Computer Aid or Donate a PC		
Uniforms, corporate clothing	Uniforms and corporate clothing or products can also be used by fraudsters so ensure that these items are destroyed correctly when you no longer need them. If you use a third party supplier to destroy electronic equipment ( <i>see above</i> ) or corporate uniforms for example, make sure they have <b>BSIA</b> (British Security Industry Association) Accreditation		
Company logo	Do not email or send out artwork files of the company logo unless you are sending it to a known recipient with a legitimate business reason. Always ensure your logo is protected on websites and in emails so that it can not be saved as an image and used without your permission		
Headed Paper	Do not throw away or give out blank paper to customers or suppliers and always shred any information on headed paper		

## AND A FEW EXTRA TIPS:

- Never leave papers in meeting rooms, on photocopiers or printers, especially if they do contain sensitive information
- Always clear your desk at night and lock away protectively marked papers and all removable computer media before you leave your office
- Shred unwanted papers and Cds/DVDs before you leave the office or department – don't leave them lying around for someone else to destroy
- If you are responsible for any security furniture like lockable cabinets, safes etc ensure the combination is changed every 6 months or whenever someone leaves the company or no longer requires access
- Keys must be stored securely when not in use –under a plant pot or in a desk tidy is not good enough
- Look after your password – never reveal it to anyone and never write it down
- Keep your work area tidy – this will ensure that you don't accidentally forget to lock away protectively marked or sensitive material
- And finally, hold regular training and update sessions for your team/staff to ensure that they are fully aware of, and understand the steps they should take to help prevent identity fraud