

Training Needs Analysis for Information Governance Training

1. Document Control.

1.1. Document Approval

Document Control Sheet Title:		Training Needs Analysis for Information Governance Training	
Electronic File Name (if different from above):			
Consultation with:		L&OD	
Approval Level:		UCD Quality & Safety Committee/UCD Executive Committee/UCD Risk Committee (amend as per Document Development Policy)	
Dissemination Date:	TBC	Implementation Date:	
Method of Dissemination:		Via Operational Managers and Clinical Support Managers	
Distribution:		All operational/clinical and managerial staff	
<ul style="list-style-type: none"> Essential Reading for: 		All staff	

Author(s) (name and post):	[REDACTED], Head of Corporate Assurance with comments from [REDACTED] [L&OD]	
Approved by:	Function	Name
	DPO	[REDACTED]
	CG	Dr Jim Heptinstall
Version No:	V1.00	
Supersedes:		
Summary of Changes from Previous Version:		
Approval Date:	24/06/2021	
Review Date:		
Next review date:	24/06/22	

Contents

1. Document Control.....	2
1.1. Document Approval.....	2
2. Introduction	4
2.1. Purpose	4
2.2. Scope.....	4
3. Process	5
4	

2. Introduction

2.1. Purpose

The Department of Health has mandated the use of the NHS DSP Toolkit (DSPTK) for all NHS organisations' compliance. One of the requirements of the DSPTK is that all relevant staff complete their annual mandatory Information Governance (IG) Training to be taken between 01/04 and 31/03.

The NHS Information Governance Training Tool (IGTT) ensures a consistent and measurable approach to IG Training. There are a large variety of modules and these cover distinct areas of IG and can be related to various roles in the organisation

DSPTK identifies holistically the various requirements and standards for handling patient data and deals with the following areas:

- Confidentiality
- Information Security
- Records Management
- Data Quality
- Data Protection, Subject Access
- Freedom of Information

The organisation must continue to ensure and demonstrate that information is used legally and ethically and prove to be a trustworthy and considerate data custodian when carrying out the high-quality services that the organisation's reputation is based upon.

This Guidance ensures that the organisation

- will be compliant with the DSPTK requirements;
- that staff can demonstrate through the IGTT reports the required level of understanding; and
- that staff are provided with training on internal procedures that support the Information Governance agenda.

2.2. Scope

This Guidance applies to all staff, including contracted, non-contracted, temporary, honorary, secondments, agency, students, volunteers or locums.

3.5 Responsibilities

3.5.1 The Senior Information Risk Owner and Caldicott Guardian will, in conjunction with the Learning &

Development team;

- Issue prompts and updates to all staff via email, intranet, team meeting briefings and newsletters regarding completion of annual mandatory Information Governance Training as per this Guidance.
- Monitor staff completion of Information Governance Training.
- Issue periodical reports showing the organisational progress for Information Governance Training to the executive for discussion. The reports will be statistical only (no personal data) and obtained from the Learning & Development team.

Provide ad hoc reports to Line Managers for monitoring staff performance on the Information Governance Training Tool. The reports will provide detailed information for Line Managers staff and will show completion of modules. This will be for everyone the completion of the EI4H Data Security Awareness - Level 1, but for certain individuals it will include bespoke additional role specific training.

3.5.2 Line Managers are responsible for:

Confirming and monitoring that their staff have completed the relevant annual mandatory Information Governance Training via the Performance Development Review process.

Agreeing actions and associated timescales with staff that have not completed their identified training.

Agreeing any reasonable adjustments as required in the training delivery method or approach for staff if required for reason of disability or other factor, such as access to a computer for roles that do not have access at work, allowing allocated time in work to complete the assessment and IT assistance such as help in logging on to a computer.

3.5.3 Staff are responsible for:

Completing identified Information Governance Training within the specified timescales.

Keeping themselves informed and up to date about changes to all corporate policies and procedural documents.

Notifying their Line Manager when they cannot complete the identified Information Governance Training online as soon as possible.

3. Process

3.1 Training Needs Analysis

When?: Annual IG Training is a mandated requirement of the DSPTK. All the organisation's Line Managers must ensure that the appropriate modules are completed:

- During staff induction into the organisation
- When a change in role and/or responsibilities occurs
- As part of the annual staff performance development review

How?:

- New starters complete IG training on appointment as part of their induction.
- Staff will also have access to the IG Training Tool modules on Learning for Health via the intranet or external web access.
- This training will be supplemented by local IG workshops, coffee break bite size sessions and bulletins. These will be coordinated and facilitated via the divisional IG groups for standardisation of information shared.

Assurance:

- As part of a holistic approach to training delivery it is intended to assure staff understanding of IG through:
- Annual IG audits The Information Governance Lead may also request that additional Information Governance training is undertaken by relevant staff as a result of a security breach or Serious Incident Requiring Investigation (SIRI) involving information assets.
- The frequency that staff are expected to complete the IGTT modules is located at Appendix 1.

3.2 Minimum training requirements

The organisation has agreed that it cannot be assumed that any staff do not process Personal Identifiable Data (PID), and that as a minimum the following module is mandatory for all staff:

3.3 Data Security Awareness Level 1 e-learning package

The Data Security Awareness Level 1 e-learning package, which replaces the annual IG training provided through the IG Training Tool can be accessed for training through the intranet.

The organisation will accept equivalents from other providers (e.g. it's called information governance if completed on skills for health).

Certificates must be printed by staff and kept for review and provided to their line manager at the annual staff performance development review as proof of completion of training. Line managers are expected to encourage and remind staff to complete the relevant courses.

Certificates also need to be sent to L&OD for processing.

3.4 Implementation and compliance

- Information about this Guidance will be disseminated via e-mail, intranet, bulletins, website, staff meetings, team meeting briefings.
- All staff are obliged to adhere strictly to all the organisational policies and a failure to do so may lead to disciplinary action.
- Managers must ensure that staff are made aware of this Guidance, understand the Guidance and adhere to it.
- Implementation and compliance with this Guidance may be audited by the Information Risk Owner.
- The Department of Health will review compliance via access to the Information Governance Training Tool and Data Security and Protection Toolkit Submissions by the organisation.

4. Related Policies and Procedures

- Information Governance Security Policy V-IG992
- Records Management Policy P28
- Records Retention Policy V-IG976
- GDPR Handbook V-IG 966
- Information Security Handbook V-IG 972
- V-IG 757 Information Governance related Serious Incidents Requiring Investigation (IG SIRI) Policy

Other policies and procedures may become available during the lifespan of this policy.

- Related Guidance from external sources
- The NHS Code of Confidentiality

4. Appendices

Appendix 1

Information Governance Training Tool – Training Modules to be undertaken by staff.

All staff must undertake the Data Security Awareness Level 1 e-learning package, which replaces the annual IG training provided through the IG Training Tool, available for training on the intranet. This needs to be completed by all staff annually April to March

The relevant modules identified for each job role are mandatory and must be undertaken within six weeks of

being allocated and within every three years thereafter. The identified relevant modules are mandatory.

The courses relating to the role of the Caldicott Guardian, the role of the SIRO and introduction to risk management are provided by specialist organisations such as

www.advent-im.co.uk

<https://www.healthcareconferencesuk.co.uk/>

Modules	DSA level 1 eL4H	Role of Caldicott Guardian	Introduction to Risk Mgt
SIRO	Mandatory to all new staff, existing staff & contractors. Annually [April 1 st to 30 th march]	Recommended annually	Mandatory annually
Caldicott Guardian	Mandatory to all new staff, existing staff, & contractors. Annually [April 1 st to 30 th march]	Mandatory annually	Recommended [3 yearly]
DPO	Mandatory to all new staff, existing staff & contractors annually April 1 st to 30 th march]	Recommended	Mandatory [3 yearly]
Executive team	Mandatory to all new staff, existing staff & lay members. Annually April 1 st to 30 th march]	NA	Recommended
Information risk owner	Mandatory to all new staff, existing staff & contractors Annually April 1 st to 30 th march]	NA	Mandatory [3 yearly]
information asset owner	Mandatory to all new staff, existing staff & contractors Annually April 1 st to 30 th march]	NA	Mandatory [3 yearly]
All other staff	Mandatory to all new staff, existing staff & contractors Annually April 1 st to 30 th march]	NA	NA