Remote Worker’s Data Audit

Use this checklist to identify any “rogue” data on your personal devices

Data type	Should it be stored/ accessed on a personal device?	Detail
Personal HR information	✓	You can store data that relates only to you on your own device, but make sure you’re following the usual best practice advice ie strong passwords, keeping operating system up to date.
HR information pertaining to others	×	This should not be available to anyone other than employees that need access (the HR dept, relevant line manager) and should not be saved to personal devices.
Marketing or product information that’s already been published	✓	If it’s already in the public domain, eg. as website copy, it can be saved on personal devices if necessary.
Product or service information that’s not yet publicly available	×	Keep this under wraps by storing securely on your network with access allowed only to those that need it, via VPN/remote desktop. Use your email service provider (MailChimp, Active Campaign) to access these via VPN/remote desktop and do not download to personal devices. Allow access only via remote desktop or VPN. This data should not be downloaded to personal devices.

Data type	Should it be stored/ accessed on a personal device?	Detail
Marketing contact lists	×	Use your email service provider (MailChimp, Active Campaign) to access these via VPN/remote desktop and do not download to personal devices.
Sales prospect & lead information	×	Allow access only via remote desktop or VPN. This data should not be downloaded to personal devices.
Emails	×	No company emails should be saved to personal devices. Access them using your business's cloud technology or email server.
Plain text passwords	×	Don't save plain text passwords anywhere, on any device.
Passwords saved to browser	×	Use a company password manager accessed via VPN/ remote desktop to secure passwords.
Customer billing information	×	Should be subject to the same stringent security it would be when employees are working in the office.
Hard copies of data	×	It's obviously not possible to store these on a device, but apply the same principles you would in the office. Keep confidential data under lock and key and shred anything that needs to be disposed of.

About Beaming

We are a specialist business Internet Service Provider offering fast, reliable and secure connectivity and remote working solutions to thousands of organisations across the UK.

Beaming is serious about service with a network built for business; we make sure you stay connected.

To stay up to speed with the latest cyber security threats plus industry research stats and resources visit www.beaming.co.uk or find us on Twitter @BeamingNews