An introduction to

CYBER SECURITY

CYBER AWARE

skillsforcare

Local Government Association

The Care Provider ALLIANCE

NHS Digital

1. FOREWORD

Thank you for taking the time to read this guidance, which has been produced for Care Providers and for anyone else who would find it of assistance.

It was written by the Care Provider Alliance in collaboration with the Social Care Programme at NHS Digital, with significant contributions from many other agencies including the Home Office (Cyber Aware Team) and the National Cyber Security Centre. The guidance can be found on the Care Provider Alliance website.

For extra information about cyber security, the guidance includes links to web pages from Government approved organisations. They also contain important information about other areas such as: The Data Security and Protection Toolkit (replacing the existing Information Governance Toolkit April 2018) and GDPR (applies from 25th May 2018). Please see **'5. Resource Library'** for more details.

If you have feedback about the websites used in this guidance, please contact the organisation concerned.

2. TECHNOLOGY AND BENEFITS

There are fantastic benefits to embracing technology and working securely online in health and social care. Technology allows greater and faster information sharing, so we can improve the quality of care and support which we provide e.g. personalised care planning, transfers of care, viewing medications, etc. Individuals can fully participate and have better access to, and input into, their records.

However, as we use technology more, we must continue to do all we can to keep data safe and secure, ensuring that disruption to care and support at best is avoided or that any disruption is minimised.

The global ransomware attack in May 2017, which in the UK particularly affected the NHS, is a reminder to us all why it is worth taking the necessary precautions.

3. WHAT IS CYBER SECURITY?

Cyber security is the name for the safeguards taken to avoid or reduce any disruption from an attack on data, computers or mobile devices.

Cyber security covers not only safeguarding confidentiality and privacy, but also the availability and integrity of data, both of which are vital for the quality and safety of care.

Security breaches can occur when we use paper records, send information using fax machines and even verbally. However, the consequences of security breaches with digital information are potentially far more severe, as information can be distributed more easily and to a far wider audience.

Cyber-breaches are costly – in terms of expense, recovery time and through damage to reputation. In a Government Cyber Breaches Survey in 2017, 46% of businesses reported a cyber-breach or attack.

That is why cyber security is a high priority for business and why all staff must be aware of how to implement protective measures.

Individuals should also be aware of basic cyber security safeguards for personal use and when participating in the management and coordination of their care and support.

4. IMPROVING CYBER SECURITY

Cyber security is a constantly changing area and sometimes can seem quite confusing.

However, there are many effective and relatively simple steps that can be taken to protect information and protect you and your organisation.

Taking some simple actions and practising safe behaviours will reduce online threats.

The most important steps to improve online security are ensuring you:

a. MOVE AWAY FROM USING UNSUPPORTED SOFTWARE

This is when software e.g. operating systems such as Windows, apps, web browsers, etc. are no longer updated by the supplier. Although the software will continue to operate, it will no longer protect against online threats through updates or patching (a software update, often relates to improving security).

If a security weakness is discovered, software can be compromised and become vulnerable to a cyber-attack.

For benefits to be gained from up-to-date security measures, such as improved speed and efficiency, only use supported software on your systems and devices (see **b**.). If you must use unsupported software, ensure that you properly manage the risk by having a strong firewall and up-to-date anti-virus and/or anti-malware software (see **c**.).

For more information, please click here.

b. ALWAYS DOWNLOAD AND INSTALL THE LATEST SOFTWARE AND APP UPDATES

Software updates are designed to fix weaknesses in software and apps which could be used by hackers to attack your device. Installing them as soon as possible helps to keep your device secure.

You can set desktops, laptops, smartphones and tablets to automatically install software updates when an update is available. You can choose to install updates overnight whilst your device is plugged in, or you can set your device to automatically update when you are connected to Wi-Fi.

For more information, please click here.

c. RUN UP-TO-DATE ANTI-VIRUS SOFTWARE

Your computers, tablets and smartphones can easily become infected by small pieces of software known as malware. Common types include viruses or spyware and ransomware. To help prevent infection, install internet security software, like anti-virus and/or anti-malware on your devices and keep it up to date.

For more information, please click here.

d. USE STRONG PASSWORDS

Passwords should be easy to remember and difficult to guess. It's best not to use words such as your child's name, pet's name or your favourite sports team as this type of information might be easily viewed on your social media page e.g. Facebook.

Use 3 random words to create a strong password

Numbers and symbols can still be used but using three random words is the key to creating a strong password.

Use a strong, separate password for your email and other important accounts

This means if hackers steal your password for one of your less important accounts they cannot use it to access your most important ones such as your main email account. Hackers could potentially use your email to access many of your personal accounts and find out personal information, such as your bank details, address or date of birth, leaving you vulnerable to identity theft or fraud.

For your most important accounts, if it's available, you should use Two-Factor Authentication. This means involving a second step after entering your password e.g. providing a fingerprint, answering a security question, or entering a unique code sent to your device.

For more information, please click here.

Remember – always keep your passwords secret

e. DELETE SUSPICIOUS EMAILS AND AVOID CLICKING ON UNKNOWN ATTACHMENTS OR LINKS

Email is an excellent communication tool but is frequently used to deliver unwanted or unwelcome material, often referred to as 'spam' or 'junk' email. At best this is annoying and at worst it can be malicious, causing considerable harm to your computer and organisation.

Delete suspicious emails and do not click on links or open attachments in these emails before you delete them as they may contain fraudulent requests for information or contain links to viruses.

Do not respond to such 'phishing' emails (a scam where criminals typically send emails to thousands of people) even if they seem to come from a company or person you may know, because doing so can confirm the address is legitimate to the sender.

For more information, please click here.

f. BACK UP YOUR DATA

If your device is infected by a virus or accessed by a hacker, your data may be damaged, deleted, stolen or even held to ransom, which means you won't be able to access it.

You should therefore safeguard your most important data by backing up to a secure external hard drive or storage system based in the Cloud.

You should also ensure you regularly test your back-ups and, if you are saving confidential data off-site e.g. the Cloud, follow all appropriate data protection measures and government standards and guidance that relate to health and social care organisations.

For more information, please click here.

g. TRAIN YOUR STAFF TO BE CYBER AWARE

Make sure staff are trained to know the benefits of operating digitally, but are also aware of cyber security threats and how to deal with them. Due to the rapid development and changes in digital technology it is a good idea to add cyber security to your annual training plans/ matrix.

NHS Digital's Data Security Awareness Programme, in conjunction with Health Education England, includes Data Security Awareness Training which is for everyone working in health and care. It has been designed to inform, educate and upskill different groups of staff in data security and information sharing.

The Open University has developed a generic Introduction to Cyber Security course supported by the National Cyber Security Programme.

For more information, please click here.

h. MANAGE SECURITY RELATIONSHIPS WITH SUPPLIERS AND PARTNERS

As your organisation grows and works with more suppliers and partners, you become a link in one or more complex supply chains.

It is important to observe good practice (and in many cases, compliance) because vulnerabilities will place not only your own organisation at risk, but also others within the supply chain.

If you use third-party managed IT services, check your contracts and service level agreements, and ensure that whoever handles your systems and data has security controls in place.

One way to demonstrate that you have the security controls in place is to undertake a basic assessment and achieve your Cyber Essentials certificate. You can ask your suppliers to do the same.

For more information, please click here.

5. RESOURCE LIBRARY

The information below lists some of the organisations who offer advice to the public and businesses, including those in health and social care, about the best ways to protect devices and data.

Taking these actions will also be valuable with regards to the Department of Health guidance, Data Security and Protection for Health and Care Organisations, which outlines the steps expected from health and care organisations up to and beyond April 2018.

NHS Digital

NHS Digital is where you will find information about The Data Security and Protection Toolkit which will be replacing the existing Information Governance Toolkit in April 2018.

Good Practice Guides are also available as well as information about national systems for health and care, such as NHSmail.

NHS Digital also has a Data Security Centre which has live reporting on cyber security threats in health and care. By going to the website, anyone can sign up to receive updates on the latest threats. The aim is to help health and care organisations respond to cyber-attacks quickly and effectively to minimise impact.

The Information Governance Alliance can also be found on the NHS Digital website.

The Information Commissioner's Office (ICO)

The ICO is a UK independent body set up to uphold information rights, organisations' obligations and how to comply, including protecting personal information and providing access to official information.

This includes guidance for organisations about GDPR which will apply in the UK from the 25th May 2018.

Cyber Aware

The Cyber Aware website aims to influence businesses and individuals to adopt simple secure online behaviours to help protect themselves from cyber criminals. It is delivered by the Home Office alongside the National Cyber Security Centre, and funded by the National Cyber Security Programme in the Cabinet Office.

For further information about the Cyber Aware campaign or to find print-ready and digital communications materials visit the Cyber Aware toolkit or email cyberaware@homeoffice.x.gsi.gov.uk

Get Safe Online

The Get Safe Online website aims to provides comprehensive practical advice and resources on how to protect yourself and your business.

The site also provides advice on a wide range of topics including; Mobile Devices, Fraud, Identity Theft, Network and Computer Security, User Accounts, Business Security Plan's, Business Continuity & Disaster Recovery, etc.

There is also a Jargon Buster.

The National Cyber Security Centre (NCSC)

The NCSC site is the authority on cyber security and has some useful guidance and resources. The NCSC's main purpose is working together with organisations and businesses and individuals to reduce the cyber risk by improving cyber security and cyber resilience to ensure the UK is the safest place to live and do business online.

There is also a Glossary.

Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cybercrime where fraud can be reported if you have been scammed, defrauded or experienced cybercrime.

Report Fraud Online: www.actionfraud.police.uk/report_fraud
Telephone: 0300 123 204