ORGANISATIONS

# SOCIAL MEDIA CHECKLIST
# FOR SMALL BUSINESSES

digital
**TOOLKIT**
Guidance for Organisations



JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

## Setting up an Account

- [ ] Make sure you are signing into the real social network website;
- [ ] Use a strong, unique password for each social network. If it is strong you should not 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;
- [ ] Set up your security answers. This option is available for most social media sites;
- [ ] Set up two-factor authentication;
- [ ] If you have business social media apps accessible on your phone, be sure to password protect your device;
- [ ] 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? Are people aware of what they can/cannot post?

## Proceed with caution

- [ ] Be wary of suspicious direct messages and connection requests;
- [ ] Do not share, retweet or tag profiles you do not recognise;
- [ ] Click links with caution. Social media accounts are regularly hacked. Look out for language or content that does not look like something a connection of yours would post;
- [ ] Be careful about what you share, especially when it comes to third party data. For example, if you have taken a photograph which features a data subject/individual, do you have their consent to publish their photograph?
- [ ] Do not reveal personal information i.e. financial information. The more you post, the easier it is to have your identity stolen;
- [ ] Think carefully about the terminology and language you use on each social media platform.

**TIP**

Personal information is any information that can reasonably identify an individual. This could include name, phone number or email address.



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

All business personnel that deal with personal information should receive training as to their obligations, and a business should consider whether its privacy policy accurately discloses its practices with regard to collection, use and disclosure of personal information, including with respect to social media.

*For example, disclosure of information that was imparted in confidence can also lead to legal issues. An example that is particularly relevant to companies is the non-disclosure clauses sometimes present in business to business contracts. They might outline that any public disclosure of the relationship between the businesses is not allowed or is only allowed with permission of the other party. But will the excited sales team member posting on social media about landing a big deal with a well-known company be aware of those clauses?*

Check out other social media risks – defamation, advertising standards, misleading conduct, copyright infringement. When using social media it is critical that you use appropriate language, terminology and imagery. Get into the habit of drafting and rereading your posts for errors which may cause offence or damage your reputation and the possibility of revealing information that you should not be sharing.

## Settings

- [ ] Become familiar with the privacy policies of the social media channels you use and customise your privacy settings to control who sees what;
- [ ] Protect your computer by installing antivirus software to safeguard. Also ensure that your browser, operating system and software are kept up to date;
- [ ] Audit social media access and permissions quarterly.

## What can a Business do to Mitigate Risks?

The appropriate steps will differ depending on the business and the industry in which it operates but some recommended compliance procedures include:

- [ ] A company policy for digital communication and social media;
- [ ] Terms of use or house rules for users who post or upload content;
- [ ] Regular monitoring and moderating of online and social media sites to remove inappropriate and unlawful content, including allocation of site monitoring responsibilities to individual staff members who report to a suitably experienced manager;
- [ ] Regular staff training on company policy and legal requirements;

- [ ] Internal digital security measures (for example, password access to company sites);
- [ ] Online filters (for example, age restrictions and/or language restrictions);
- [ ] A current **privacy policy** which is easily accessible to consumers and which clearly outlines how the company will use personal information, including collection of unsolicited personal information;
- [ ] Legal review of campaigns including obtaining copyright clearances.

**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