DATA AND CYBER SECURITY TRAINING MATERIALS:

Their suitability for social care staff

June 2020

IN THE KNOW

Digital Social Care

Next Page >

WHO IS THIS GUIDANCE FOR AND WHY IS TRAINING AND DEVELOPMENT NEEDED?

This guidance is for adult social care providers who source training and development opportunities for themselves or their staff. Technology is increasingly being used in the sector, including by providers, to support the planning and delivery of adult social care and support. All organisations need to keep their data and systems safe and ensure that their staff are fully aware of the dangers presented by data and cyber security threats. This guidance makes suggestions as to how you might do this. **It is organised in three sections, linked to the training pathway:**

Background reading – information sources > **Raise awareness – materials** > **Source training courses**

Data and cyber security is a major issue for all organisations. It is about safeguarding confidentiality and privacy of people's personal data as well as the availability and integrity of that data, all of which are vital to ensure the quality and safety of care. Data and cyber security should be included in your overall training plans alongside other keys areas such as moving and handling, health and safety and safeguarding.

Cyber security is the safeguards taken to avoid or reduce any disruption from a cyber attack on data, computers or mobile devices. This is not just about technology, but also about individuals understanding their responsibilities and organisations having appropriately trained staff. Cyber attacks are increasing in number and sophistication, however, if staff are well trained, procedures are in place and regularly tested, and technical defences in use (e.g. a firewall or antivirus software) then the risk of cyber attack being successful is reduced.

BACKGROUND READING – INFORMATION SOURCES

Digital Social Care

The key information source for social care providers is **Digital Social Care.** This site provides sector-specific information, guidance and resources, and includes an **introduction to cyber security.**

There are also UK government and other trusted sources available, which are listed at **Appendix 1: Trusted sources of information.** To note, cyber security in particular is a rapidly evolving area and it is recommended that you refresh your knowledge regularly.

< Previous Page

Next Page >

RAISE AWARENESS – MATERIALS

Making staff aware of the need for data and cyber security, through a variety of methods, should be a major component of your training programme. Awareness is needed by all types of workers from care staff to managers and office staff.

Materials to promote awareness

There is a wide range of resources, including posters, leaflets, stickers, videos and PowerPoint slides, that are freely available for you to use. Examples of these are included at **Appendix 2: Materials to promote awareness.** However, do please note that this list is not exhaustive and new materials will become available all the time.

Ways to increase data and cyber security awareness

Think about your overall approach: good materials used badly will not raise awareness. **Some useful tips are:**

- Focus on the most important areas and target key staff
- Ask your staff – what worries them?
- Repeat key messages in different ways, e.g. through posters and videos
- Make it visual by using pictures and posters
- Use your IT system to convey key messages, such as via 'pop ups' on log in
- Make data and cyber security a key component of any induction process
- Focus on a monthly theme

Ensure your approach includes proactive activities in addition to those which monitor practice.

SOURCE TRAINING COURSES

Data and cyber security training will be needed across your organisation and should cover board members, owners, managers, office staff and frontline care workers.

Areas training should cover

Suggestions for subject areas that training should cover are provided below, together with the types of staff for whom that training might apply. This includes recommendations for the organisation's 'data protection champion' i.e. the person within the organisation who is responsible for the protection of data and will champion the principles of good data protection. Skills for Care have developed a **data protection champion job description.**

Area of training	Types of staff/staff role
Data and cyber security awareness and good practice, including: • Data protection • Data quality • Record keeping • Data security • Confidentiality • Rights of individuals under GDPR including subject access requests	All (board members, managers, office staff, frontline care workers)
Physical security including paper records and files	All
Email – good practice	Those who use email
Passwords – good practice	Those who need password(s) to access company systems
Preventing data and cyber security threats including awareness of potential threats, and reporting incidents (data breaches) including near misses	All
Safe use of company computers and systems, and removeable media (e.g. memory sticks)	Those who need to use a computer to do their work
Safe use of **company** laptops/phones/tablets including when out and about	Those who are provided with company devices

SOURCE TRAINING COURSES

Safe use of personal mobile phones to carry out company business	Those who use generic systems such as WhatsApp for work or who use an App to view or update care records using their own phones. Those who access company email and/or documents or systems from their own devices.
Data Security and Protection Toolkit	Data protection champion, managers
Business continuity planning and data protection impact assessments (DPIA)	Data protection champion, managers
Company IT infrastructure, including: • Operating system updates • Backups • Firewalls • Anti-virus software installation/updates • Network management (if a network of computers is in place)	Internal IT support. If the organisation does not have internal IT support, then these tasks may be the responsibility of an external IT support company. If there is no IT support then the data protection champion or manager may require training.
How to ensure secure use of company computers, laptops, tablets, phones, including: • Encryption • PINs or operating system passwords • Two factor authentication • Remote tracking and wiping of mobile devices • Limiting downloads to verified software or Apps	As above
Company systems, including: • Software updates • Setting up and removing separate user accounts • Control of who accesses which parts of systems	As above

SOURCE TRAINING COURSES

Analyse training needs and decide on training methodology

The training needed depends on role and function and the extent to which technology is used in communicating, storing and manipulating data. We suggest that organisation-wide data security and protection training needs analysis is undertaken annually. A training needs analysis (TNA) is a means of identifying existing training levels for your staff and assessing whether that is enough or more training needs to be provided.

You can use the following method to conduct your analysis:

1. Assess what training is already in place in your organisation for all staff. This will act as your baseline. You may have nothing in place, which gives you a clean slate to implement training.
2. Identify the scope – who should be included and excluded e.g. maternity /paternity, long term sick and agency staff.
3. Identify which staff will need a higher level of knowledge around data security and protection than others (see above). For instance, the data protection champion or senior staff who often handle and make decisions about personal data. Also consider if you would need to provide more training for members of staff who use computers or mobile devices during their work compared to any staff whose work is completely paper based.
4. Make a note of each of these steps and ensure that each decision is signed off by the necessary person in your organisation as this will be evidence for your TNA.

Once you have identified your training needs, you should consider methodology. There are two key questions here:

- Do we want an off-the-peg package/course or bespoke training?
- How do we want the training to be delivered? As a rule of thumb eLearning is best for learning that needs repeating (e.g. at induction and at annual updates). However, if most staff do not have access to computers then 'classroom' learning may be more effective.

SOURCE TRAINING COURSES

Choosing a training provider

At the time of writing, choices for sector-specific training are limited. Skills for Care, the workforce body for the social care sector, recognise this as a gap and are currently working with partners to address this to ensure the sector has access to assured, good quality training.

It is recommended that you select UK-based, government approved, and / or sector-specific training providers. The following routes to finding a provider are recommended.

Route	Notes
Your local CCG or council	CCGs, health trusts and councils will have training in place for their health and care staff and it may be worth approaching them to see if these courses can be accessed by your organisation. This would be either through recommendations for the external training providers that they use, or via their internal training provision's existing courses.
Local police	Local police may offer awareness training workshops and visits to check your organisation's arrangements for data and cyber security.
The National Cyber Security Centre	The National Cyber Security Centre (NCSC) lists providers accredited by GCHQ **here.** Relevant providers here will be listed under the "Awareness Level Courses" section.
Digital Social Care	Digital social care signposts to free online training courses **here.**
Your care management system software supplier	Your existing software supplier may provide training in how to use your software safely and securely.
Specialist social care training providers	Some specialist social care training providers offer GDPR training. When we reviewed the courses on offer from specialist social care training providers, we could not find any offering training on cyber security.
Other commercial companies	The recruitment company Reed lists many online cyber security courses costing £50 or less **here.** Courses range in duration from one hour up to 8 hours or more.

SOURCE TRAINING COURSES

Whichever route is taken, it will be important to ensure that the training provider has the following:

- Knowledge of the sector and the practical application of data protection legislation
- Information about how your organisation operates including policies in place
- Knowledge and experience in data and cyber security
- Experience in how to deliver effective training

Seek out references from previous customers and/or ask colleagues in similar organisations for recommendations.

Free cyber security training courses

Provider	Course/s	Suitable for	Notes
National Cyber Security Centre	Top tips for staff	All who use computers and phones for work purposes	Free online course that's easy-to-use and takes less than 30 minutes to complete. Not sector-specific, but good generic advice on how to stay safe. An excellent quiz at the end.
eLearning for Healthcare at Health Education England	Data Security Awareness – Level 1	All including frontline care workers	Free online course with 8 modules. The language and examples are mainly NHS-based and the style is a bit clunky, but the course provides basics including for frontline care workers. Some guidance will be needed to ensure people understand this course is designed primarily for NHS staff and to only select the modules relevant to them. For example, the module on Freedom of Information Requests is not relevant to social care, and the module The Principles of Data Protection is only likely to be relevant to data protection champions. A good eAssessment at the end.

SOURCE TRAINING COURSES

FutureLearn at the Open University	Introduction to Cyber Security	Data protection champion, managers and office staff	Free online training that is accredited by GCHQ. Online 8 short modules with self-study and tests per module, to help you understand online security and to protect your digital life. The course introduces concepts like malware, viruses, trojans, network security, cryptography, identity theft, and risk management.
BT Skills for Tomorrow	• Keeping your personal data safe • Being safe online • Keeping your device safe • Improve your online business security	All including those very new to computers, through to the data protection champion	Free online courses. Not sector-specific but clear structured lessons from how to create strong passwords through to securing employee devices and networks. Technical aspects are presented in accessible language. Whilst these aspects are not covered in depth, there are good prompts as to what you need to think about. Each module has tests to check your knowledge.

Digital Social Care is a dedicated space to provide advice and support to the sector on technology and data protection. It is run by social care providers for social care providers.

This guidance has been written as part of a wider programme supporting the delivery of the National Cyber Security Strategy across adult social care services. This programme, which is led by Digital Social Care, the Local Government Association, NHS Digital and NHSX, works to develop practical solutions to the data and cyber security challenges faced by adult social care providers in England.

This guidance has been published on behalf of Digital Social Care by the Registered Nursing Home Association. It may be copied freely for use by adult social care providers but it may not be used or adapted for any commercial purpose without the prior written consent of the copyright holders.

APPENDIX 1 – TRUSTED SOURCES OF INFORMATION

Digital Social Care

Has a range of adult social care specific **resources** available on the **website.** These include a helpful **introduction to cyber security** and information about how to complete the **Data Security and Protection toolkit**.

The National Cyber Security Centre

The National Cyber Security Centre (NCSC) is the government's specialist cyber security agency set up support the most critical organisations in the UK, the wider public sector, and industry as well as the general public. When incidents do occur, NCSC provides effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future. The NCSC provides training, guidance and advice relevant to small businesses, including the excellent **Small Business Guide: Cyber Security** and more in depth guidance on how organisations can protect themselves in cyberspace, including **Ten steps to Cyber Security**. Detailed research, advice and guidance is available on a wide range of topics here: **https://www.ncsc.gov.uk/section/advice-guidance/all-topics**

The Information Commissioner's Office

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. The ICO provides resources and support to improve and promote information rights practices in organisations, including detailed information about GDPR and the Data Protection Act here: **https://ico.org.uk/for-organisations/**

Cyber Essentials

Cyber Essentials is a government-backed scheme to help organisations protect themselves against common online threats. Organisations can get certification at two levels: Cyber Essentials, which is a self assessment option, and Cyber Essentials Plus. The Cyber Essentials website has some straightforward advice on cyber security and some useful checklists at: **https://www.cyberessentials.ncsc.gov.uk/advice/**

Get Safe Online

Get Safe Online is a UK public private sector partnership supported by the government, which provides a wealth of free expert advice and resources to help people and organisations stay safe online. Advice for businesses is available at **https://www.getsafeonline.org/business/**

Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cyber crime. Should you fall victim, you should report it to Action Fraud by visiting their website or calling **0300 123 2040**. The website also features warnings about emerging scams, helping to keep you one step ahead.

APPENDIX 2 – MATERIALS TO PROMOTE AWARENESS

We have looked to identify a range of resources that are available for you to use, but this list is not exhaustive and new materials will become available all the time.

NHS

The NHS has run a campaign called 'Keep I.T. confidential' and has identified a range of materials that can be used by NHS organisations and others as part of the campaign. **https://keepitconfidential.nhs.uk/campaign/**

The National Cyber Security Centre

The National Cyber Security Centre (NCSC) is the government's specialist cyber security agency. NCSC have a range of materials available including a Stay safe onlin' infographic that is free and easy to access at: **https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available**. They also provide a range of guidance documents including the End User Guide available at: **https://www.ncsc.gov.uk/collection/end-user-device-security**

The Information Commissioner's Office

The Information Commissioner's Office (ICO) has a range of free posters and stickers to download and print that can help promote awareness of cyber security that are available here: **https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/**

Get Safe Online

Get Safe Online have a range of resources that can be used for awareness raising, including leaflets, posters, PowerPoint presentations, audio reconstructions and videos at: **https://www.getsafeonline.org/business/resources/**

Commercial organisations

There are a number of commercial organisations that appear to provide free materials (sometimes in exchange for your company details, presumably in return for a possible business opportunity). They are fairly easy to find using a search engine and a topic such as 'Free cyber security posters UK'. For staff who use email, InfoSec provide a series of posters here (without asking for any of your details): **https://resources.infosecinstitute.com/celebrate-cyber-security-awareness-month-with-free-training-resources/#gref**