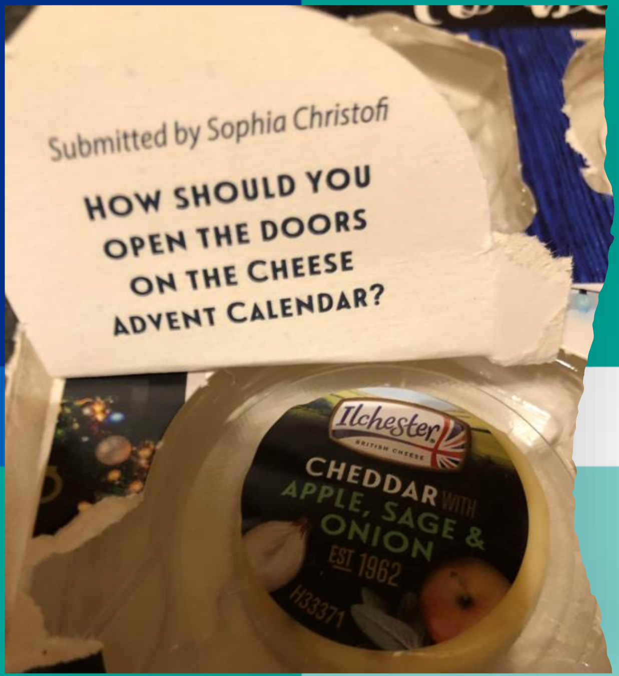
Data Security and Protection Toolkit

Training and Awareness update

DSPT 2023-24

13 December 2023


Submitted by Sophia Christofi
HOW SHOULD YOU OPEN THE DOORS ON THE CHEESE ADVENT CALENDAR?
Ilchester
BRITISH CHEESE
CHEDDAR WITH APPLE, SAGE & ONION
EST 1962
H33371

John Hodson

DSP Toolkit 23-24

Fully Incorporated in DSPT.
Big Picture Guides
Minor Changes overall

Biggest change is to the Data Security Awareness requirement

Update Tooltips based on feedback

Baseline 29th February 2024

MFA update required in the Baseline

Final Publication 30th June 2024

Key IT Suppliers and OES Providers move to CAT1

All companies will follow a triage to see if they are Key IT Suppliers based on criteria like ICO and Companies House records

OES providers under NIS will have to amend primary sector to a CAT1 sector on login to DSPT next month

Emails to OES providers explaining the change

Review enforced at first login of 23-24 DSPT

Will review to follow up with any relevant Key IT suppliers or OES providers

Criteria for IT Suppliers (https://www.dsptoolkit.nhs.uk/Help/5)

If you are a company who meets **all** the criteria of:

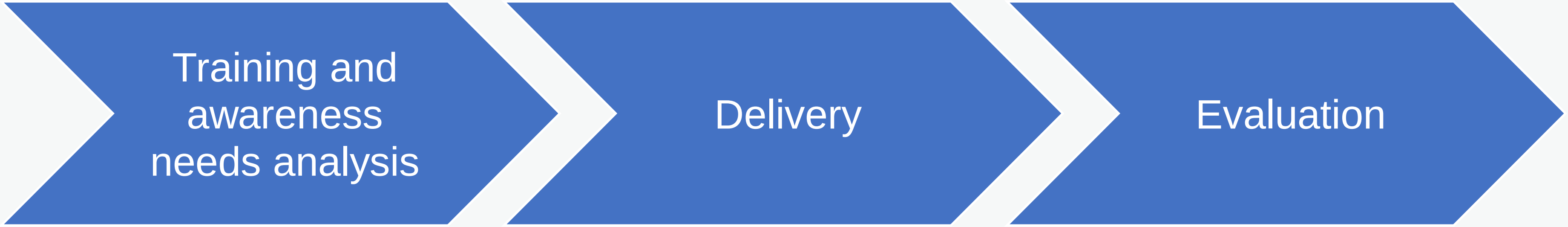
- supplies digital (either software and / or physical) goods and services to the NHS and/or care,
- 50+ staff,
- a turnover of £10m+
- If you don’t meet the above criteria, you should select the category ‘Other (including charities and NHS business partners)’.

Staff Training and Awareness

Impacting NHS Trusts, ICBs, CSUs, ALBs,
Independent providers who are Operators of Essential Services
and Large IT Suppliers

What this means for you

Category 1 organisations: CAF outcomes for **training** and **culture** written into evidentiary requirements that fit the current DSPT structure and presentation



Training and awareness needs analysis

Delivery

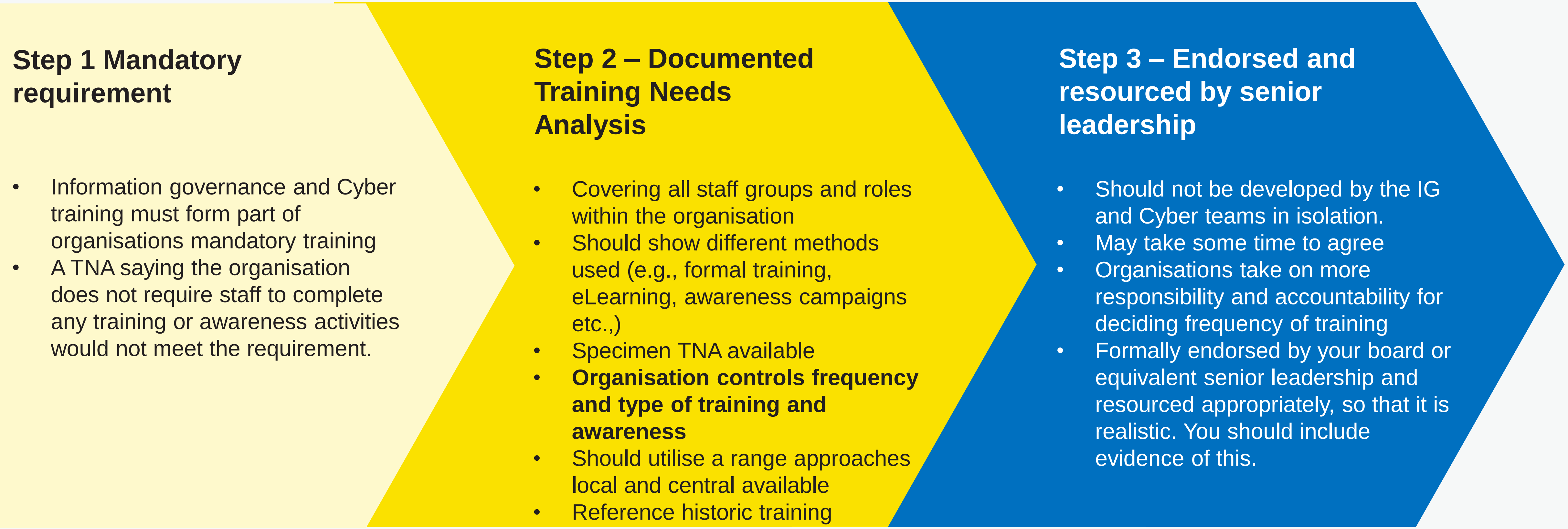
Evaluation

- **Start early** and talk across your ICS
- ‘Data Security Awareness’ national e-learning is still an option
- **Audited requirement** for 2023/24

Category 3 and 4 organisations: no change to previous assertion (95%)

To meet the DSP Toolkit

3.1.1 Training and awareness activities form part of organisational mandatory training requirements, with a training and awareness needs analysis (covering all staff roles) that is formally endorsed and resourced by senior leadership



Step 1 Mandatory requirement

- Information governance and Cyber training must form part of organisations mandatory training
- A TNA saying the organisation does not require staff to complete any training or awareness activities would not meet the requirement.

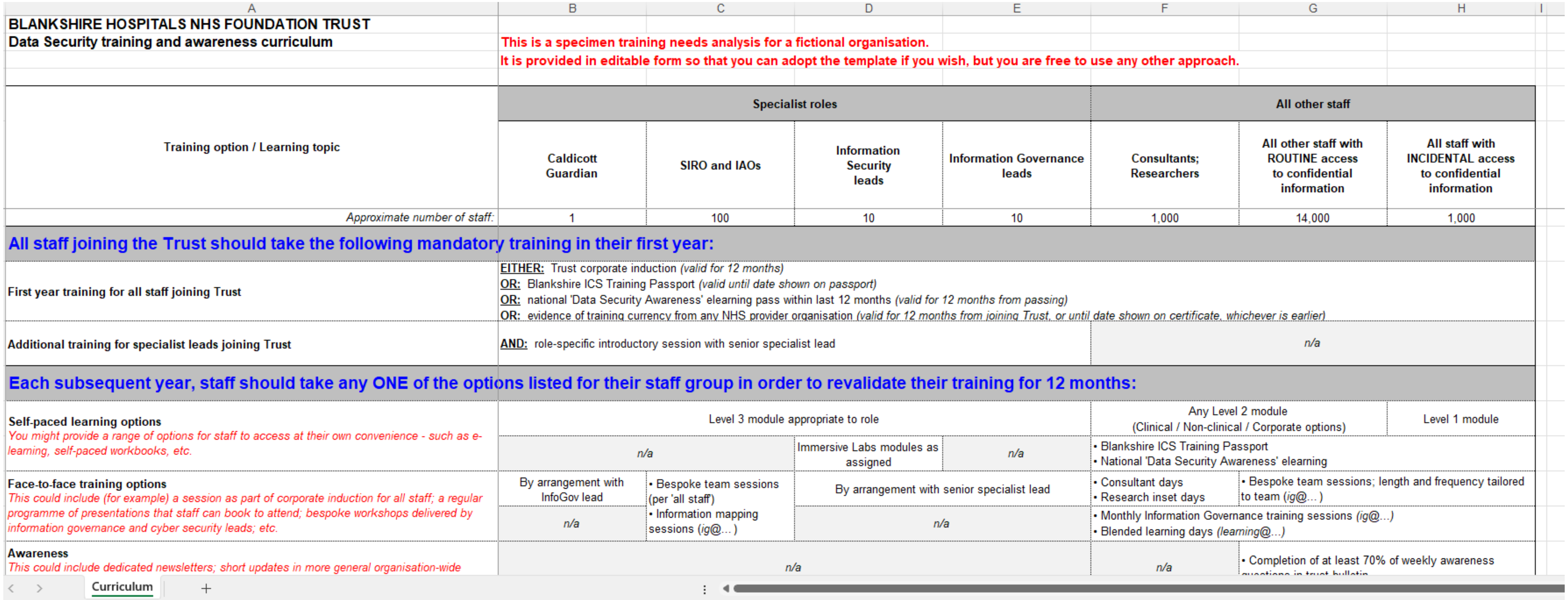
Step 2 – Documented Training Needs Analysis

- Covering all staff groups and roles within the organisation
- Should show different methods used (e.g., formal training, eLearning, awareness campaigns etc.,)
- Specimen TNA available
- **Organisation controls frequency and type of training and awareness**
- Should utilise a range approaches local and central available
- Reference historic training

Step 3 – Endorsed and resourced by senior leadership

- Should not be developed by the IG and Cyber teams in isolation.
- May take some time to agree
- Organisations take on more responsibility and accountability for deciding frequency of training
- Formally endorsed by your board or equivalent senior leadership and resourced appropriately, so that it is realistic. You should include evidence of this.

Sample Training Needs Analysis

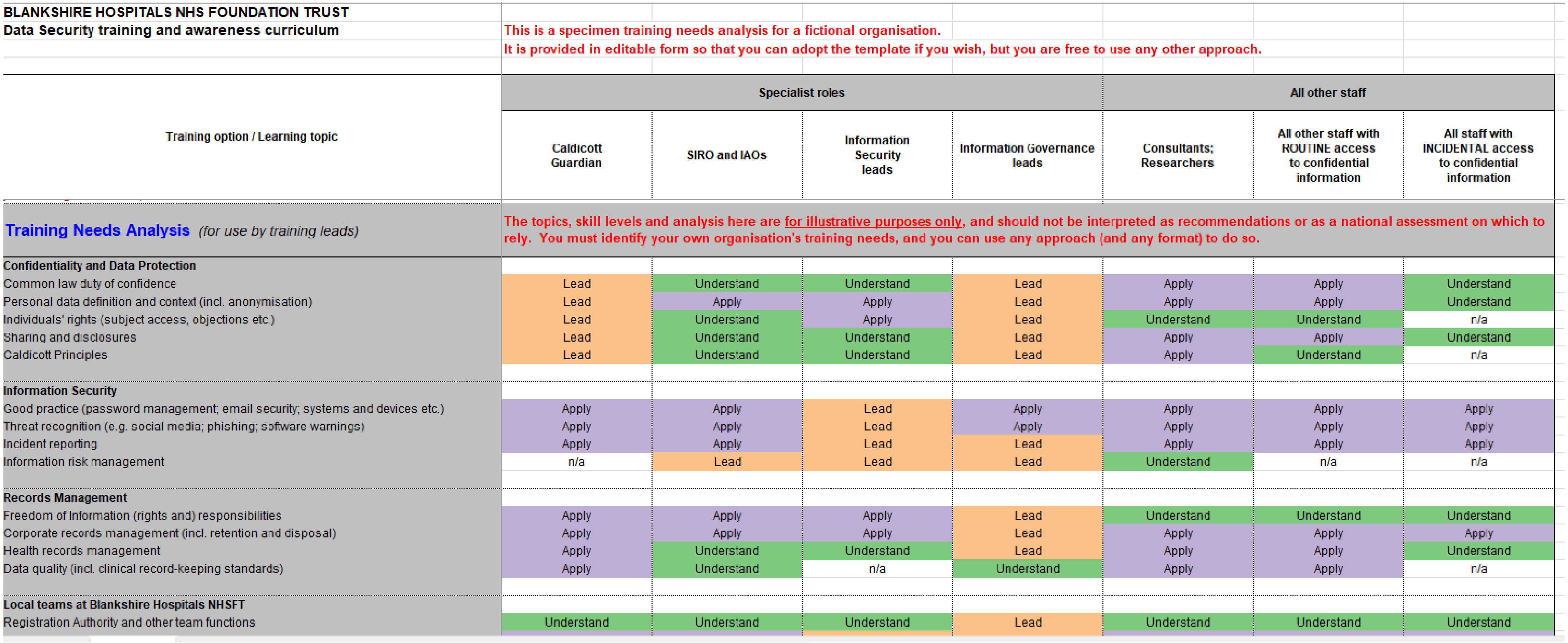


BLANKSHIRE HOSPITALS NHS FOUNDATION TRUST
Data Security training and awareness curriculum

This is a specimen training needs analysis for a fictional organisation.
It is provided in editable form so that you can adopt the template if you wish, but you are free to use any other approach.

A	B	C	D	E	F	G	H
Training option / Learning topic	**Specialist roles**				**All other staff**		
	Caldicott Guardian	**SIRO and IAOs**	**Information Security leads**	**Information Governance leads**	**Consultants; Researchers**	**All other staff with ROUTINE access to confidential information**	**All staff with INCIDENTAL access to confidential information**
Approximate number of staff:	1	100	10	10	1,000	14,000	1,000
All staff joining the Trust should take the following mandatory training in their first year:							
First year training for all staff joining Trust	**EITHER:** Trust corporate induction *(valid for 12 months)* **OR:** Blankshire ICS Training Passport *(valid until date shown on passport)* **OR:** national 'Data Security Awareness' elearning pass within last 12 months *(valid for 12 months from passing)* **OR:** evidence of training currency from any NHS provider organisation *(valid for 12 months from joining Trust, or until date shown on certificate, whichever is earlier)*						
Additional training for specialist leads joining Trust	**AND:** role-specific introductory session with senior specialist lead				*n/a*		
Each subsequent year, staff should take any ONE of the options listed for their staff group in order to revalidate their training for 12 months:							
Self-paced learning options *You might provide a range of options for staff to access at their own convenience - such as e-learning, self-paced workbooks, etc.*	Level 3 module appropriate to role				Any Level 2 module (Clinical / Non-clinical / Corporate options)		Level 1 module
	n/a		Immersive Labs modules as assigned	*n/a*	• Blankshire ICS Training Passport • National 'Data Security Awareness' elearning		
Face-to-face training options *This could include (for example) a session as part of corporate induction for all staff; a regular programme of presentations that staff can book to attend; bespoke workshops delivered by information governance and cyber security leads; etc.*	By arrangement with InfoGov lead	• Bespoke team sessions (per 'all staff') • Information mapping sessions (*ig@...*)	By arrangement with senior specialist lead		• Consultant days • Research inset days	• Bespoke team sessions; length and frequency tailored to team (*ig@...*)	
	n/a		*n/a*		• Monthly Information Governance training sessions *(ig@...)* • Blended learning days *(learning@...)*		
Awareness *This could include dedicated newsletters; short updates in more general organisation-wide*	*n/a*				*n/a*	• Completion of at least 70% of weekly awareness questions in trust bulletin	

Sample Training Needs Analysis



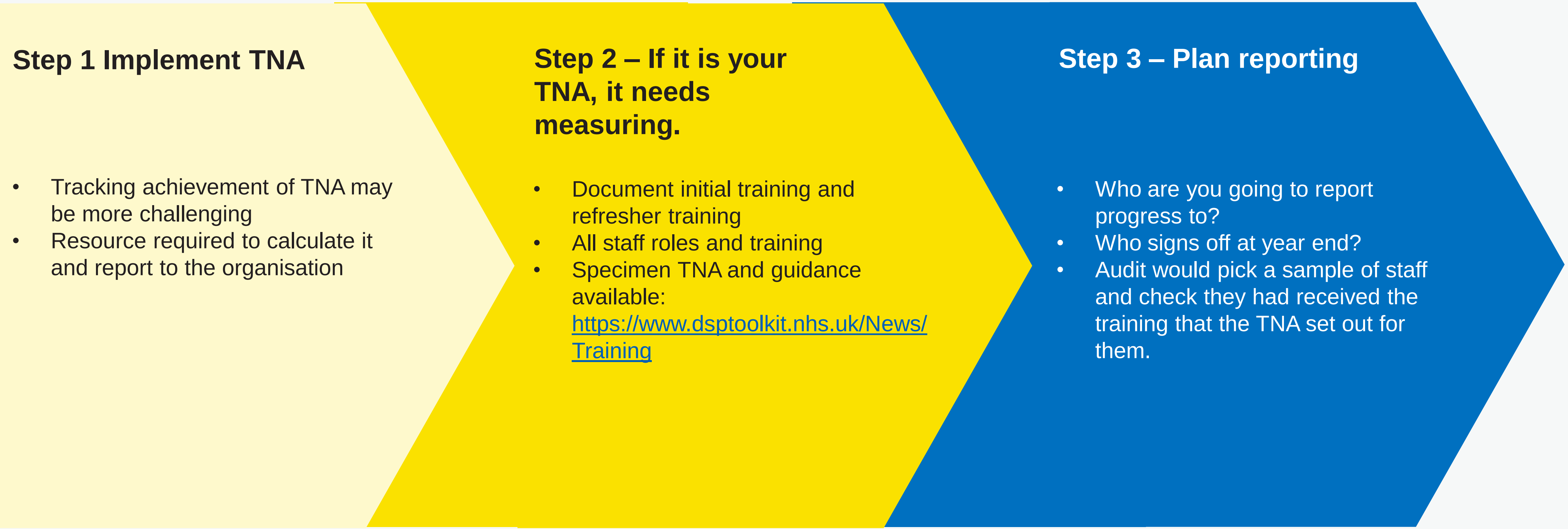
BLANKSHIRE HOSPITALS NHS FOUNDATION TRUST
Data Security training and awareness curriculum

This is a specimen training needs analysis for a fictional organisation.
It is provided in editable form so that you can adopt the template if you wish, but you are free to use any other approach.

	Specialist roles				All other staff		
Training option / Learning topic	Caldicott Guardian	SIRO and IAOs	Information Security leads	Information Governance leads	Consultants; Researchers	All other staff with ROUTINE access to confidential information	All staff with INCIDENTAL access to confidential information
Training Needs Analysis *(for use by training leads)*	The topics, skill levels and analysis here are for illustrative purposes only, and should not be interpreted as recommendations or as a national assessment on which to rely. You must identify your own organisation's training needs, and you can use any approach (and any format) to do so.						
Confidentiality and Data Protection							
Common law duty of confidence	Lead	Understand	Understand	Lead	Apply	Apply	Understand
Personal data definition and context (incl. anonymisation)	Lead	Apply	Apply	Lead	Apply	Apply	Understand
Individuals' rights (subject access, objections etc.)	Lead	Understand	Apply	Lead	Understand	Understand	n/a
Sharing and disclosures	Lead	Understand	Understand	Lead	Apply	Apply	Understand
Caldicott Principles	Lead	Understand	Understand	Lead	Apply	Understand	n/a
Information Security							
Good practice (password management; email security; systems and devices etc.)	Apply	Apply	Lead	Apply	Apply	Apply	Apply
Threat recognition (e.g. social media; phishing; software warnings)	Apply	Apply	Lead	Apply	Apply	Apply	Apply
Incident reporting	Apply	Apply	Lead	Lead	Apply	Apply	Apply
Information risk management	n/a	Lead	Lead	Lead	Understand	n/a	n/a
Records Management							
Freedom of Information (rights and) responsibilities	Apply	Apply	Apply	Lead	Understand	Understand	Understand
Corporate records management (incl. retention and disposal)	Apply	Apply	Apply	Lead	Apply	Apply	Apply
Health records management	Apply	Understand	Understand	Lead	Apply	Apply	Understand
Data quality (incl. clinical record-keeping standards)	Apply	Understand	n/a	Understand	Apply	Apply	n/a
Local teams at Blankshire Hospitals NHSFT							
Registration Authority and other team functions	Understand	Understand	Understand	Lead	Understand	Understand	Understand

To meet the DSP Toolkit

3.1.2 Your organisation’s defined training and awareness activities are implemented for and followed by all staff.



Step 1 Implement TNA

- Tracking achievement of TNA may be more challenging
- Resource required to calculate it and report to the organisation

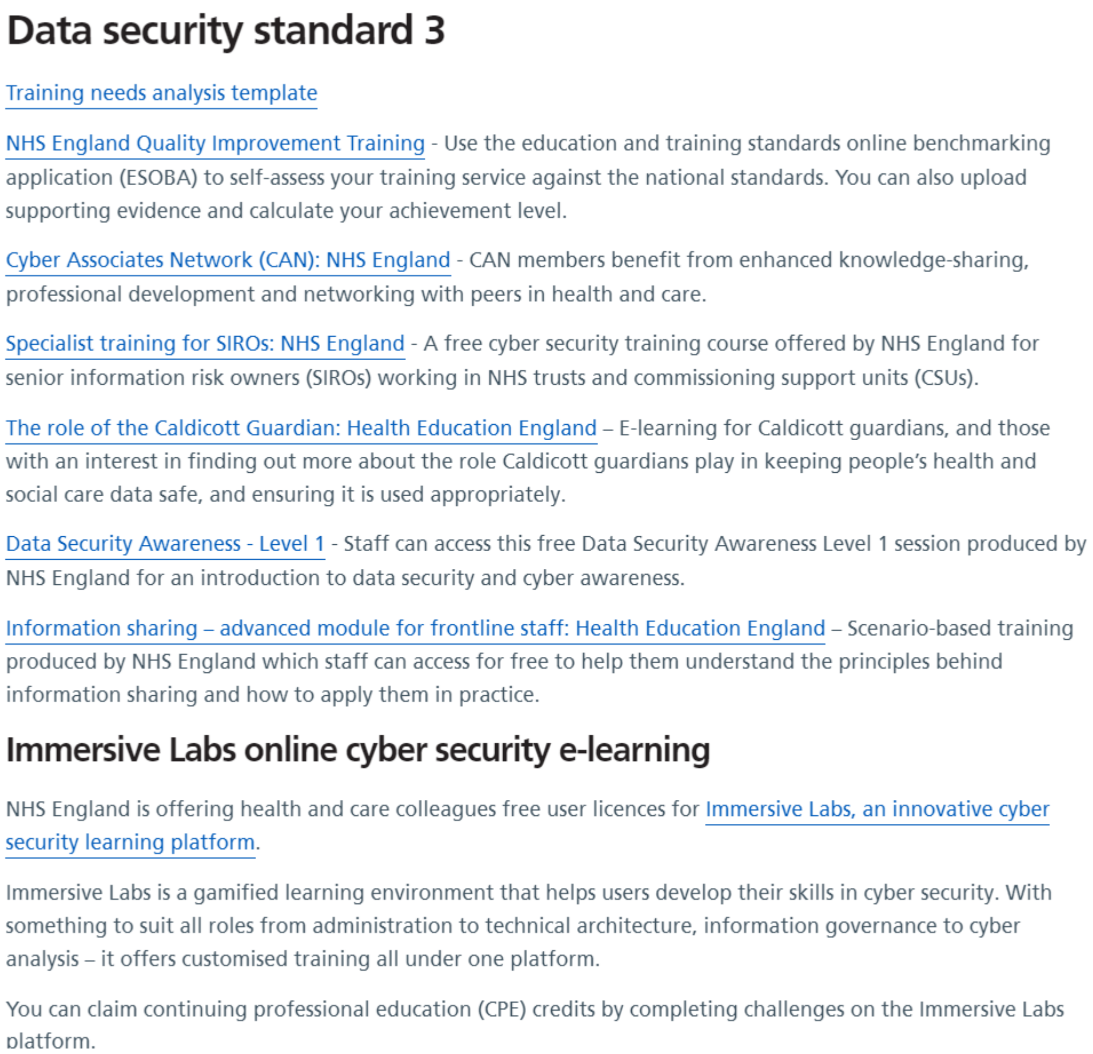
Step 2 – If it is your TNA, it needs measuring.

- Document initial training and refresher training
- All staff roles and training
- Specimen TNA and guidance available: https://www.dsptoolkit.nhs.uk/News/Training

Step 3 – Plan reporting

- Who are you going to report progress to?
- Who signs off at year end?
- Audit would pick a sample of staff and check they had received the training that the TNA set out for them.

Useful training resources



Data security standard 3

Training needs analysis template

NHS England Quality Improvement Training - Use the education and training standards online benchmarking application (ESOBA) to self-assess your training service against the national standards. You can also upload supporting evidence and calculate your achievement level.

Cyber Associates Network (CAN): NHS England - CAN members benefit from enhanced knowledge-sharing, professional development and networking with peers in health and care.

Specialist training for SIROs: NHS England - A free cyber security training course offered by NHS England for senior information risk owners (SIROs) working in NHS trusts and commissioning support units (CSUs).

The role of the Caldicott Guardian: Health Education England – E-learning for Caldicott guardians, and those with an interest in finding out more about the role Caldicott guardians play in keeping people’s health and social care data safe, and ensuring it is used appropriately.

Data Security Awareness - Level 1 - Staff can access this free Data Security Awareness Level 1 session produced by NHS England for an introduction to data security and cyber awareness.

Information sharing – advanced module for frontline staff: Health Education England – Scenario-based training produced by NHS England which staff can access for free to help them understand the principles behind information sharing and how to apply them in practice.

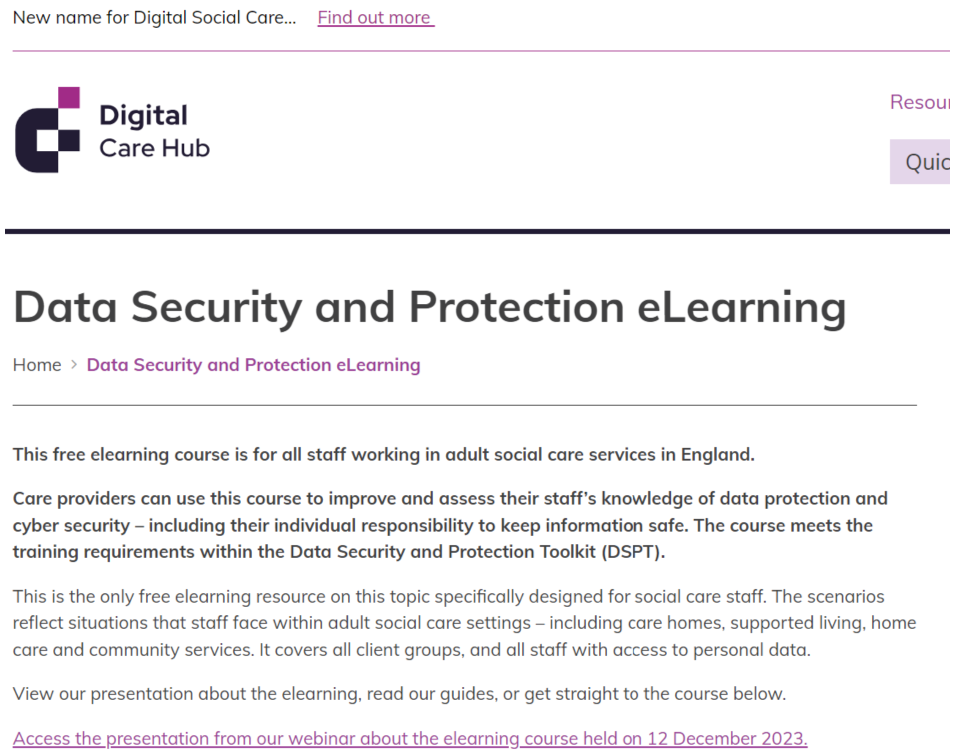
Immersive Labs online cyber security e-learning

NHS England is offering health and care colleagues free user licences for Immersive Labs, an innovative cyber security learning platform.

Immersive Labs is a gamified learning environment that helps users develop their skills in cyber security. With something to suit all roles from administration to technical architecture, information governance to cyber analysis – it offers customised training all under one platform.

You can claim continuing professional education (CPE) credits by completing challenges on the Immersive Labs platform.

Free training resources



New name for Digital Social Care... Find out more

Digital Care Hub

Resou

Quic

Data Security and Protection eLearning

Home › Data Security and Protection eLearning

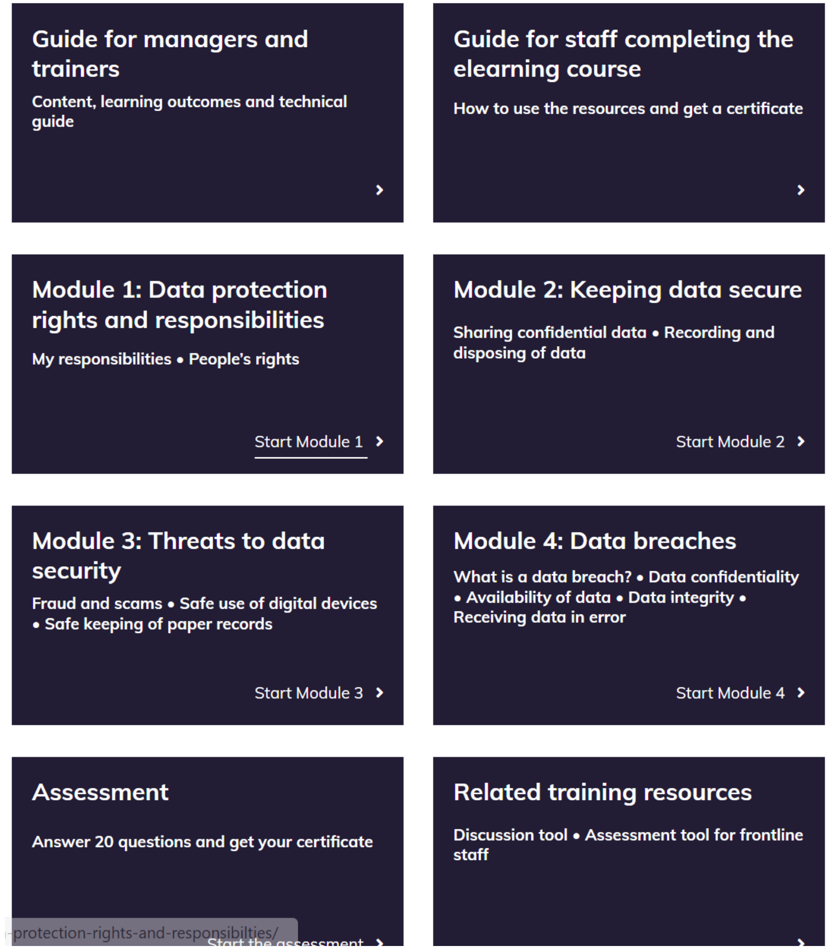
This free elearning course is for all staff working in adult social care services in England.

Care providers can use this course to improve and assess their staff's knowledge of data protection and cyber security – including their individual responsibility to keep information safe. The course meets the training requirements within the Data Security and Protection Toolkit (DSPT).

This is the only free elearning resource on this topic specifically designed for social care staff. The scenarios reflect situations that staff face within adult social care settings – including care homes, supported living, home care and community services. It covers all client groups, and all staff with access to personal data.

View our presentation about the elearning, read our guides, or get straight to the course below.

Access the presentation from our webinar about the elearning course held on 12 December 2023.



Guide for managers and trainers

Content, learning outcomes and technical guide ›

Guide for staff completing the elearning course

How to use the resources and get a certificate ›

Module 1: Data protection rights and responsibilities

My responsibilities • People's rights

Start Module 1 ›

Module 2: Keeping data secure

Sharing confidential data • Recording and disposing of data

Start Module 2 ›

Module 3: Threats to data security

Fraud and scams • Safe use of digital devices • Safe keeping of paper records

Start Module 3 ›

Module 4: Data breaches

What is a data breach? • Data confidentiality • Availability of data • Data integrity • Receiving data in error

Start Module 4 ›

Assessment

Answer 20 questions and get your certificate

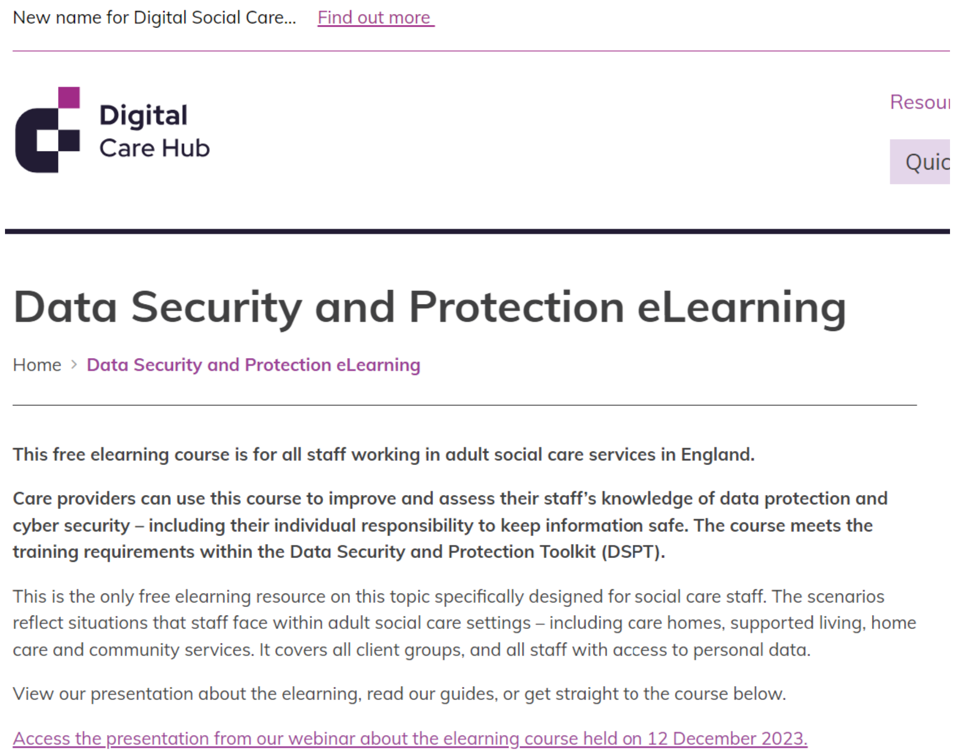
-protection-rights-and-responsibilties/

Start the assessment ›

Related training resources

Discussion tool • Assessment tool for frontline staff ›

Free training resources



New name for Digital Social Care... Find out more

Data Security and Protection eLearning

Home > Data Security and Protection eLearning

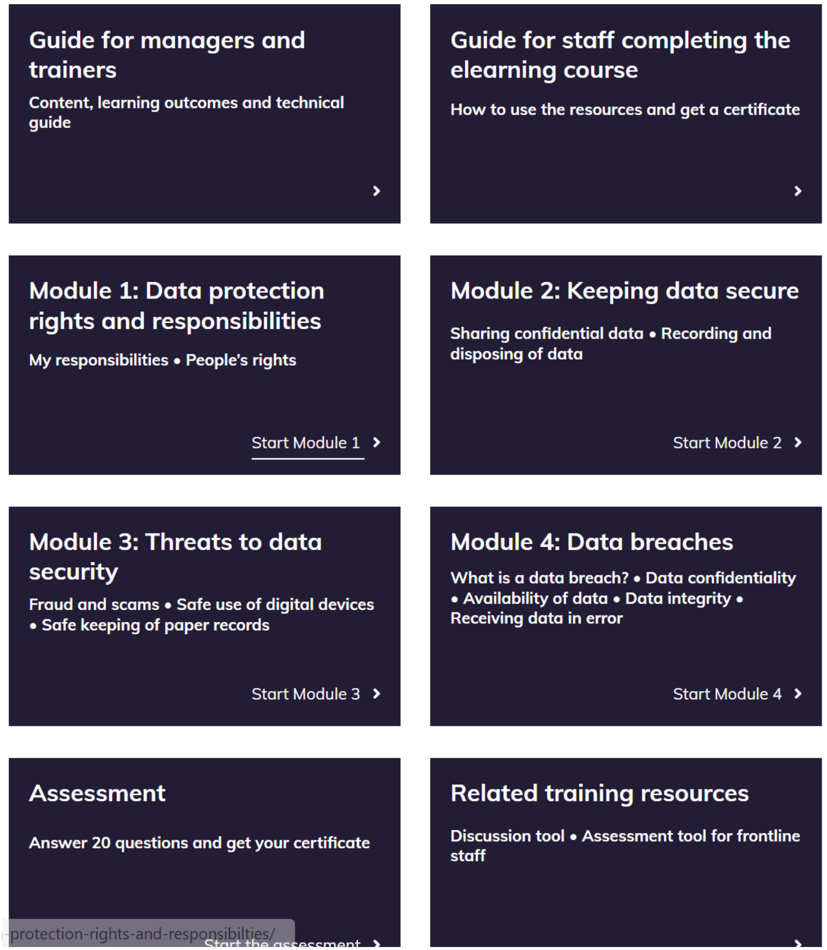
This free elearning course is for all staff working in adult social care services in England.

Care providers can use this course to improve and assess their staff's knowledge of data protection and cyber security – including their individual responsibility to keep information safe. The course meets the training requirements within the Data Security and Protection Toolkit (DSPT).

This is the only free elearning resource on this topic specifically designed for social care staff. The scenarios reflect situations that staff face within adult social care settings – including care homes, supported living, home care and community services. It covers all client groups, and all staff with access to personal data.

View our presentation about the elearning, read our guides, or get straight to the course below.

Access the presentation from our webinar about the elearning course held on 12 December 2023.



Guide for managers and trainers

Content, learning outcomes and technical guide

Guide for staff completing the elearning course

How to use the resources and get a certificate

Module 1: Data protection rights and responsibilities

My responsibilities • People's rights

Start Module 1 ›

Module 2: Keeping data secure

Sharing confidential data • Recording and disposing of data

Start Module 2 ›

Module 3: Threats to data security

Fraud and scams • Safe use of digital devices • Safe keeping of paper records

Start Module 3 ›

Module 4: Data breaches

What is a data breach? • Data confidentiality • Availability of data • Data integrity • Receiving data in error

Start Module 4 ›

Assessment

Answer 20 questions and get your certificate

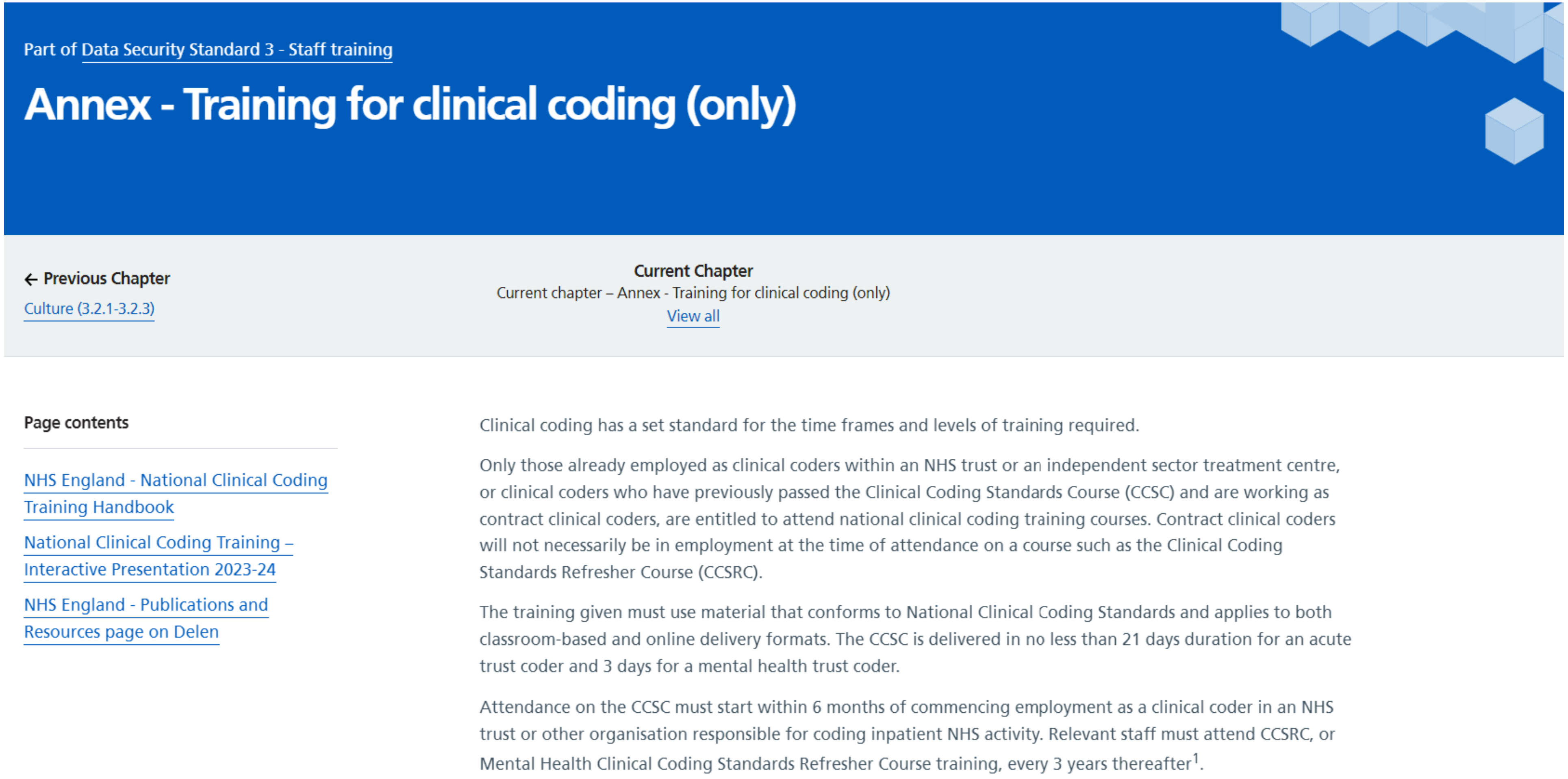
-protection-rights-and-responsibilties/

Start the assessment ›

Related training resources

Discussion tool • Assessment tool for frontline staff

Clinical Coding training resources



Part of Data Security Standard 3 - Staff training

Annex - Training for clinical coding (only)

Page contents

- NHS England - National Clinical Coding Training Handbook
- National Clinical Coding Training – Interactive Presentation 2023-24
- NHS England - Publications and Resources page on Delen

Clinical coding has a set standard for the time frames and levels of training required.

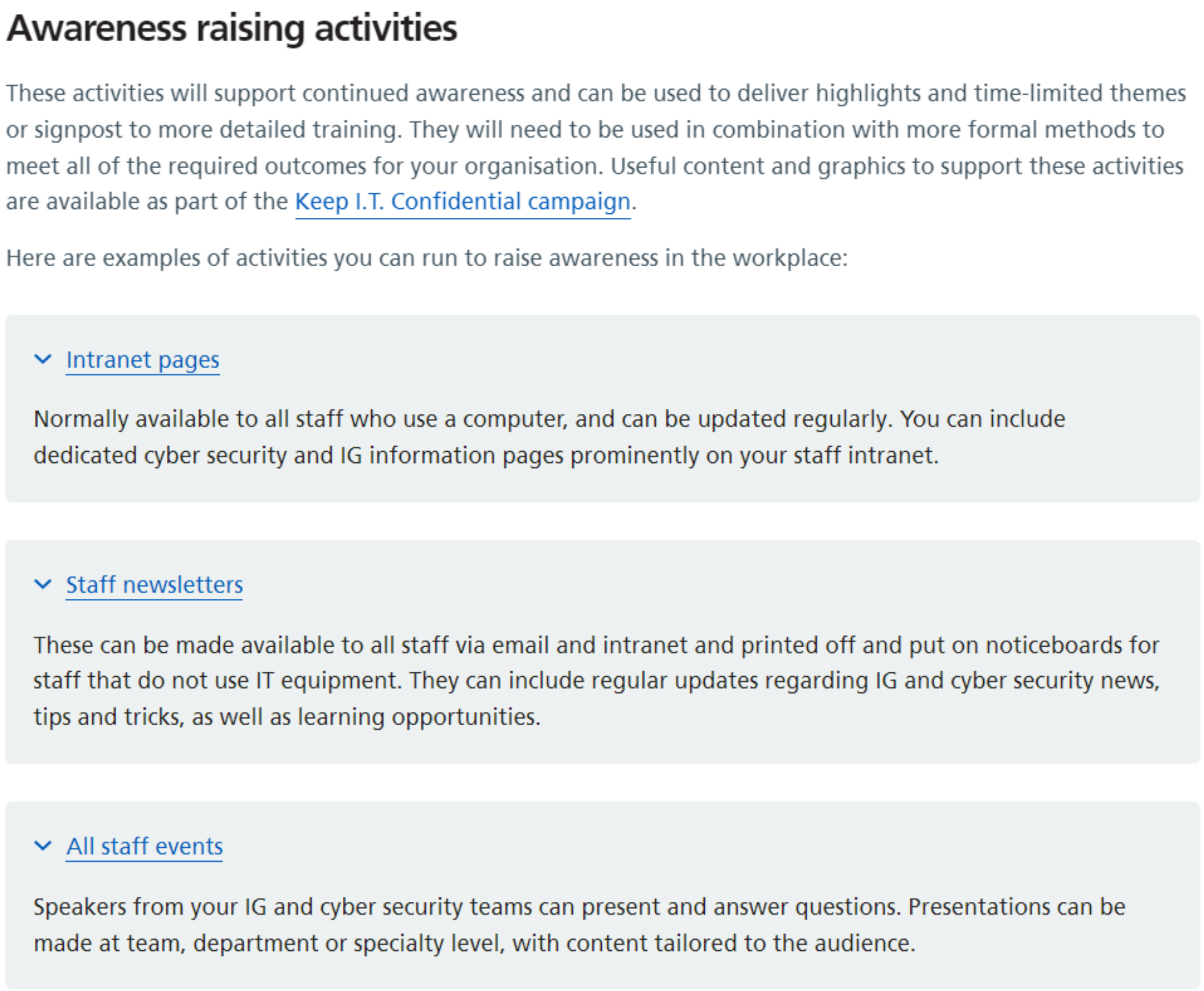
Only those already employed as clinical coders within an NHS trust or an independent sector treatment centre, or clinical coders who have previously passed the Clinical Coding Standards Course (CCSC) and are working as contract clinical coders, are entitled to attend national clinical coding training courses. Contract clinical coders will not necessarily be in employment at the time of attendance on a course such as the Clinical Coding Standards Refresher Course (CCSRC).

The training given must use material that conforms to National Clinical Coding Standards and applies to both classroom-based and online delivery formats. The CCSC is delivered in no less than 21 days duration for an acute trust coder and 3 days for a mental health trust coder.

Attendance on the CCSC must start within 6 months of commencing employment as a clinical coder in an NHS trust or other organisation responsible for coding inpatient NHS activity. Relevant staff must attend CCSRC, or Mental Health Clinical Coding Standards Refresher Course training, every 3 years thereafter[1].

Awareness raising activities

https://digital.nhs.uk/cyber-and-data-security/campaigns/keep-it-confidential/run-your-own-cyber-security-campaign



Awareness raising activities

These activities will support continued awareness and can be used to deliver highlights and time-limited themes or signpost to more detailed training. They will need to be used in combination with more formal methods to meet all of the required outcomes for your organisation. Useful content and graphics to support these activities are available as part of the Keep I.T. Confidential campaign.

Here are examples of activities you can run to raise awareness in the workplace:

⌄ Intranet pages

Normally available to all staff who use a computer, and can be updated regularly. You can include dedicated cyber security and IG information pages prominently on your staff intranet.

⌄ Staff newsletters

These can be made available to all staff via email and intranet and printed off and put on noticeboards for staff that do not use IT equipment. They can include regular updates regarding IG and cyber security news, tips and tricks, as well as learning opportunities.

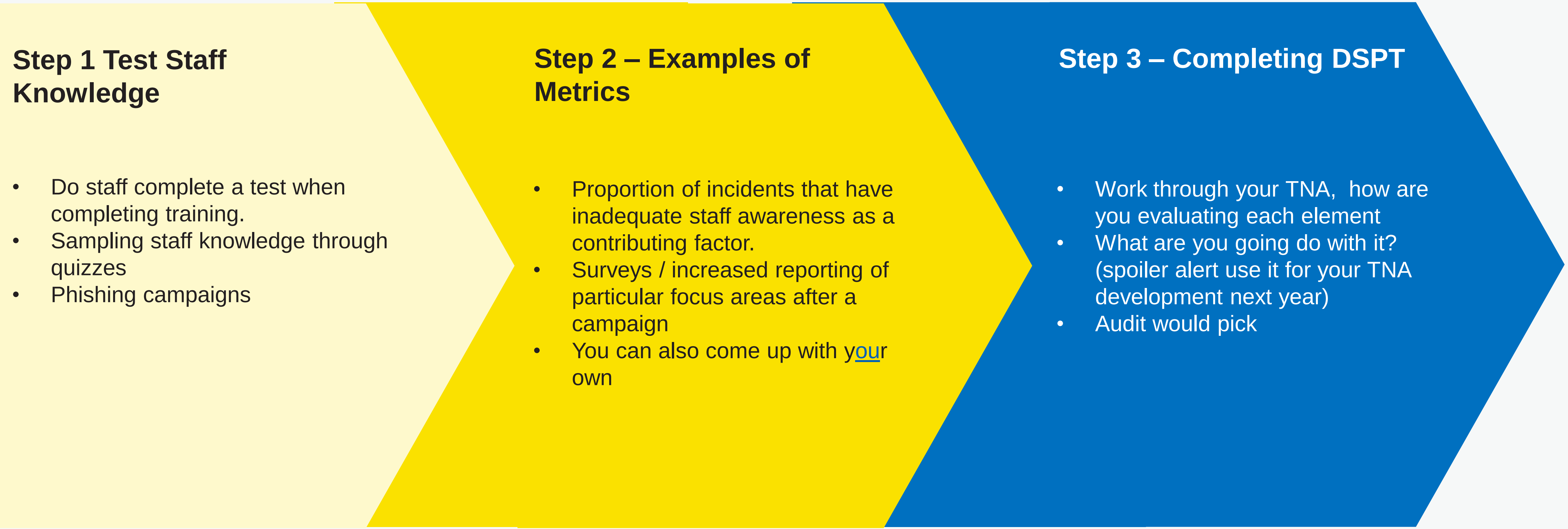
⌄ All staff events

Speakers from your IG and cyber security teams can present and answer questions. Presentations can be made at team, department or specialty level, with content tailored to the audience.

To meet the DSP Toolkit

3.1.3 Provide details of how you evaluate your training and awareness activities.

- https://www.dsptoolkit.nhs.uk/News/Training



Step 1 Test Staff Knowledge

- Do staff complete a test when completing training.
- Sampling staff knowledge through quizzes
- Phishing campaigns

Step 2 – Examples of Metrics

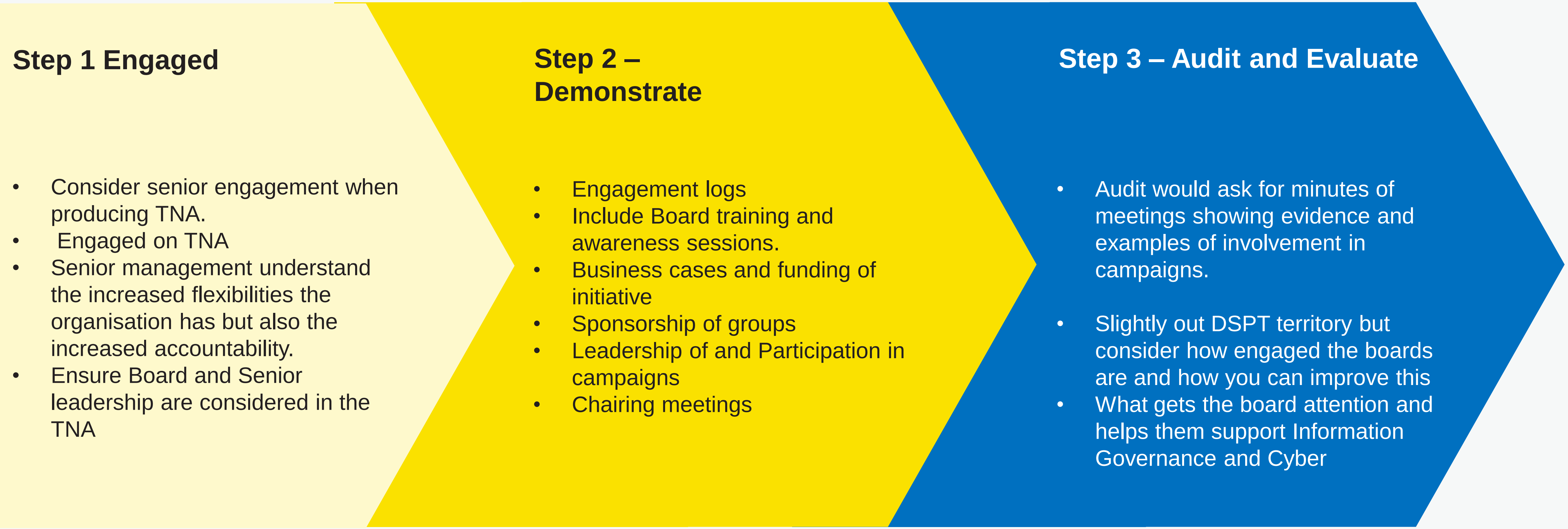
- Proportion of incidents that have inadequate staff awareness as a contributing factor.
- Surveys / increased reporting of particular focus areas after a campaign
- You can also come up with your own

Step 3 – Completing DSPT

- Work through your TNA, how are you evaluating each element
- What are you going do with it? (spoiler alert use it for your TNA development next year)
- Audit would pick

To meet the DSP Toolkit

- **3.2.1 Information governance and cyber security matters are prioritised by the board or equivalent senior leaders.**



Step 1 Engaged

- Consider senior engagement when producing TNA.
- Engaged on TNA
- Senior management understand the increased flexibilities the organisation has but also the increased accountability.
- Ensure Board and Senior leadership are considered in the TNA

Step 2 – Demonstrate

- Engagement logs
- Include Board training and awareness sessions.
- Business cases and funding of initiative
- Sponsorship of groups
- Leadership of and Participation in campaigns
- Chairing meetings

Step 3 – Audit and Evaluate

- Audit would ask for minutes of meetings showing evidence and examples of involvement in campaigns.

- Slightly out DSPT territory but consider how engaged the boards are and how you can improve this
- What gets the board attention and helps them support Information Governance and Cyber

DSPT Audit

For Large NHS Organisations

What will the Audit Cover for 23-24

13 assertions:

1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency
2.2 Staff contracts set out responsibilities for data security
3.1 Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness
3.2 Your organisation engages proactively and widely to improve data security, and has an open and just culture for data security incidents
4.4 You closely manage privileged user access to networks and information systems supporting the essential service
5.1 Process reviews are held at least once per year where data security is put at risk and following DS incidents
6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway
7.1 Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services
8.4 You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service
9.2 A penetration test has been scoped and undertaken
9.5 You securely configure the network and information systems that support the delivery of essential services
9.6 The organisation is protected by a well-managed firewall
10.2 Basic due diligence has been undertaken against each supplier that handles personal information

https://www.dsptoolkit.nhs.uk/News/auditnews

CAF for 24-25

What you need to know

- In August 2024 the DSPT will be changing to adopt the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.

- This change will lead to Cat 1 organisations (NHS Trusts, CSU, ALB and ICBs) seeing a different interface when they log in, which sets out CAF-aligned requirements in terms of Objectives, Principles and Outcomes.

- The goal of the CAF is to set out broad principles to drive good decision-making, rather than a "compliance checklist" of good practices.

- Expectations for cyber security and IG controls should remain at a reasonably comparable level to the current DSPT, tightening only in areas where NHSE and DHSC believe the higher standard to be a necessary obligation.

- Guidance will be produced and webinars will be stood up to help organisations understand the content, approach and expectations of the CAF-aligned DSPT.

Implementation timescale

Summer 2024 **(DSPT for 2024-25, with submissions due 30 Jun 2025)**	**New user interface based on the CAF will apply to:** • **NHS trusts and foundation trusts** • **Integrated care boards** • **Commissioning support units** • **Arm’s length bodies** **Other organisations retain the current interface and will respond to a list of prescriptive controls, which will be mapped nationally ‘in the background’ against a CAF profile.**
Summer 2025 **(DSPT for 2025-26, with submissions due 30 Jun 2026)**	**New user interface based on the CAF will also apply to:** • **Larger IT suppliers (specific criteria)** • **Independent healthcare providers designated as operators of essential services** **Other organisations retain the current interface and will respond to a list of prescriptive controls, which will be mapped nationally ‘in the background’ against a CAF profile.**
Not yet decided	**Other organisations may move to the CAF-based interface in the future after appropriate analysis and consultation.** **Some types of smaller organisations may never be asked to respond directly to CAF outcomes and instead always be given a list of prescriptive controls (mapped nationally ‘in the background’ against a CAF profile).**

This only illustrates the **interface** change that organisations will see. The **requirements** that are set within the DSPT may vary for different types of organisations even if they see the same interface – as shown on the next page.

DSPT categories

Current groupings for 2023/24: *Categories have no intrinsic meaning – they are simply groupings of organisations sharing a particular question set.*

Category 1	Category 2	Category 3	Category 4
NHS trusts and foundation trusts	***(none)***	**All other organisation types**	**General practices**
Integrated care boards			
Commissioning support units			
Arm's length bodies			
Larger IT suppliers (specific criteria)			
Independent providers designated as operators of essential services (OESs)			

Likely groupings for 2024/25: *Categories are now groupings of organisations sharing a particular DSPT interface (CAF-based vs question list) <u>and</u> a particular CAF profile or set of questions. In this table the category labels have been kept as consistent as possible, to illustrate the effective changes, but they are nonetheless just arbitrary labels.*

Category 1A (CAF-based interface; CAF profile "1A")	**Category 1B** (CAF-based interface; CAF profile "1B")	**Category 2** (Question-based interface; question set "2")	**Category 3** (Question-based interface; question set "3")	**Category 4** (Question-based interface; question set "4")
	NHS trusts and foundation trusts	**Larger IT suppliers (specific criteria)**	**All other organisation types**	**General practices**
	Integrated care boards	**Independent OESs**		
	Commissioning support units			
CNI-operating arm's length bodies (TBC)	**Other arm's length bodies (TBC)**			

Multi-factor authentication policy

Publication 29th August 2023.

Timeline

- **Published on 29th August (https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy)**
- **Compliance check – 29 Feb 2024** – interim DSPT submission

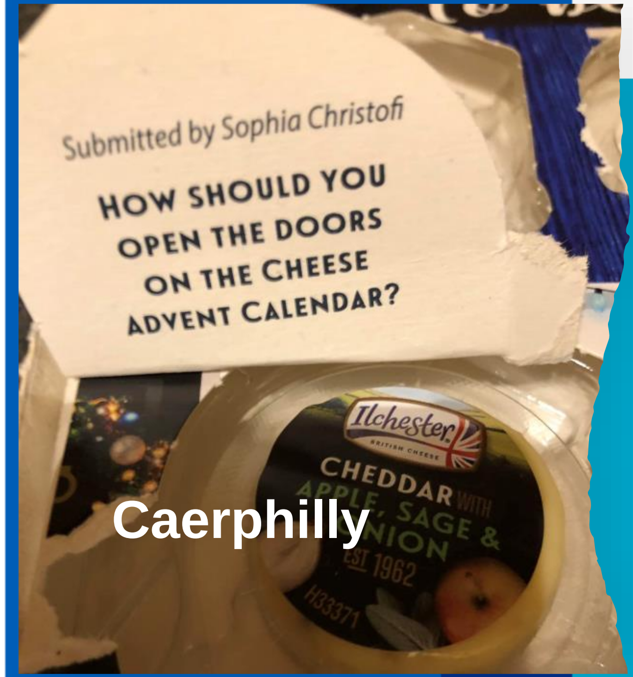
Provide your plans to achieve compliance (i.e. meet 4.5.3) by 30 Jun 2024 (email being sent out about this)

- **Compliance – 30 Jun 2024** – full DSPT submission
- NIS information notices

Action may also be considered if organisations not taking reasonable steps towards compliance

Next Steps

- Interested in participating in User research sessions for the move to CAF
- If you struggling with funding your DSPT audit, get in touch we might be able to help
- email cybersecurity@nhs.net



Submitted by Sophia Christofi

How should you open the doors on the cheese advent calendar?

Caerphilly

Thank You

@nhsengland

company/nhsengland

england.nhs.uk