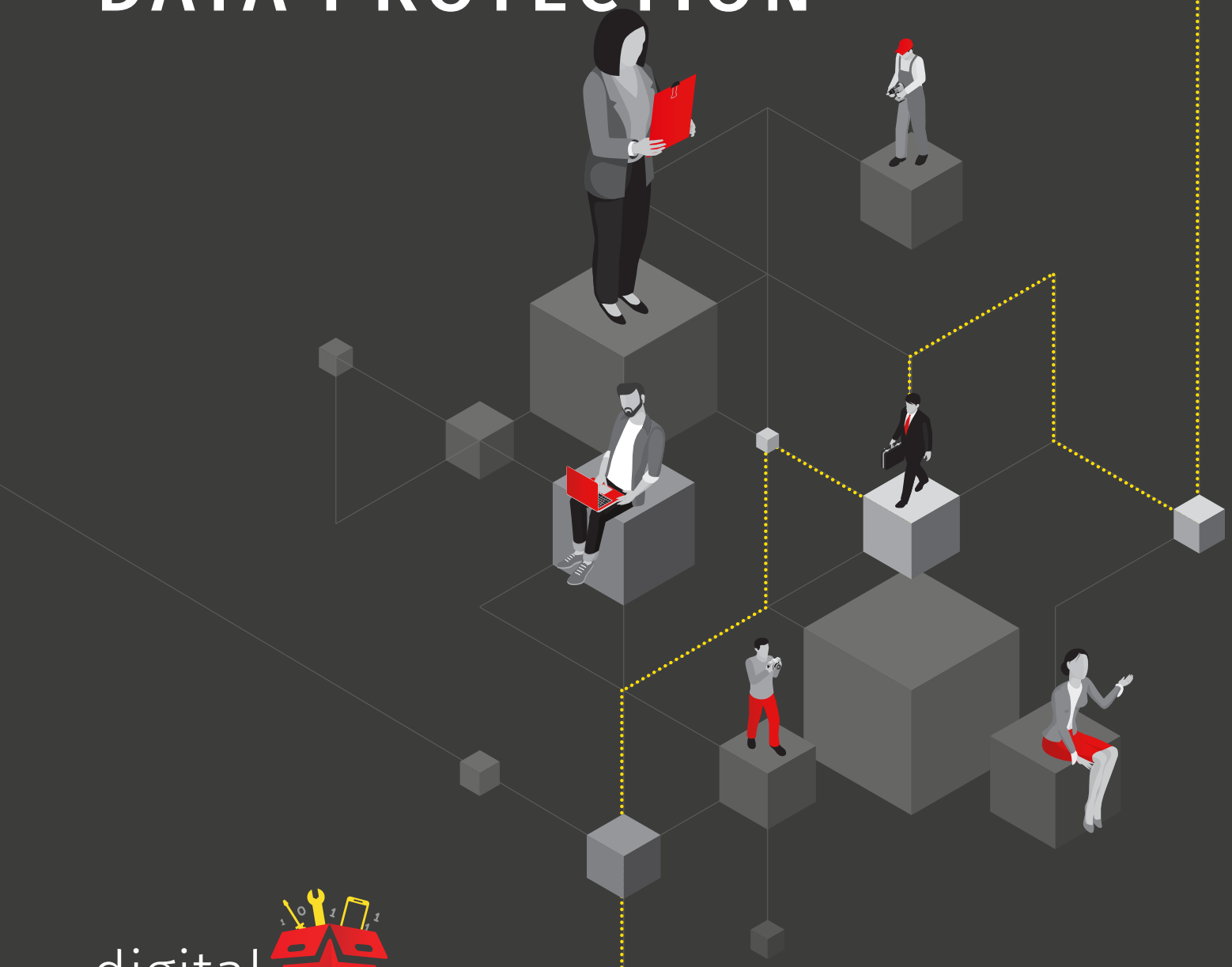
ORGANISATIONS

WORKING FROM HOME AND **DATA PROTECTION**



digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Working from Home - Checklist

We have produced the below checklist to advise on the Dos and Don'ts of working from home.

Security - have you considered?

Domestic internet security – Do staff have secure WiFi (one with password access) and anti-virus software, firewall and/or VPN as appropriate?

☐ Yes ☐ No

Are their computers (operating systems and software) up to date with all patches and updates applied?

☐ Yes ☐ No

Is this a normal activity for your member of staff? If not brief and train them first about protocols set out below.

☐ Yes ☐ No

Have you thought carefully about physical security of all documents, including paper records?

☐ Yes ☐ No

Do you have a plan for how physical paperwork is going to be transported from work to home (for example in a locked briefcase and not left in open view in a car)?

☐ Yes ☐ No

Have you checked that staff members only have access to those parts of the company systems that they need?

☐ Yes ☐ No

Do you have the ability to find any devices that get lost and remote wipe them if you need to?

☐ Yes ☐ No

Setting up home working

Have you set up your office in a physical space where family members and visitors cannot see the paperwork or access laptops?

☐ Yes ☐ No

Do you lock paperwork/equipment away securely when not in use?

☐ Yes ☐ No

Do your staff know how to report and handle a data breach if one should occur?

☐ Yes ☐ No

Are all employees aware of what to do if a physical file is lost and have you tested that plan?

☐ Yes ☐ No

Who needs to know?

Has your organisation ensured work is being conducted in accordance with data security and home working policies?

☐ Yes ☐ No

Have you considered having a sign-in / sign-out procedure for when taking files and personal data home?

☐ Yes ☐ No

Do contracts of employment have compliant data privacy clauses and refer to appropriate security, homeworking and transporting data rules?

☐ Yes ☐ No

What are the risks of a data breach?

Whilst working from home, being distracted and leaving unlocked devices or paperwork loose or unattended, is easy to do.

Are you aware that if an unauthorised person is able to access the computer or paperwork you are working on, this is a data breach?

☐ Yes ☐ No

Top Tips

- ☐ We recommend working in a private, secure place in your home;
- ☐ Do not leave unlocked devices unattended or paperwork lying around;
- ☐ Ensure all paper files are secure in a locked area which is not accessible to anyone else;
- ☐ Ensure you have secure WiFi (one with a password access) and anti-virus software;
- ☐ Ensure that your operating system and software is up to date;
- ☐ If you take work between the office and home, only take home what is absolutely necessary and return if when you no longer need it;
- ☐ Ensure staff are aware of how to report and handle a data breach if one should occur;
- ☐ Ensure 'working from home' policies / contracts are in place and all staff are provided with adequate training about working safely from home (including in respect of things like recognising phishing attaches etc.).

Jersey Office of the Information Commissioner, 2nd Floor, 5 Castle Street, St Helier, Jersey JE2 3BT
Telephone number: +44 (0) 1534 716530 | **Email:** enquiries@jerseyoic.org