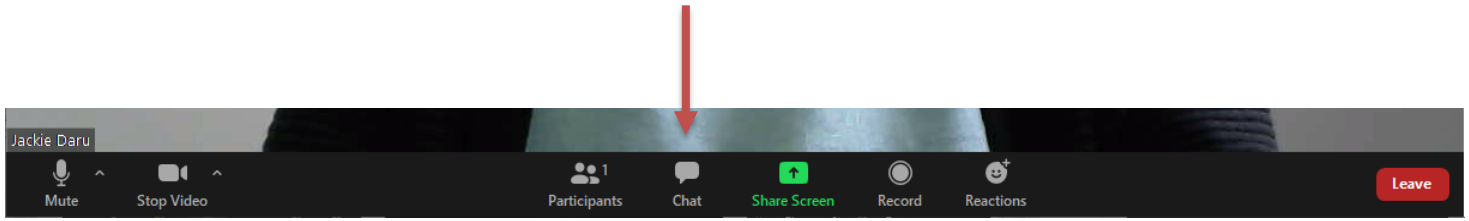
Start here – the data protection and cyber security training your staff need Welcome

- This webinar is being recorded for others to watch
- Attendees are on mute
- Please use the Chat function to ask questions. This is monitored by facilitators



- On a phone, tap the screen to see the controls – choose More and then Chat
- There may be questions that we can't answer – if so we will park these and come back to you
- This webinar will last no longer than 45 minutes

OXFORD BROOKES UNIVERSITY

Our approach

- No jargon
- No assumptions
- Want to give you a succinct, digestible amount of information
- Signposting at the end to more information and help

‘Start here’ programme of webinars

- How to register on the Data Security and Protection Toolkit (DSPT)
- What you need to know about data security
- The policies and procedures you need for better security
- The data protection and cyber security training your staff need
- Protect your IT systems and devices from cyber threats

- To sign up for live webinars, go to: https://www.digitalsocialcare.co.uk/events/

ipc institute of public care

Driving improvement and innovation in care

Start here – the data protection and cyber security training your staff need

OXFORD BROOKES UNIVERSITY

http://ipc.brookes.ac.uk

What we'll be covering in this webinar

- The Data Security and Protection Toolkit (DSPT) – what is it and why use it?
- The Who
  - The importance of data protection and cyber security training for all staff
  - Why your business needs a suitably trained Data Security and Protection Lead
- The What
  - From basic induction training to taking overall responsibility, depending on the staff role
- The How
  - How to carry out a training needs analysis for all staff
  - How to find the right training materials and providers for your needs

- Your questions
- Next steps and further support
- Where to find help
- Useful links

Data Security and Protection Toolkit (DSPT) – what is it and why use it?

- The DSPT is a really helpful guide and self-assessment tool for data security in social care
- It will help you keep people's confidential information safe
- It will help protect your business from the risk of being fined for a data breach and from the disruption of a cyberattack
- The DSPT will demonstrate compliance with CQC requirements
- It's what local councils and CCGs will expect you to have
- The DSPT will be your passport to shared care records with health services, enabling you to be part of a truly joined up care network with the interests of the people you support and care for at the centre of it

Data security and protection - Knowing your responsibilities

OXFORD BROOKES UNIVERSITY

What the DSPT questions ask

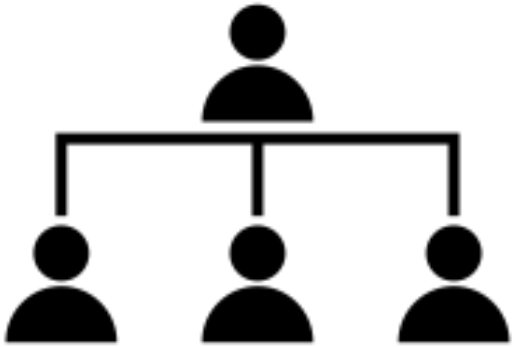
- **Who has responsibility for data security and protection and how has this responsibility been formally assigned?**

Who has responsibility for what?

Who leads data security?

- You need a Data Security and Protection Lead
- For small businesses this may be the owner
- Usually incorporated into someone's role but has additional skills and knowledge
- Elements of the role can be delegated
- Whoever it is they must be named, and it must be recorded - perhaps in their job description

Who has overall responsibility?



Data Security and Protection Lead

The lead person in your business for your data security and protection work:

- **Ensures individual's personal data rights are upheld**
- **Monitors information handling to ensure compliance with law**
- **Defines data protection policies and procedures**
- **Understands and completes the Data Security and Protection Toolkit, annually**
- **Champions good data protection practice**
- **Has good knowledge and appropriate skills around data security and protection**

Data Security and Protection - Specialist Support Roles

Data Protection Officer (DPO)

- Under legislation (GDPR) certain types of organisations must appoint a DPO
- For social care providers this is likely to only apply to large multi-site organisations

Caldicott Guardian

- The Caldicott Guardian is a senior person who is responsible for protecting the confidentiality of people's health and care information and making sure that it is used properly
- It is mandatory for NHS and all local authorities providing social services to have a Caldicott Guardian

What the DSPT questions ask

- **Do all employment contracts, and volunteer agreements, contain data security requirements?**

Clauses in contracts and agreements must reference data security

Draft staff contract clause

- During or after your employment with us, you must not disclose any trade secrets or any information of a confidential or sensitive nature about:

1. insert organisation name here; or
2. any of our service users; or
3. any of our employees.

- There is an exception if you need to share this information as part of your job or if you are made to by law.
- It is the responsibility of all staff to ensure data security. You will be responsible for the confidentiality, integrity and availability of all data which you have access to in the course of your work.

Further information and guidance

- Data security and protection responsibilities and specialised roles: https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/
- Information on the role of the Data Security and Protection Lead: https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/04/3.-Data-Security-and-Protection-Responsibilities-v5.pdf
- Example staff contract clause available from Digital Social Care: https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/

Staff training

What the DSPT questions ask

- Does your organisation have an induction process that covers data security and protection, and cyber security?
- Has a training needs analysis covering data security and protection, and cyber security, been completed in the last 12 months?
- Have the people with responsibility for data security and protection received training suitable for their role?
- Have at least 95% of people in your organisation completed training on data security and protection, and cyber security, within the last 12 months?

Induction training

Induction training should cover

- The importance of data security in the care system
- The National Data Guardian's data security standards, relating to personal responsibility
- The applicable laws (GDPR, etc) knowing when and how to share and not to share
- Physical security
- How to protect information
- Knowing how to spot and report data security breaches and incidents

- Understanding safe use of social media and email
- The dangers of malicious software

Training needs analysis

"A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across your organisation"

Your organisation's training needs analysis should identify the level of training required by your staff and should be reviewed annually

Training needs analysis
Where to start?

What training is already in place? This is your baseline

Scope. Who needs to be included? Do you have agency staff for example?

Who needs what? All staff will require some training but which staff will need additional or in-depth training?

Make a note of the steps you work through, this will evidence your Training Needs Analysis

Training needs analysis
All staff (example)

Area of training	Types of staff	Staff member name
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 Frontline Care Staff Office Staff Managers Board members	
Physical security including paper records and files	All	
Preventing data and cyber security threats including awareness of potential threats, and reporting incidents (data breaches) including near misses	All	

Training needs analysis
Additional training (example)

Area of training	Types of staff and roles
Email good practice	Staff who use email
Password good practice	Staff using passwords to access company systems
Safe use of removable media (memory sticks) with company computers	Staff using computers to do their work
Safe use of company laptops, tablets and phones	Staff provided with company devices
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 care records using their own phones. Those who access company email and/or documents or systems from their own devices.

Training staff with responsibility for data security and protection

- Your Training Needs Analysis will identify the people with responsibility for data security and protection. It is pivotal that they receive appropriate training
- Training in the content of the Data Security and Protection Toolkit as a minimum for your Data Security and Protection Lead
- Decide which functions will be covered by your Data Security and Protection Lead and which will be ‘out-sourced’ to IT supplier/support

Training staff with responsibility for data security and protection

Training required for your Data Security and Protection Lead

Area of training	Type of staff and roles
DSPT	Data Security and Protection Lead, managers
Business continuity planning and data protection impact assessments (DPIA)	Data Security and Protection Lead, managers
Software updates	Data Security and Protection Lead, managers

Training staff with responsibility for data security and protection

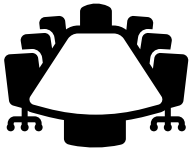
Area of training	Type of staff and roles
IT infrastructure, including: Operating system updates • Backups • Firewalls • Anti-virus software installation/updates • Network management (if a network of computers is in place)	Internal or external IT support. If there is no IT support then the Data Security and Protection Lead or manager may require training
Secure use of company hardware: • Encryption • PINs and two factor authentication • Remote tracking/wiping of mobile devices • Limiting downloads to verified software	As above
Software updates Setting up user accounts and control of access to which parts of systems	As above

Annual training standard – the 95%

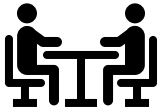
- Your Training Needs Analysis identifies who handles personal data, and therefore who needs training annually
- You must keep records to identify possible gaps if staff leave and timings for annual refresher training
- Records of who have completed what training is essential so you know 95% of staff have been trained
- Training can be delivered in a variety of ways and sourced dependent on how specialist the subject matter

Annual training standard - Ways to train

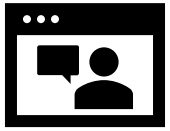
- Induction training



- Discussions in team meetings



- E-learning – can be useful for refresher training



- Formal training

- Specialist training, e.g. from a care management software supplier

Annual training standard - Sources of training

- Digital Social Care
- Local NHS CCG
- Local authority
- The National Cyber Security Centre
- Your care management software supplier
- Specialist social care training providers

You must record exactly what training staff have completed and when

Further information and guidance – training resources for staff

- National Cyber Security Centre new cyber security training for staff available via: https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available
- Induction and refresher training for staff – new videos coming from Skills for Care / Digital Social Care expected November 2020
- An 'Introduction to Information Sharing for Staff' available from Digital Social Care: https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/06/An-Introduction-to-Information-Sharing-for-Staff-v.3.pdf
- National Care Forum has 'crib sheets' on email and messaging etc: https://www.nationalcareforum.org.uk/digital-enabling-to-help-get-online/

Further information and guidance

- Guidance on training, including sources of free online data and cyber security training: https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/
- Recommended training for the Data Security and Protection Lead: https://www.e-lfh.org.uk/programmes/data-security-awareness/

Questions?

‘Start here’ programme of webinars

- How to register on the Data Security and Protection Toolkit (DSPT)
- What you need to know about data security
- The policies and procedures you need for better security
- The data protection and cyber security training your staff need
- Protect your IT systems and devices from cyber threats
- To sign up for live webinars, go to: https://www.digitalsocialcare.co.uk/events/

Further support

- From January 2021, your region/local area will be supporting providers to complete the Toolkit through things like:
  - Webinars
  - Interactive online workshops
  - 1:1 support
  - Peer support

- To find out what's happening in your area, go to Digital Social Care https://www.digitalsocialcare.co.uk/

There is help out there

For help with registration on the Data Security and Protection Toolkit (DSPT)	For further information about data and cyber security in social care
NHS Digital DSPT Helpdesk in Exeter Telephone 0300 303 4034 Or Email exeter.helpdesk@nhs.net	Digital Social Care www.digitalsocialcare.co.uk Digital Social Care helpline 0208 133 3430 (Monday – Friday, 9.00-17.00) or Email help@digitalsocialcare.co.uk

Thank you for attending/watching this webinar

- Let us know what you think by completing the very short survey at the end of this webinar
- Please visit Digital Social Care for further information and to catch up on all of the 'Start here' programme of webinars:
- https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/data-security-and-protection-toolkit/getting-started-with-the-data-security-protection-toolkit-webinars/
- A copy of these slides and action plan will be available here: https://ipc.brookes.ac.uk/events/data_security.html
- Comments or questions to Jackie Daru jdaru@brookes.ac.uk