Staffing and Roles

DSPT
Better security.
Better care.

Kent County Council & Kent Integrated Care Alliance

DSPT@kent.gov.uk

September 2021

KiCA
KENT INTEGRATED
CARE ALLIANCE

Kent
County
Council
kent.gov.uk

Better Security, Better Care

- National programme funded by NHSX

- Its overall aim is to help make sure adult social care providers have good data and cyber security in place

- By helping care providers to register on and complete the Data Security and Protection Toolkit (DSPT), which demonstrates good practice in this area

- Local and national support e.g. Digital Social Care - dedicated space to provide advice and support to the sector on technology and data protection https://www.digitalsocialcare.co.uk/

How the training will work

- We will take you through each question for this section of the Toolkit
- If there is anything that you cannot answer straight away:
  - Make a note of what you need to do on the action plan
  - We will follow up on these next time

What we'll be covering in this module

- Why your business needs a suitably trained Data Security and Protection Lead
- The importance of data protection and cyber security training for all staff
- Staff records and contracts
- How to carry out a training needs analysis for all staff
- How to find the right training materials and providers for your needs
- Useful links
- Where to find help
- Next steps

Login to the Toolkit

- Go to https://www.dsptoolkit.nhs.uk/Account/Login
- Or put in 'DSPT login'

Staff records

What the DSPT questions ask

- 4.1.1 Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?

Data security and protection - Knowing your responsibilities

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

- Do you know who would be the Data Security and Protection Lead within your organisation?

- Do you know if this role has been formally assigned?

- If you're not sure, what do you need to do to find out? What needs to be put in place

Who has responsibility for what?
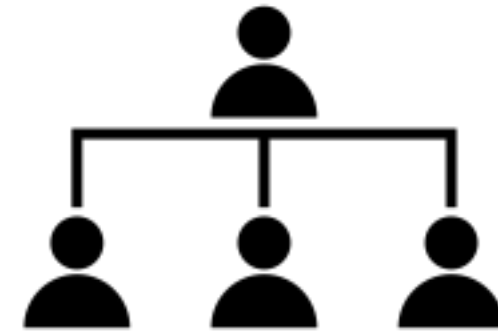
Who leads data security?

- 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

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

Clauses in contracts and agreements must reference data security

Issue	Example
Confidentiality	Maintaining all information confidentially; this includes careless conversations, sending information to the wring address, records being hacked
Integrity	Records are maintained accurately ie any inaccuracies or errors are corrected
Availability	The required data is available when required

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.

Do your staff contracts contain a clause to cover this?
What would need to happen to put this in place?

Further information and guidance

- Data security and protection responsibilities and specialised roles including the Dang the Data Security and Protection Lead https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/

- The role of the Data Security and Protection Lead guide from Skills for Care: https://www.skillsforcare.org.uk/Leadership-management/managing-a-service/Digital-technology-and-social-care/Cyber-security-and-data-protection.aspx

- Staff data security contract clause template from Digital Social Care: https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/

What the DSPT questions ask relating to training

- 2.1.1 Does your organisation have an induction process that covers data security and protection, and cyber security?

- 3.1.1 Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?

- 3.2.1 Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?

- 3.4.1 Have the people with responsibility for data security and protection received training suitable for their role?

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
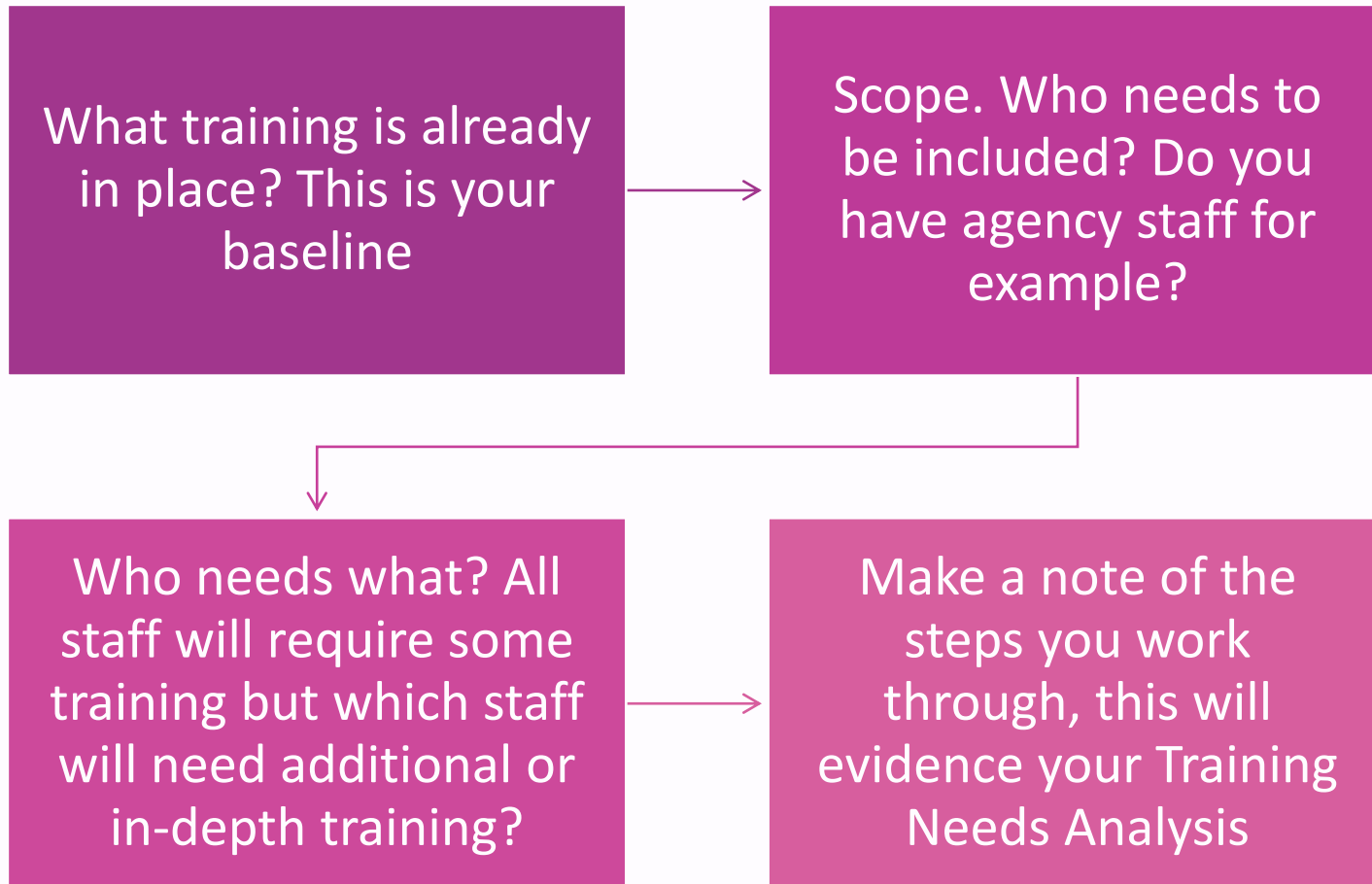
Induction training

- Does your induction training cover the above?
- If not, does it cover some of those things? What might be missing?
- What would need to happen to make sure all the areas are covered?

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

"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

KiCA
KENT INTEGRATED CARE ALLIANCE

Kent County Council
kent.gov.uk

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	

CARE ALLIANCE

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.

CARE ALLIANCE

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
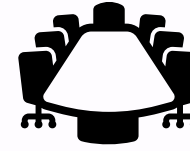
Annual training standard - Sources of training

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

- What are your arrangements for training?
- What sorts of training methods are used?
- How are relevant staff included?

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

- Skills for Care introductory learning resources (videos) for managers; for staff; and for GDPR: https://www.skillsforcare.org.uk/Leadership-management/managing-a-service/digital-skills/Data-protection-GDPR-information-sharing.aspx

- 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/projects/resources-to-help-digital-enabling/

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/

- Staff training videos available via the link above:
  - Keeping your care service cyber-secure
  - Data protection – care services training
  - Data and cyber security – care services training

- Recommended training for the Data Security and Protection Lead: https://www.e-lfh.org.uk/programmes/data-security-awareness/

- Digital Social Care '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/

Any final questions?

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	Local help and support
NHS Digital DSPT Helpdesk in Exeter	**Digital Social Care** www.digitalsocialcare.co.uk	**Website** www.designandlearningcentre.com/data-security-protection-toolkit
Telephone 0300 303 4034	**Digital Social Care helpline 0208 133 3430 (Monday – Friday, 9.00-17.00)**	**Local helpline: TBC (Monday – Friday, 9.00-16.00)**
Email exeter.helpdesk@nhs.net	**Email** help@digitalsocialcare.co.uk	**Email** dspt@kent.gov.uk

KiCA
KENT INTEGRATED CARE ALLIANCE

Kent County Council
kent.gov.uk

Next steps

- For the questions where you know the answer, make sure you have logged in to the Toolkit and completed these questions

- Review your action plan to make sure you've captured what you need to do next

- We will follow up on your actions next time