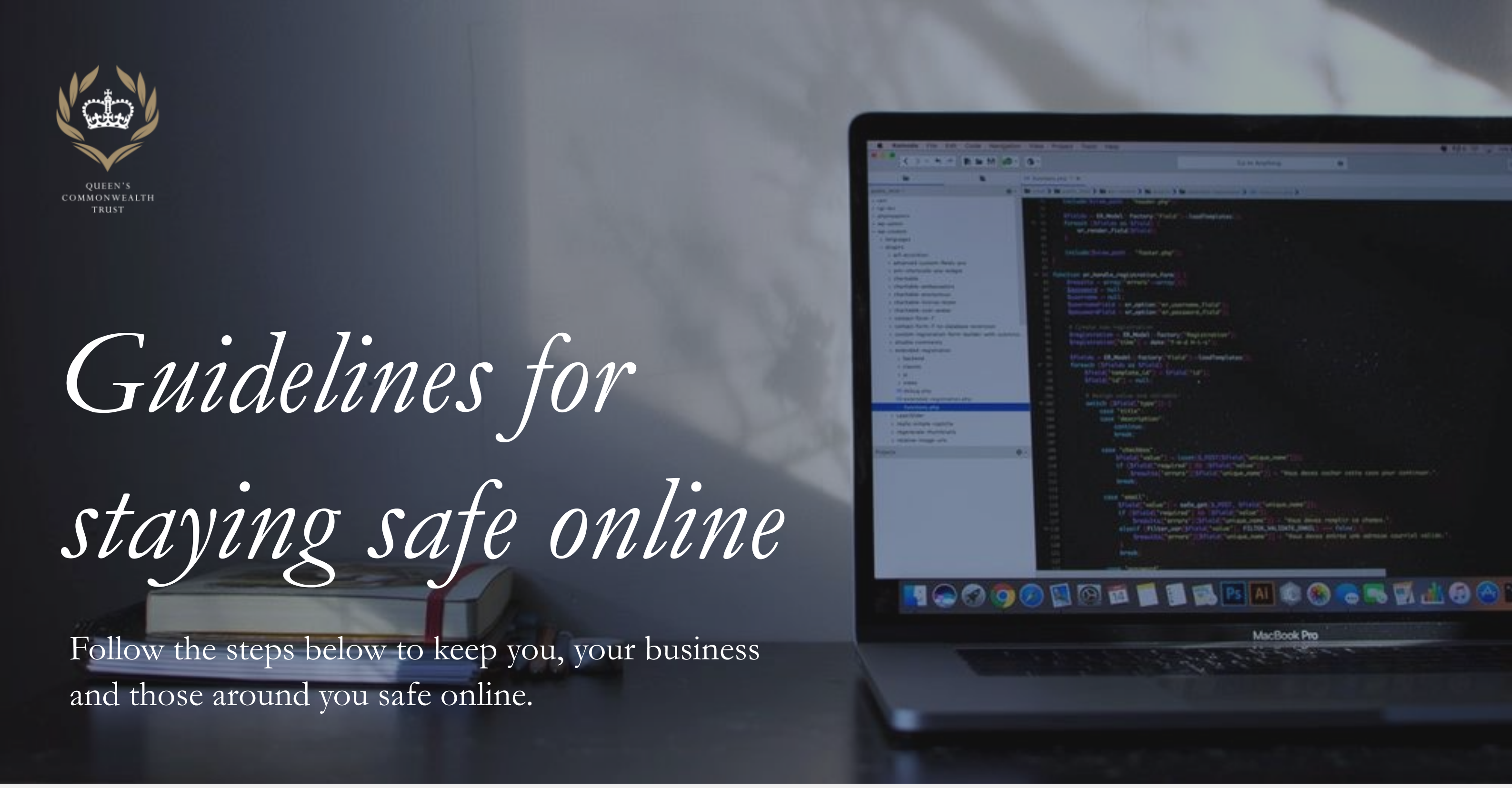

QUEEN'S COMMONWEALTH TRUST

# *Guidelines for staying safe online*

Follow the steps below to keep you, your business and those around you safe online.

## *Summary*

1. **Use a complex password:** It should be hard for other people to guess your password, so utilize letters, numbers and symbols to better protect yourself. It's also a good idea to change them regularly.
2. **Be careful what you share:** Once something is online, it's out of your control. If you'd be embarrassed to have that content attributed back to you later in life – don't post it now.
3. **Protect your space:** Don't accept people you don't personally know or have any clear reason for being connected. Keep your account private to maximise control over who sees what.
4. **Know when to ask permission:** Not everything online is for the taking. Check with the owner before reposting original content.
5. **Talk about it:** If you see something online that makes you upset or uncomfortable, report it to the relevant platform or, if serious, to the police. Share your experiences with someone you trust to get help with dealing with any form of abuse or bullying.

## *Social Media guidance*

- **Choose a strong password** which uses a mixture of letters, numbers and symbols.
- **Aim to have a different password** per social network and/or website, so if one account is compromised, your others remain protected.
- **Never share personal** information including your address, mobile number or passwords and always remember to log out of shared computers and other devices.
- **Adjust your privacy settings and review them often.** By default, a lot of social media accounts will assume that you want to be visible to their entire online community. Choosing a private account will require individuals to request access to your personal page before they can see or comment on anything that you have posted, giving you complete control.
- **Only accept friend requests from people you know personally** and ignore and/or block direct messages from people you don't know.
- **Be kind!** Be considerate of others when choosing what to post, taking positive steps to avoid content that could be deemed offensive or abusive towards others. Always remember that anything we post online can potentially be viewed by anyone not just now, but in the future as well.

### *Top Tip!*

*Use phrases instead of words to create stronger passwords. For example: 'QCTsupp0rtYoungLe&der5' will be harder to guess than 'youngleader'.*

## Report it!

- Abuse, bullying, harassment or impersonation of any kind is ***unacceptable***. If you see something that looks suspicious, or you have received a message or image that you feel is inappropriate in its nature, report it to the relevant social media channel, or if serious, to the police. If you still feel concerned talk about it with a trusted friend who will be able to offer advice.

- If you see harmful comments or inappropriate behaviour towards other people's posts, you are within your rights to report this as well. Likewise, if you feel someone's content could be harmful to them or others, it may be a good idea to flag this as triggering content too. If they are a friend, then why not reach out over the phone, send a direct message, or chat in person and let them know they have your support.

## Social Network Safety Centres

*Click on the below icons to be taken to the relevant support centre*

TikTok

## Data Protection and Usage Rights

- **Keep an eye on your emails**. If something doesn't look quite right, or the original sender isn't someone you recognise, then mark it as Junk, block the sender and delete it. Never click on links from emails you don't trust.

- **Get familiar with the laws in your region:** For example**, if** you have a business active within the EU, then the GDPR means you must collect and store data in a way that enables you to quickly provide individuals with:
  - **Access to their own data**, and information on how their data is processed;
  - **An easy way to transfer their personal data** between service providers, ('right to data portability')
  - A right to have their **personal data erased** if there is no legitimate reason for retaining it; ('right to be forgotten')
  - Notification if their **information has been hacked**.

For those of you living or acting outside this region, these are still good guidelines to bear in mind, and will ensure that any data you collect on behalf of customers or service users is transparent and easily accessible.

- **If you didn't create it, you might not be able to use it.** Copyright is a protection for any "fixed form" content, meaning the minute you type that blog post or put that photo on Insta, you're protected. With this protection, no one else can use your work without permission.

- **Get permission.** In today's online world, most people are probably happy for you to reuse their images or words, provided you give them credit – but it's safer not to assume. Where possible, always ask the content owner for permission.

- **Rights vs Licenses. I**f using stock imagery you might have come across the term 'licensing'. Companies such as iStock or Getty Images, offer a range of 'licences' which dictate the level of rights you have to that image. For example, some licenses limit the purchaser to 'personal' or 'online' use only, meaning you wouldn't be able to print the image.

### Top Tip!

*Although it feels like we can share whatever we want online, it's always safer not to assume. Always ask before reusing people's words or imagery.*

QUEEN'S COMMONWEALTH TRUST

Online safety is a constantly evolving topic, so we will be updating these guidelines as needed.
In the meantime we hope you find this useful and would love to hear how you keep protected online.
Let us know aby contacting us at info@qct.org.uk or connect with us via Facebook, Instagram or Twitter to keep up to date with our latest work and resources.