Digital safety in Bite size

Who we are, what we do

- The employer-led workforce development body for adult social care in England.
- Largely funded by Department of Health and Social Care
- Lead on workforce, leadership and learning and development.
- Develop practical resources and provide support for the workforce including front line workers, Registered Managers and people in other leadership, management and strategic roles.

- Visit www.skillsforcare.org.uk

What we are coving today

- Cyber Security - What is it and how to make improvements
- Safe use of emails and sharing information digitally
- How to use your mobile phone safely including how to use WhatsApp at work
- Social media - Do’s and don’t

What is cyber security?

- ‘Cyber security’ is the name for the safeguards that has to be taken to avoid or reduce any disruption from an attack on data, computers or mobile devices.
- Cyber security covers not only 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.
- 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
- Everyone should also be aware of basic cyber security safeguards for personal use and when working in social care
- All staff should have annual Cyber Security training

Improving Cyber security

- Cyber security is a constantly changing area and sometimes can seem quite confusing.
- Relatively simple but effective steps that can be taken to protect information and protect you and the organisation that you for.
- Steps include not using unsupported software, have an updated antivirus checks and have data backed up.
- Ensure that software and apps are updated automatically. 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.

Sharing Care Records

- You should be mindful of handling people's information securely, but you need to make sure that you are using the communication available to you (phone, email etc) to clearly and quickly communicate with your local GPs and other contacts
- Because health and care information is very sensitive, we must make sure that it is protected. This is the case no matter how we send information. Whether using fax, post, email or the phone.
- Email containing health and care information sent to and from health and social care organisations **must** meet the Secure Email Standard (DCB1596). This includes NHS mail

Using email safely at work

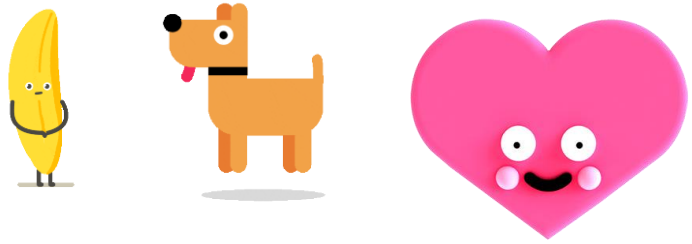
- Email is an excellent communication tool but is frequently used to deliver unwanted or unwelcome material; spam or junk email. This is annoying and can be malicious, causing considerable harm to your computer and organisation.
- Delete suspicious emails. Do not click on links or open attachments in these fake emails as they may contain fraudulent requests for information or contain links to viruses.
- Hover your mouse over email senders or links to see if the URL or email address looks valid. If it doesn't appear to match up with the sender or website it wants you to visit, don't click on it or respond to it
- Don't log into an account via a link provided in an email. If you are being asked to log into an account, instead of clicking on the link provided, go to the site directly by typing the web address into your browser. Then log in from there

Using email safely at work

- A phishing email is a scam where criminals typically send fake emails. Do not respond to them. Responding can confirm that your address is legitimate to the sender. If you are not sure if an email is genuine contact the sender on a phone number you know to be correct.
- You can forward any suspicious email to report@phishing.gov.uk
- Delete any suspicious emails
- Double check email address; especially if you are sending something sensitive.
- Use the BBC filed when sending an email to multiple of people

Use Strong Passwords

- Recent analysis outlined by the National Cyber Security Centre found that 23.2 million victim accounts worldwide used 123456 as a password!
- To create a strong password use 3 random words that you are going to remember.
- Don’t use words such as your child’s name, pet’s name, or your favourite sports team. This type of information might be easily viewed on your social media page.
- Numbers and symbols can still be used but it is advised that three random words is the key to creating a strong password.

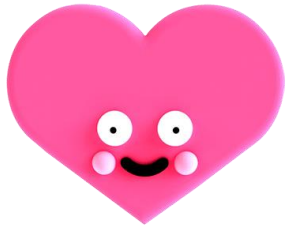


Bananadogheart

Use Strong Passwords

- Always keep your passwords secret
- Do not share your password (or keep it written down)
- You are responsible for your own password
- Use different password for different systems – if someone does get hold of your password it is only one system that they can get into.
- Be aware of who is around you when using your password
- Always log out when you have finished using a system or lock the screen (Control – Alt – Delete)





Bananadogheart



Using your mobile phone for work

- Use screen-lock protection – Make sure mobile devices are locked when not in use, for example with a suitably complex PIN or built-in fingerprint scanner.
- Make sure lost and stolen devices can be tracked, locked, or wiped – Install ‘find my phone’ app
- Keep devices and apps up to date – Just like a ‘desktop’ computer mobile devices and apps need to be kept up to date to ensure that critical security updates are applied.
- Only connect to trusted Wi-Fi networks – when you use public Wi-Fi hotspots there is no way to easily find out who controls the hotspot
- If you are useing your own mobile for work to access and manage data ensure that your employer use the National Cyber Security A Bring Your Own Device (BYOD) approach.

Safe use of WhatsApp

- WhatsApp is protected by ‘end to end encryption’, which means that no one, not even WhatsApp, can read or listen to messages sent between users.
- WhatsApp has an additional security function called ‘two-step verification’. This means to open WhatsApp you will be required to enter another password
- Keeping WhatsApp updated - Keeping the App updated is crucial to the security of the information held on WhatsApp and its functionality
- WhatsApp has adjustable controls to help protect yourself, these features are important to anyone working in the adult social care sector. It includes controlling who can see your information, what you see and with whom you interact and what you share

Safe use of WhatsApp

- Any message created with a contact will mean they have full access to the conversation and any attachments sent. This means they can re-share this with others on and off WhatsApp.
- When using WhatsApp for work purposes you will need to ensure your data protection and protocols/ procedures are in place and are understood. – Ask your manager if you are not sure
- If you do discuss the people you care for, use initials rather than names.
- *As much as possible* limit the use of people's personal/confidential information.
- Ensure you don't mix up contacts, especially if you have similar names stored in your address book

Safe use of WhatsApp

- Be careful when sharing images in WhatsApp group, all group members will have that photograph automatically stored on their personal device gallery. This means these photographs will be mixed in with the photographs you have taken on your mobile phone.
- Images of Individuals who are in receipt of care and support, their relatives and visitors must NOT be shared via WhatsApp unless written consent has been given by those individuals
- Turning off notifications -. WhatsApp will automatically alert you on messages in a WhatsApp group. These conversations may continue beyond ordinary working hours - It is important to balance this with your own mental wellbeing, allowing yourself mental space away from work.

Safe use of WhatsApp

- A guide to WhatsApp at www.skillsforcare.org.uk/whatsapp-guide
- Staying safe on WhatsApp https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp
- How to use two-step verification on WhatsApp https://www.youtube.com/watch?v=H7ebvsiohFo
- How to stop saving WhatsApp media to your phone's gallery https://faq.whatsapp.com/android/how-to-stop-saving-whatsapp-media-to-your-phones-gallery
- How to turn off your notifications https://www.youtube.com/watch?v=E5qfckF6h9o

What is Social media?

Social media

- By Social Media we mean Facebook, Twitter, Instagram, LinkedIn, and Snapchat
- You can professionally learn lots from social media by looking at what people are saying around a particular topic, best practice and sharing your thoughts and opinions.
- You can make useful professional connections and networks with other people
- Does you organisation use social media to recruit, blog, posts about your service – can you get involved?

Social Media

- **Think before you post**. Assume that what you post could be shared and read by anyone.
- **Think about who can see what you share** and manage your privacy settings accordingly. Remember that privacy settings cannot guarantee that something you post will not be publicly visible.
- **Do not post information which could identify a service user unless you have their permission (in writing).** Remember to consider if the person has capacity to make this decision.
- **Maintain appropriate professional boundaries** Avoid adding service users and their family/friends as “friends” and commenting on their posts.
- **Do not share confidential information** – Remember your confidentiality training

Social Media

- **Do not post inappropriate or offensive material**. Use your professional judgement in deciding whether to post or share something. Consider if your profile identify your employer
- **Do not make negative comments on social media about your employer –** If you have a a grievance or concern about something associated with work discuss it with to your line manager
- **Consider if any post or comment could be considered as bullying and harassment of your colleagues**
- **Follow your employer's social media policy**. Does it allow limited private use in the workplace; are you clear about what this means in practice?
- When in doubt, **get advice**.

Social Media

What is next…

Your action plan

- If you have not already had cyber security training in the last 12 months ask you employer about it. They can access free training on the National Cyber security centre
- If your service is not using NHS mail – speak to your manager to ensure that if you are sending care records that your emails are secure.
- Install the ‘find my phone’ app
- If you are using your own mobile at work speak to your manager about the Bring Your Own Device (BYOD) approach.
- Make sure that you use WhatsApp safely – turn off storing photos shared in the gallery
- Ask your employer about their social media policy

More information

- Introduction to Cyber security https://www.skillsforcare.org.uk/Documents/Topics/Digital-working/An-Introduction-to-Cyber-Security.pdf
- Guidance on social media https://www.hcpc-uk.org/globalassets/resources/guidance/guidance-on-social-media.pdf?v=637106443130000000
- Guidance on using social media responsibly https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/social-media-guidance.pdf
- Using social media to promote your service
- https://www.ncsc.gov.uk/guidance/byod-executive-summary
- Digital Social Care https://www.digitalsocialcare.co.uk/
- www.skillsforcare.org.uk/digital

Additional Free training

05
Nov 2020

Start Here – the Policies and Procedures You Need for Better Data Security

Date: Thursday 5 November 2020
Location: Webinar

Read more ›

10
Nov 2020

Start Here – Protect Your IT Systems and Devices From Cyber Threats

Date: Tuesday 10 November 2020
Location: Webinar

Read more ›

12
Nov 2020

Start Here – the Data Protection and Cyber Security Training Your Staff Need

Date: Thursday 12 November 2020
Location: Webinar

Read more ›

https://www.digitalsocialcare.co.uk/events /

Stay connected…

For further information or support, visit the Skills for Care website at:
www.skillsforcare.org.uk/

For updates, sign up to our newsletter at:
www.skillsforcare.org.uk/enews

Pia.Rathje-Burton@skillsforcare.org.uk

@PiaRathje

@sfc_LondonSE

@skillsforcare