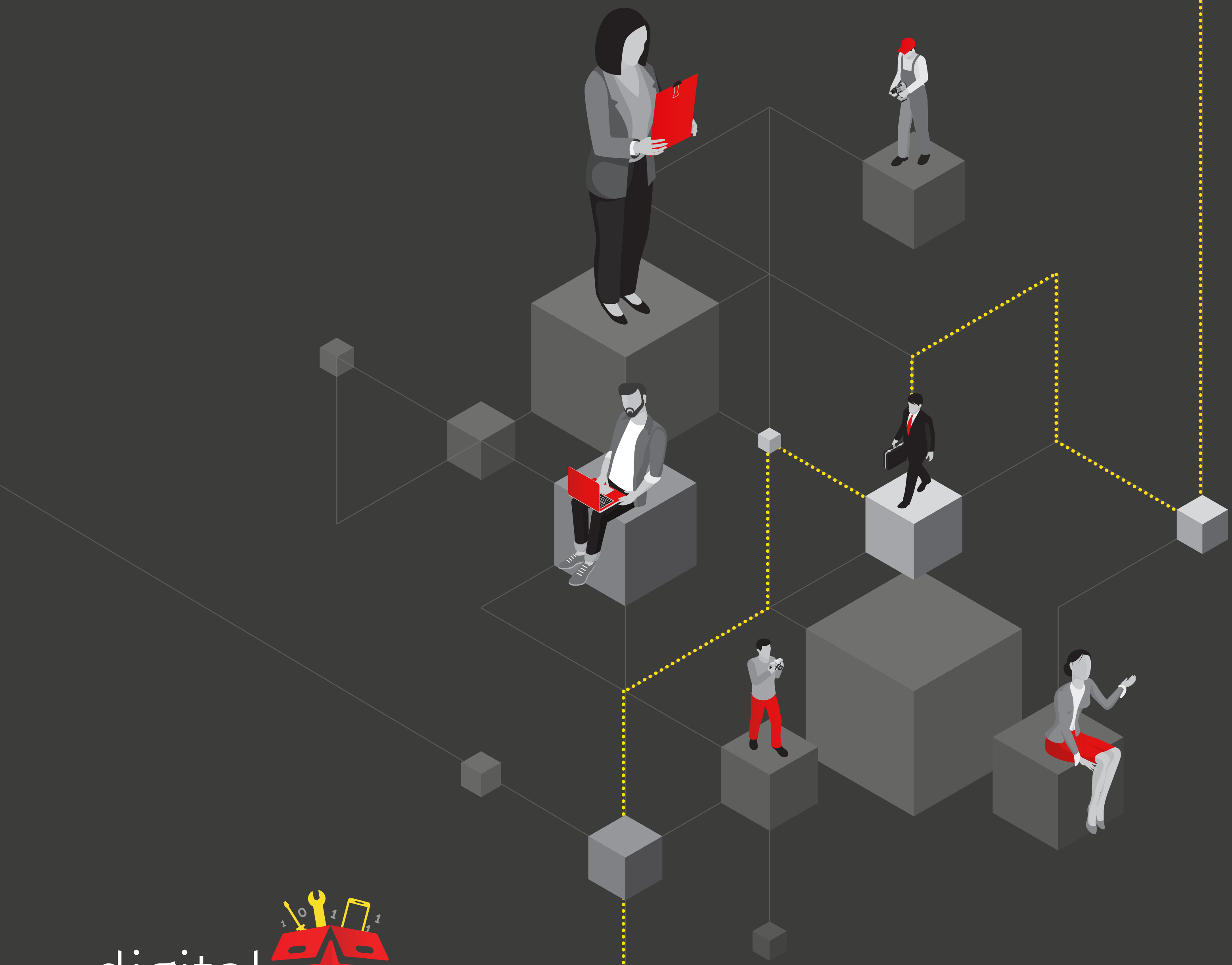
ORGANISATIONS

SOCIAL MEDIA CHECKLIST
FOR LARGE BUSINESSES



digital TOOLKIT

Guidance for Organisations

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Setting up an Account and Account Maintenance

□ Make sure you're signing into the real social network website;

□ Be wary of suspicious direct messages and connection requests;

□ Use a strong, unique password for each social network. If it is strong, you shouldn't need to change it regularly but you should change it if you think your social media account has been accessed **unlawfully**[1]. You may wish to use a password manager application to help generate unique passwords and keep a record of them for you;

□ Enforce access controls on corporate accounts and train corporate users;

□ Enable two-factor authentication for all your business social media accounts. Have the two-factor authentication linked to a corporate device that is locked down;

□ Establish automated tools to identify inbound attacks and leaked data;

□ Integrate social media data into the existing security infrastructure;

□ Keep your device's software, social network mobile application, and browser up to date;

□ Configure account monitoring for unexpected activity;

□ Have communication and action plans in place;

□ Enable a technology with functionality to automatically lock down your accounts if they exhibit strange behaviour;

□ Do not share, retweet or tag profiles you don't recognise;

□ Systematically monitor social networks for threats to your business.

Policies and training

□ Build policies for social media and explain what information should and should not be shared;

□ Train employees on policies and how to use social media safely and appropriately (including appropriate use of language);

□ Are those with access to social media accounts aware of what they can/cannot post?

[1] https://www.ncsc.gov.uk/collection/passwords

□ Stay up to date on the latest social media scams and tactics and communicate to staff as necessary;

□ Work with marketing to identify key stakeholders and employees with privileged access to social media accounts;

□ Ensure that your social media accounts are only accessible by those who need access. If your social media accounts are accessible by multiple users, do you have a social media usage policy?

□ Ensure that the corporate email accounts connected to your social media accounts follow the same user access guidelines of any other critical system.

Terminating/suspending access

□ Audit social media access and permissions quarterly.

□ When an individual exits an organisation (either permanently or is suspended from work for any period), do you have procedures in place to ensure that individual can no longer access any of the corporate social media accounts? Do you have a Bring Your Own Device ('BYOD') policy that allows you to remotely access an individual's device to delete any information belonging to the organisation?

□ Do your contracts of employment contain any clauses about ownership of contact lists on a social media account when employees leave an organisation but had, say, a LinkedIn profile that was set up by your organisation? Are you clear about who 'owns' those employee social media accounts and what an employee's obligations are when they leave?