#Derbyshire Online

Cyber Security Toolkit for Voluntary Organisations in Derbyshire

Version 1.1

Derbyshire Constabulary

Contents

Version History

Version	Date	Reason
Version 1.0	24/10/18	Completed for publication
Version 1.1	9/8/19	Document reviewed/updated

Introduction

What is cyber security?

Cyber security is any strategy, processes, practices or technologies that organisations have in place to secure their networks, computers or other devices, and the data they hold, from damage, attack or unauthorised access.

Why is cyber security important?

The government commissioned Ipsos MORI to conduct research to explore the awareness, attitudes and experiences around cyber security of charities in the UK. The MORI report, entitled 'Cyber security among charities', was published in August 2017. The research found that voluntary organisations may be vulnerable to cyberattacks if they:-

- Do not consider cyber security to be a priority
- Assume that businesses are more likely to be targeted
- Are not well informed about the topic
- Have not seriously considered cyber security or sought out any information
- Have no internal specialist staff with technical skills to cover cyber security
- Do not receive cyber security training.

Cyber security is an important issue for charities and voluntary organisations because they hold sensitive personal data on donors, volunteers or service users, but often it has not been prioritised for a number of reasons:-

- Naivety – 'it won't happen to us', 'we don't have anything of value'
- Lack of knowledge
- Lack of investment
- Lack of training for staff/volunteers/trustees.

What are the risks?

The National Cyber Security Centre (NCSC) has completed a 'Cyber threat assessment: UK charity sector', which identifies who might target the voluntary sector and why. Cyber threats include:-

- Viruses
- Phishing e-mails
- Ransomware attacks
- Identity theft
- Distributed denial of service ie website takedowns
- Financial fraud
- Insider threat.

The risks and potential implications of not taking steps to improve your cyber security include:-

- Loss of personal data, leading to:-
    - loss of trust and confidence amongst donors, service users and other stakeholders
    - financial penalties from the Information Commissioners Office
- Financial loss to the charity, or people involved with the charity
- Loss of reputation
- Loss of access to IT systems and data, affecting 'business continuity'.

What can voluntary organisations do about Cyber Security?

The National Cyber Security Centre (NCSC) has produced the 'Cyber Security: Small Charity Guide', which outlines the basic steps that voluntary organisations should take to protect their organisation and its assets. Many of the suggestions are quick, easy and low cost.

Using this Toolkit

This document is designed to be a basic toolkit to enable charities and voluntary organisations in Derbyshire to assess their areas of weakness in relation to cyber security and find out how to access detailed advice from reliable sources.

This document is not a technical assessment. The questions on pages 5-10 are designed to prompt you to consider which areas are a priority for your organisation and prompt you to seek further information and advice, as necessary.

This toolkit also provides links to additional resources, covering:-

- What to do in the event of a cyber attack
- How to report different types of cybercrime
- Glossary of terms
- Online cyber security assessments
- Comprehensive cyber security advice and information
- Development of information security policies
- Training opportunities
- Procuring IT services
- General Data Protection Regulations (GDPR)
- Cyber liability insurance
- How to access support from Derbyshire Constabulary.

What is your exposure to digital risk?

What IT equipment does your organisation use that needs to be 'cyber secure'?		
Response		*Advice*
Desktop computer(s)	☐	**Prevent malware damage** • Use anti-virus software on all devices that are connected to the internet. • Use the 'automatic update' option to ensure that anti-virus software is always up to date. • Scan for malware and change passwords if you suspect a cyberattack. • Limit access to USB sticks and don't allow them to be used in other devices, such as home computers. • Choose the most secure settings for your devices and software. **Keep mobile devices safe** • Think about the physical security of laptops, USB sticks, tablets and phones – don't leave them unattended. • Switch on PIN/password protection/fingerprint recognition. • Turn on storage encryption. • Set devices so they can be tracked, remotely wiped or remotely locked if lost or stolen. • Use the 'automatic update' option to ensure operating systems and apps are always up to date. • Replace devices if they are no longer supported by the manufacturer. **Passwords** • Make sure all laptops use encryption products that require a password to boot, particularly if they hold sensitive data. • Change manufacturer default passwords on all devices, including routers.
Laptop(s)	☐	
Tablet(s)	☐	
Mobile phone(s)	☐	
USB stick(s)	☐	
Broadband router(s)	☐	
Server(s)	☐	
Bring your own device(s) (i.e. use of personal devices)	☐	
Other (list below)	☐	

What systems and software do you use?		
Response		*Advice*
Operating software	☐	**Prevent malware damage** • Switch on the firewall included within the operating system. • Only install recognised software that is necessary to undertake the work of the organisation. • Only install apps from approved stores, such as Google Play or Apple App Store. • Use the 'automatic update' option to ensure operating systems, software and apps are always up to date. • Replace devices and software when they are no longer supported by the manufacturer or supplier. • Don't click on links within unsolicited emails. **Passwords** • Change default passwords on all software and apps. • If possible, use two factor authentication for important websites, e.g. banking. • Passwords need to be changed if you suspect a security breach. • Consider using a password manager. If you do, ensure the master password is a strong one. • Ensure staff can easily re-set their own passwords. • Disable user accounts when staff, volunteers, trustees leave the organisation. **Social Media** • Check security, privacy and location settings. • Review permissions for individual apps to check they are not accessing unnecessary features. • Be careful what you share and who you connect with, as information on social media could be used to commit identity theft and cybercrime. • Disable user accounts when staff, volunteers, trustees leave the organisation.
Networks	☐	
Email	☐	
Finance systems	☐	
Organisation's website	☐	
Cloud-based systems	☐	
Apps	☐	
Social media	☐	
Online donations or payments	☐	
Other software packages (list below)	☐	

<table>
<tr><th colspan="3">Who uses your IT equipment?</th></tr>
<tr><td>Response</td><td></td><td>Advice</td></tr>
<tr><td>Trustees</td><td>☐</td><td rowspan="5">Policies
Have information security policies in place. Examples of what these should cover include:-
Acceptable use of IT, e.g. email, internet
Passwords
Data handling
How to deal with a security breach
Remote/home working and ‘Bring your own device’, if appropriate.
Ensure all staff, volunteers and trustees are aware of the information security policies and adhere to them.
Provide information security training
Ensure all staff, volunteers and trustees are equipped with basic online safety and information security knowledge.
Ensure all staff, volunteers and trustees are trained to spot scams.
Ensure all staff, volunteers and trustees know how to recognise and report data breaches.
Provide regular updates and reminders to reinforce the training.
Passwords
Each individual should have an individual username and password to access the network.
Ensure users are deactivated when they cease to be involved with the organisation.
Choose strong passwords of at least twelve characters (preferably longer) and include capital letters, numbers and symbols
Avoid using family and pet names or common words like ‘passw0rd’.
Try using a phrase known to you (but not this one!) MAMl2g^coaS. (My Aunt Mary loves to go mountain climbing on a Sunday.)
You could use three random words, such as rainbowpositivekangaroo and then add numbers and symbols to make it even more secure.
Set up security questions that are hard to guess, so don’t use information that could be found on social media.
Do not reveal your password to anyone.</td></tr>
<tr><td>Paid staff</td><td>☐</td></tr>
<tr><td>Volunteers</td><td>☐</td></tr>
<tr><td>Service users</td><td>☐</td></tr>
<tr><td>General public</td><td>☐</td></tr>
</table>

		Avoid phishing attacks and scams
		• Don't click on links or attachments within unsolicited emails.
		• Only enter passwords or payment details into legitimate websites and ensure the web address includes the padlock symbol  .
		• Check for indicators that an email or website is not genuine:-
		  ○ unusual requests
		  ○ emails from organisations that you don't do business with
		  ○ poor spelling, grammar and punctuation
		  ○ low quality versions of recognisable logos
		  ○ requests for usernames, passwords or bank details
		  ○ imitation email addresses or web addresses (you can hover over the link to check)
		  ○ suggesting a sense of urgency
		  ○ not addressed to you by name
		  ○ if it sounds too good to be true…
		• If you have concerns, independently the check contact details or bank details.
		• Encourage people to report concerns.

Where is the IT used?		
Response		*Advice*
Office	☐	**Physical security** • Take steps to ensure the physical security of IT equipment to reduce the risk of unauthorised access, damage or theft. For example, door locks, security lighting, alarm systems, CCTV, visitor signing-in procedures, challenging unrecognised people on the premises. • Equipment used outside of the office or home needs more protection than if office-based. • Maintain a register of all IT equipment and who it has been allocated to. • Securely erase all data on devices before disposal. **Mobile Equipment** • Don't connect to public WiFi to access, or send, sensitive date – always use 3G, 4G or a Virtual Private Network (VPN). • Ensure the screen is not overlooked in order to protect security details and confidential information. • Do not leave devices unattended in public places.
Home	☐	
Other premises	☐	
Public places	☐	

<table>
<tr><th colspan="3">What data do you hold?</th></tr>
<tr><td>Response</td><td></td><td>Advice</td></tr>
<tr><td>Financial data</td><td>☐</td><td rowspan="3">Backup your data
Identify what devices hold your data.
Identify what essential data needs to be backed up.
Consider the different methods for backup.
Keep your backup secure and separate from your computer.
Consider using cloud services so the data is stored in a separate location.
Consider options for automatic backups.
Initiate anti-virus scans before saving backups.
Take <u>regular</u> backups of your important data and <u>test</u> they can be restored.
Keep your data secure
Ensure compliance with the General Data Protection Regulations (GDPR).
Review all processes involved as you collect, store, use, share and dispose of personal data.
Consider how sensitive, or confidential, the data you hold is and the impact of a security breach in terms of damage, or distress, to individuals, but also the impact on your reputation.
If storing sensitive or confidential data, it should be encrypted.
Have adequate information security policies in place.
If contracting cloud services, check the data security policy of your provider and consider where the data is held.</td></tr>
<tr><td>Sensitive personal data - HR data (trustees, staff, volunteers), service users, donors</td><td>☐</td></tr>
<tr><td>Commercial data</td><td>☐</td></tr>
</table>

How do you share data?		
Response		*Advice*
Secure email	☐	**Sharing data** • All data sharing must comply with the General Data Protection Regulations (GDPR). • Data should not be transferred to personal email accounts or personal cloud storage. • Secure email depends on the email address you are sending it from and to – if in doubt, check. • If documents must be sent via email, protect the document with a password and separately advise the recipient of the password. • File transfer, or file sharing, services enable you to password protect documents and make them available to the recipient to download for a specified period. • If using USBs or other portable media, ensure the data is encrypted and keep the device safe and secure. **Website** • Check the public information on your website. Could it be used to launch a phishing attack or scam your organisation?
Encrypted USB	☐	
File transfer services	☐	
Cloud services	☐	
Other	☐	

Who manages your IT systems?		
Response		*Advice*
Trustee	☐	**Administrator accounts** • Administrator accounts should have a separate log-in and not used for everyday use. • User access should be the lowest that is required to enable them to perform their role. **Outsourced IT providers** • Approach recommended or 'approved' IT providers and check their reputation, experience, qualifications and membership of a professional body. • Choose an IT provider with the skills and experience relevant to the technology you need supporting. • Consider a provider who is Cyber Essentials certified. • Have a Service Level Agreement in place. • Review the IT provider's security arrangements and policies.
Paid staff	☐	
Volunteer	☐	
Charity head office	☐	
External provider	☐	

What to do in the event of a cyberattack

You should have an internal policy or process in place that details how a cyber security breach should be dealt with, how it is reported to managers and / or trustees within your organisation and how it should be reported externally.

If you have purchased a cyber insurance policy, there may be a requirement to report a breach to the insurance company within a certain timeframe. This should be incorporated into your internal procedures.

If you think you have been the victim of a cybercrime, scan your systems and devices for malware and change all passwords, as soon as possible.

If you are the victim of a ransomware attack, do not pay the ransom. www.nomoreransom.org provides advice and information and decryption keys for some known types of ransomware.

How to Report Cybercrime

Personal data breaches

A personal data breach is where a security incident has affected the confidentiality, integrity or availability of personal data, i.e. whenever any personal data is lost, destroyed, corrupted or disclosed. For example, if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable because it has been encrypted by ransomware, or is accidentally lost or destroyed.

You should follow your internal data protection procedures and, in accordance with GDPR, notifiable breaches should be reported to the Information Commissioners Office within 72 hours on 0303 123 1113, or online at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Fraud and cybercrime

Fraud and cybercrime should be reported to the police national reporting centre, Action Fraud, on 0300 123 2040 (8am-8pm Mon-Fri).

If you are currently experiencing a live cyberattack, the Action Fraud number can be used 24 hours, alternatively contact Derbyshire Constabulary on 101.

Alternatively, Action Fraud have an online reporting tool to:-
Report Fraud, attempted fraud or cybercrime and receive a police crime reference number
Report phishing campaigns where you have not lost any money or exposed your personal details

If you or someone else is in immediate danger or risk of harm, dial 999.

If you think you may have compromised the safety of your bank details and/or have lost money due to fraudulent misuse of your cards/bank account, you should immediately contact your bank.

The Charities Commission requires charities to report serious incidents by emailing RSI@charitycommission.gsi.gov.uk . A serious incident is an adverse event, whether actual or alleged, which results in or risks significant:-

- harm to your charity's beneficiaries, staff, volunteers or others who come into contact with your charity through its work
- loss of your charity's money or assets
- damage to your charity's property
- harm to your charity's work or reputation.

If you have been the victim of cybercrime or fraud, identify the causes and take steps to rectify the issue and ensure it does not happen again.

Resources

Glossary

A glossary, to explain commonly used terminology, can be found on the Safer Derbyshire website at https://www.saferderbyshire.gov.uk/what-we-do/cyber-crime/cyber-crime.aspx

Cyber Security and Online Safety Advice

There is more detailed cyber security and online safety advice available on government-backed websites.

Organisation	Website
National Cyber Security Centre	https://www.ncsc.gov.uk/
Cyber Essentials	https://www.cyberessentials.ncsc.gov.uk/
Cyber Aware	https://www.cyberaware.gov.uk
Get Safe Online	https://www.getsafeonline.org/
Take Five to Stop Fraud	https://www.takefive-stopfraud.org.uk/
National Council for Voluntary Organisations	https://knowhownonprofit.org/how-to/how-to-secure-your-it-systems
Derbyshire Constabulary	https://www.derbyshire.police.uk/cybercrime

Cyber Security Assessments

There are free resources available to undertake comprehensive cyber security assessments to help you identify areas of information security risk within your organisation.

Resource	How to access it
Government-backed Cyber Essentials	https://www.cyberessentials.ncsc.gov.uk/
Information Commissioners Office Information Security Checklist	https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/information-security-checklist/
Scottish Council for Voluntary Organisations Digital Check Up	https://scvo.org.uk/digital/evolution/check-up
Fraud Advisory Panel Fraud Checklist	https://www.fraudadvisorypanel.org/wp-content/uploads/2018/03/Tackling-Charity-Fraud-Checklist-March2018-1.pdf
Derbyshire County Council Data Protection and Information Security Checklist	https://derbyshire.gov.uk/site-elements/documents/pdf/working-for-us/data/supplier-information-security-policy.pdf

Technical Support

There is a wealth of free technical information available online from reliable sources.

Topic	Organisation	Link
Cloud computing	National Cyber Security Centre	https://www.ncsc.gov.uk/guidance/cloud-security-collection
	Information Commissioners Office	https://ico.org.uk/your-data-matters/online/cloud-computing/
	National Council for Voluntary Organisations	https://knowhownonprofit.org/how-to/how-to-move-to-the-cloud
	Get Safe Online	https://www.getsafeonline.org/information-security/the-cloud/
Malware protection	Microsoft	https://support.microsoft.com/en-us/help/17228/windows-protect-my-pc-from-viruses
Mobile device security	Home Office	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/510735/Mobile_device_security_leaflet_240316_web.pdf
	National Cyber Security Centre	https://www.ncsc.gov.uk/guidance/10-steps-home-and-mobile-working
Passwords	National Cyber Security Centre	https://www.ncsc.gov.uk/guidance/helping-end-users-manage-their-passwords https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
Fraud	Charity Commission	https://www.gov.uk/guidance/protect-your-charity-from-fraud#cyber-fraud https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/654821/Chapter3.pdf
Safe computer disposal	Get Safe Online	https://www.getsafeonline.org/protecting-your-computer/safe-computer-disposal/
Backups	Get Safe Online	https://www.getsafeonline.org/protecting-your-computer/Backups/
	National Cyber Security Centre	https://www.ncsc.gov.uk/guidance/backing-your-data
Cyber security incident management	National Cyber Security Centre	https://www.ncsc.gov.uk/guidance/10-steps-incident-management
Online giving	Institute of Fundraising	https://www.institute-of-fundraising.org.uk/library/making-the-most-of-digital-donations/
Secure settings for devices	National Cyber Security Centre	https://www.ncsc.gov.uk/guidance/end-user-device-security
Virtual Private Network (VPN)	National Cyber Security Centre	https://www.ncsc.gov.uk/guidance/end-user-devices-vpns-1

Policies and Procedures

There are free resources available to help you develop information security policies.

Resource	**How to access it**
National Council for Voluntary Organisations	https://knowhownonprofit.org/organisation/operations/policies-and-procedures
Get Safe Online	https://www.getsafeonline.org/rules-guidelines-and-procedures/staff-policies/
NHS Digital	https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/information-security-guidance-for-health-and-care-organisations/information-security-policy-example-policy
Sans Institute	https://www.sans.org/security-resources/policies/

Training

In addition to the websites providing cyber security and online safety advice, there are free online e-learning courses and other resources available to enable you to upskill you and your staff / volunteers / trustees.

Organisation	**Link**
Open University	https://www.futurelearn.com/courses/introduction-to-cyber-security
Friends Against Scams	https://www.friendsagainstscams.org.uk/course.php/2/friends_against_scams_online_learning?jssCart=dc2403a16d7166ec84373d6560bf5e67
Take Five to Stop Fraud	https://takefive-stopfraud.org.uk/scam-academy/
Centre for the Protection of National Infrastructure	https://www.cpni.gov.uk/security-awareness-campaigns
Fraud Advisory Panel	https://www.fraudadvisorypanel.org/resources/cyber-fraud-e-learning-resource/ https://www.fraudadvisorypanel.org/resources/identity-fraud-e-learning-resource/
Information Commissioners Office	https://ico.org.uk/about-the-ico/news-and-events/events-and-webinars/cyber-security-webinar/

Procurement

Free Information and advice is available if your voluntary organisation decides to outsource your IT security.

Organisation	**Link**
Get Safe Online	https://www.getsafeonline.org/software/it-support/ https://www.getsafeonline.org/information-security/cyber-information-security-support/
Crown Commercial Service	https://ccsheretohelp.uk/sector/charities/
National Council for Voluntary Services	https://www.ncvo.org.uk/practical-support/trusted-suppliers
Scottish Council for Voluntary Services	https://charitycatalogue.com
tt exchange	https://www.tt-exchange.org/

General Data Protection Regulations (GDPR)

The Information Commissioner has produced specific GDPR guidance for charities and voluntary organisations, which is available at https://ico.org.uk/for-organisations/charity/

The ICO provide access to the Think Privacy Toolkit for Charities.

There is a dedicated helpline for charities and small businesses – tel: 0303 123 1113.

Cyber Liability Insurance

If you are considering cyber liability insurance, read the advice available from Get Safe Online to find out what to look for in a good policy - https://www.getsafeonline.org/rules-guidelines-and-procedures/cyber-liability-insurance/

Contact Details

Derbyshire Constabulary have experts who can provide voluntary organisations with tailored advice and information about improving your cyber security.

Tel: 0754 5100698

Email: Jodie.Nevin.17222@Derbyshire.PNN.Police.UK

@DerbyCyberBiz

Feedback

If you have any feedback or comments about this toolkit, please email community.safety@derbyshire.gov.uk