

Information Assurance Training Needs Analysis

Document Control

Title	Training Needs Analysis
Version	V3
Status	This is a Live Document
Place in Organisation	ICT
Produced by	Data Protection Officer

Amendment History

Date	Summary of Changes	Author(s)	Version Number
February 2024		Su De	

Document Approval

Approved By	NA
Approved Date	NA
Next Review	Continuous Monitoring

Contents

1. Introduction	4
2. Purpose	4
3. Scope.....	4
4. Duties and Responsibilities	5
5. The Information assurance Training	6
6. What training do I have to do?	6
7. . Monitoring and Compliance	7
8. Contact Details.....	8
Appendix 1 - Training Needs Assessment Matrix	9
Appendix 2 - Information assurance Letter and IA Spot Check Questionnaire ..	Error! Bookmark not defined.

1. Introduction

Information Assurance training has become increasingly important due to the proliferation of data in various formats at different levels in the Trust. A well-defined information assurance program ensures that employees have the appropriate level of understanding of data security and data protection.

This TNA looks into the following:

- assess the level of training appropriate for each employee group
- plan resources needed to deliver training
- deliver role-specific training
- identify and address potential gaps in training.

As the Trust completes one cycle of training, the TNA will be reviewed and updated to reflect new national requirements, refinements in the delivery of training based on employee feedback, or changes within your organisation that impact the TNA.

The TNA will be endorsed by the Senior leadership and resourced appropriately as required under the Data Security and Protection Toolkit. The main deliverable of the TNA process is a Training Needs Report.

Purpose

The purpose of this TNA is to ensure:

- that employees are able to understand, and recognise the importance of, the basic principles in line with their role and are therefore adequately prepared to apply their knowledge to different scenarios in their daily working routines.
- a direct link with the Trust's objectives and expected outcomes that covers the ethical standards and requirements for handling personal data and corporate data;
- That the Trust can address individual learning requirements systematically assesses the learning needs of employees;
- The training and awareness are delivered with minimal impact on 'business as usual', using methods which are appropriate to the needs of the training audiences within acceptable timeframes. These includes specialised roles that should receive additional training and support to help them perform in their work duties;
- Action is taken where key information assurance requirements or gaps are identified and need to be addressed.

2. Scope

The category of employees who will be targeted are:

- All employees
- Students (including Apprentices, placement students and ASYE SWs)
- Agency Employees / Contractors
- Employees who are jointly appointed by Trust and another employer
- Honorary employees who are appointed through the Honorary Employees Appointments Procedure

Line managers or hiring managers must ensure the mandatory training is completed as a part of the new starter's checklist. Those Managers with employees who do not have an email account and Single Sign On (SSO) log in credentials as part of their role must complete the pdf version of the Data

Protection Training available from the Data Protection Officer

Pre-requisites

- they have a Trust email address and/or Single Sign On (SSO) log in credentials: employees

Outside scope: The following groups are not subject to this TNA and are not required to undertake the Trust's mandatory training courses, either because they are not required to undertake the training or because they have their own arrangements for training:

- Research Students (covered through their university)
- Employees employed by Trusted Third Parties who have their own arrangements for mandatory annual training programme eg: NHS employees, Police, other Local Authority)
- General one-off visitors (not required)
- One-off guest Lecturers (not required)
- Auditors, Ofsted Inspectors or Independent Investigator
- One-off workers e.g., an event manager or a photographer, volunteer helping at an event who will not return to Trust (not required)

3. Duties and Responsibilities

Job Role	Responsibility
Chief Executive	The Chief Executive is accountable for the effective implementation of IA Training
Senior Information Risk Officer (SIRO) Nominated by the Exec Team. Director of Strategy and Transformation Deputy SIRO (nominated by the SIRO)	The SIRO will ensure the Trust Board is adequately briefed on all information risk issues associated with IA employees training. This will ensure: - <ul style="list-style-type: none"> • The Trust's approach in terms of resource, commitment and execution is effective and is communicated to all employees; • Ensure all training requirements are kept up to date.
The Caldicott Guardian Nominated by the Exec team	The Caldicott Guardian will ensure all training requirements are kept up to date in line with changes in legislation.
Information Assurance Group (IAG)	The IAG has full ownership of this TNA and needs to ensure its sits within the current Information assurance Framework. The DPO will ensure all the necessary review of the training needs assessments have been conducted to ensure the effectiveness of the training programme is still fit for purpose.
Line Managers	Line Managers are responsible for ensuring that all IA communication and training requirements are cascaded to junior members of employees and all employees training sessions identified are attended to.

All Employees	All employees are expected to complete / attend their IA training sessions when requested.
---------------	--

4. The Information Assurance Training

Basic IA Training at Induction

Birmingham Children’s Trust recognises that everyone needs a minimum amount of awareness and training to gain the skills and knowledge needed to start using the Trust systems and technology safely, securely and efficiently.

All new starters will receive a training session in basic IA principles via the Trust’s employees induction programme at the start their employment. This requirement will be expected to be undertaken within 6 weeks of their start date of employment at the Trust. Managers responsible for managing employees are required to comply with this requirement.

Mandatory eLearning on Data Security and Protection

All Employees are required to complete the mandatory eLearning training. This can be accessed through the [BCTA Learning Pool](#).

If you don’t have an e-learning account, go to www.bcta.learningpool.com and select the option to create a new account. You will then need to complete a short form to request access so you can be set up on the system.

If you have any issues either accessing or completing the e-learning, please contact the Academy team at BCTA@birminghamchildrenstrust.co.uk for further assistance.

Additional Role Based Training for employees in key roles

All employees in designated roles (for e.g. the SIRO, Caldicott Guardian, specialised managers etc.) will be required to undertake additional training where professional development can be demonstrated.

Departmental Training

To complement the knowledge gained from the e-learning modules and IA range of policies.

The DPO from time to time can deliver face to face sessions (subject to availability) with each department on an annual basis to support specific business requirement, including:

- Understanding and application of IA policies and procedures;
- Provision of specific departmental advice and guidance;
- Facilitation of informal Q&A session

These sessions will be provided on an ad-hoc basis, on request.

5. What training do I have to do?

The IA Training Need Analysis (TNA) matrix highlights the training modules all employees are mandated to complete for Information assurance. It also highlights the additional modules, employees having specialist roles, must complete.

New Starters / Returning to Work

If you are a [new starter](#) whether you are permanent, temporary, contractor or agency, you must complete your training within the first 6 weeks of commencing in post.

If you have changed roles within the organisation and your new role or area is one of those listed at Appendix 'A' then you will be regarded as a new starter in that role.

If you have been away from work and your required IA training status elapsed during your absence, for example maternity leave, external secondment, career break, or long-term sick.

You are required to complete your IA training within the first 6 weeks of your return.

Existing permanent employees / contractors (been in post over 12 months)

If you are an existing member of employees, you must complete the mandatory IA training module (as highlighted in matrix according to your role) on an annual basis.

6. Monitoring and Compliance

Organisations are expected to achieve 95% compliance with the mandatory eLearning Training.

Compliance against the IA training plan and TNA will be monitored throughout the year with regular reports provided to managers for employees management and governance purposes.

All compliance relating to training are reported to the Information Assurance Group. An annual view of the training compliance is included in the SIRO report which is scrutinised by the Audit Team.

The IA Training Needs Analysis will be evaluated using Trust's compliance activity over the previous 12 months or any recommendations from external regulatory organisations. This will enable the Data Protection team to identify any gaps that may need to be addressed.

Any changes to further develop the IA training, will be through the Learning and Development Team in collaboration to ensure all expected requirements are identified and realised.

The success of the Training requirements will be monitored against the following performance objectives:

Measurable Objective	Evidence	Frequency of Monitoring
Achieve 85% target rate for mandatory e-learning for data protection and security in the Trust. This is under review for 2024-25	Reports from the mandatory training dashboard, e-learning programme	Monthly
IA Incidents and Data Breaches reported to the Data Protection	Reports from incident monitoring	Ongoing

team as soon as the incident is identified in the Trust.		
Feedback of employees' comments from IAO and SLT meetings.	Review of employees' comments about the current IA employees training program	Ad-Hoc
Information Asset Owner's Self-Assessment Questionnaire	Issues flagged up from the questionnaire.	Annual

7. Contact Details

For queries, please contact:

1 Avenue Road
Birmingham
B6 4AN

Email: dpo@birminghamchildrenstrust.co.uk

Appendix 1 - Training Needs Assessment Matrix

	Job Profile	Corporate Induction (new joiner)	Data Security & Protection (annual)	How to conduct a DPIA (self learning)	Information Access and Requests (Self Learning)	IAO Training (new starter refreshed 3 years)	Any ad-hoc training arising out of incident	Specialist Data Protection FOI, Audit, Information Security (as required)
Tier 1	All Employees ** In addition to the above, all social workers and members of YOS targeted training as a part of their role.	M	M				M	
Tier 2	All Line Managers	M	M				M	A
Tier 3	Project Manager / Protect Sponsors	M	M	A				A
	IT Roles (internal)	M	M					M*
	IAG Roles (renew every 3 years)	M	M	A				A
	DPO	M	M	A				M*
	Legal Roles	M	M	A				M*
	Internal Audit	M	M	A				M*
	Information Asset Administrators and Information Champions	M	M		A	A	A	
	Head of Service (IAOs)	M	M		A	M	A	
	Executive Management including the Senior Information Risk Owner (SIRO) and the Caldicott Guardian	M	M				A	M
Non-Exec Directors	M	M				A	A*	

M – Mandatory

A - Advised

*Must be relevant to role. The training must be agreed through appraisals as a part of personal development necessary for the role before approaching Learning and Development.