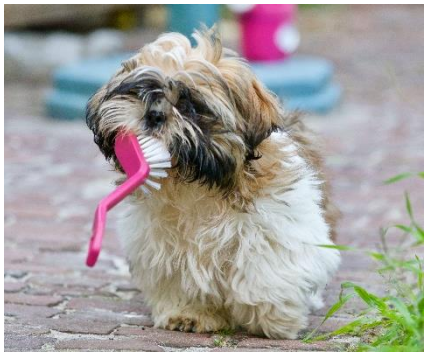
Cybersecurity and Data Protection

This guide offers a brief introduction to the key principles of Cybersecurity and Data Protection, as well as suggesting some handy pointers and where to seek further help.

Whilst the advice on Cybersecurity and Data Protection can feel like it is constantly changing, **Charity Digital** offer the motto that both should be viewed just like brushing your teeth, in that if you practice it daily it will become a simple, straightforward habit.



Here is a list of organisations who can help you 'brush up' on your Cybersecurity and Data Protection good practice:

Superhighways offer resources, training and advice with a focus on small charities.

National Cyber Security Centre (NCSC) have an incredibly helpful Guide to Cybersecurity for Small Charities. The NCSC also offers printable infographics and a Cyber Essentials Readiness Toolkit to help you think about cybersecurity within your organisation and create a personalised action plan. You and your organisation can become certified through the Cyber Essentials government backed scheme.

There can be a lot of technical terminology used at times when speaking about cybersecurity and it can be difficult to cut through this when deciphering what the advice actually means for your organisation. Luckily, the NCSC have created a Cybersecurity Glossary to help you become a cybersecurity terminology pro.

Information Commissioners Office (ICO) is the UK's independent authority to uphold information rights in the public interest. Their website has a range of toolkits, online self-assessments, webinars and training videos. Groups can seek advice via the helpline, online chat and the 'SME Hub', dedicated to helping small organisations, including charities.

Richmond CVS have a partnership with Russell-Cooke Solicitors, who offer free advice on subjects ranging from Charity Law to Data Protection. Please contact Richmond CVS to arrange a chat.

What is Cybersecurity?

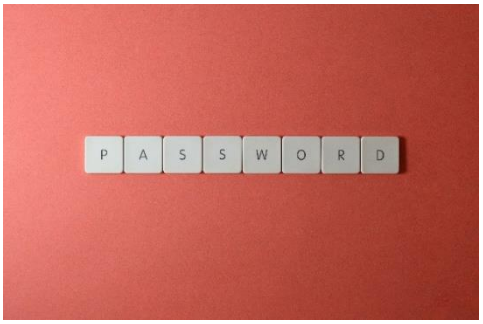
Put simply, cybersecurity is 'the means by which individuals and organisations reduce the risk of becoming victims of cyber attack' (NCSC).

Charity Digital lists the most common aims of cyber criminals to include:

- getting unauthorised access to computer systems
- infecting computer systems with viruses or other malware which enables them to steal, modify or delete data
- fooling computer users into submitting data, payment details, or other confidential data at websites controlled by the hackers
- preventing customers or service users from accessing victim organisations' computer systems by overloading them.

The most important part of cybersecurity practice is prevention. For your organisation, this may take the form of regular discussion of the latest cybersecurity best practices at team meetings, circulation of what the latest phishing scams look like, ensuring two factor authentication is used on all devices, using 'work' email addresses rather than personal, purchasing the right anti-virus and firewall software for your organisation, running the recommended updates on these and performing regular risk assessments.

Prevention:



Superhighways recommends 5 simple ways to stay protected online:

1. Backing up data
2. Preventing malware damage
3. Using passwords to protect your data
4. Keeping smart phones and tablets safe
5. Avoid phishing attacks.

Read the full article here.

For a more in-depth look, head to the NCSC page and download the Small Charity Guide. Or follow this link for an infographic summary (suggested by Superhighways to print and display): Infographic Summary.

Another great tool from the NCSC is their free online Training Module which can be completed by members of staff or volunteers in your organisation.

Charity Digital have a webinar on Five steps to improve charity security, which is free to watch on YouTube. The learning outcomes of the session include 'how to create and document security policies, build security awareness and skills throughout your team and choose and use technology to fit the way you work'.

Get Safe Online has lots of clear, jargon-free advice that's just as much relevant to individual practice as it is organisation-wise. There is a really handy section on social media, including best practice on WhatsApp, Facebook and video calls, as well as the risk of phishing on social media.

You could even follow Charity Security Forum on Twitter to receive digestible cybersecurity tips on your daily feed.

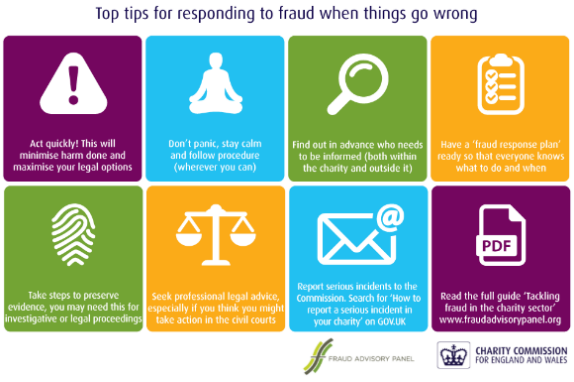
Response and Recovery:

The NCSC have a whole section of their guide dedicated to Response and Recovery.

Also provided by the NCSC is an incredibly helpful (and free!) tool called Exercise in a Box, which allows organisations to test and practice their response to a cyber attack.

Social Media advice:

Take a look at the NCSC's page on Social media: protecting what you publish, which has a section on how best to use the tools available to you on each platform.



Reporting:

Go to Action Fraud's page on Reporting Fraud at actionfraud.police.uk.

The NCSC offer advice and a form to fill in here: Reporting a cyber security incident.

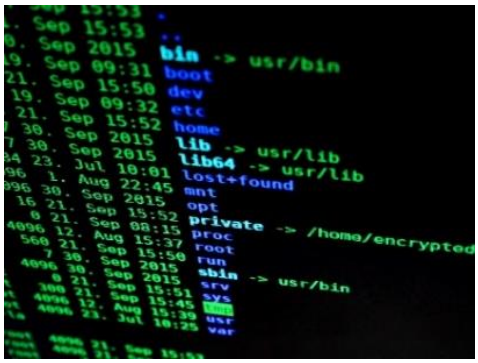
If you have been subject to a data breach, this may need to be reported to the ICO.

You may also need to report an incident to the Charity Commission. See their helpful guide on What to Report.

Data Protection

Data protection law aims to make sure that personal data is gathered, stored and used responsibly and transparently. It gives people ownership of information about themselves and works to limit how organisations use that data, forcing them to use it responsibly.

The relevant law in the UK is the Data Protection Act 2018. It was updated in 2019 with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations. The law and regulations align law in the UK closely to GDPR, the primary European regulation on data protection.



Personal Data

For many organisations, personal data is the most obviously identifiable information about a person, such as name, age, email address, full postal address or full postcode.

There are also types of legally defined sensitive personal data, called special category data, which includes:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
- genetic data
- biometric data (where used for identification)
- data about health
- data about a person's sex life
- data about a person's sexual orientation.

Understanding Data Protection Principles

You need to know and understand what the legal principles of data protection are and what they mean for your organisation (see right-hand table).

CAF offer a printable GDPR Infographic with practical tips on how to incorporate the 7 key principles of data protection into your every day.

7 Key Principles of Data Protection:

Lawfulness, fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality (security)

Accountability

Further Resources on Data Protection:

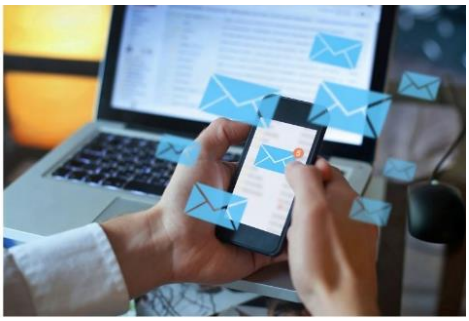
Visit the ICO Advice page for small organisations. Under the 'SME Hub', the ICO have created a Self Assessment Toolkit.

Also worth a look is the ICO's article on Mistakes and How to Fix Them

NVCO offer a number of resources on both cybersecurity and Data Protection: NCVO Data Protection

For Data Protection at a glance, visit Superhighways' article on Data Protection: 5 simple ways small charities can apply the rules. Superhighways have also made available Paul Ticher's resource on GDPR Elements.

With the rise in popularity of email marketing amongst small charities, it is vital to remember the principles of Data Protection when handling subscribers' data. The ICO have a page dedicated to Electronic Mail Marketing. Keep in mind legitimate interest and always provide an 'opt out' option. As one of the leading email marketing tools, here is Mailchimp's take on what they do to comply and what you need to do to comply: Mailchimp on Data Protection. This page also provides a downloadable Guide to GDPR.



You can download a Data Protection Policy template Here.

Alongside Data Protection, don't forget good confidentiality practice. This can be as simple as treating other individuals' data as you would like your own personal information to be treated. Russell-Cooke have a helpful article outlining some key points to consider: Confidentiality when sharing information.

Please be advised that this resource has been designed to offer guidance but is not legal advice.

Updated by Becky Daybell, Project Officer, March 2023