



## NHS Oxfordshire Clinical Commissioning Group

<b>Policy</b>	<b>Information Governance Training Requirements Policy</b>
<b>Version Number</b>	2.0
<b>Version Date</b>	January 2019
<b>Review Date</b>	January 2021
<b>Responsible Owner</b>	OCCG Governance Manager
<b>Approving Body</b>	OCCG Exec Committee
<b>Target Audience</b>	All staff

### Document Control

#### Reviewers and Approvals

This document requires the following reviews and approvals:

<b>Name</b>	<b>Version Approved</b>	<b>Date Approved</b>
OCCG Information Governance Group	V2.0	
OCCG Executive Committee	V2.0	

### Revision History

<b>Version</b>	<b>Revision Date</b>	<b>Details of Changes</b>	<b>Author</b>
2.0	15/12/2018	Draft	Draft amendments in line with GDPR and the Data Protection Act 2018
2.0	January 2019	Review	OCCG Governance team

### Links or Overlaps with Other Key Documents and Policies

<b>Document Title</b>	<b>Version and Issue Date</b>	<b>Link</b>
Information Governance Staff Handbook	V2.0 Jan 2019	

### Acknowledgement of External Sources

<b>Title / Author</b>	<b>Institution</b>	<b>Link</b>

**Freedom of Information**

If requested, this document may be made available to the public and persons outside the healthcare community as part of OCCG's commitment to transparency and compliance with the Freedom of Information Act.

**Equality Analysis**

OCCG aims to design and implement services, policies and measures that are fair and equitable. As part of the development of this Policy, its impact on staff, patients and the public has been reviewed in line with OCCG's legal equality duties.

## **Model Guidance for Information Governance Training**

### **1. Purpose**

The Department of Health has mandated the use of the NHS Data Security Protection 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.

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 CCG 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 CCG's reputation is based upon.

This Guidance ensures that the CCG:

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

### **2. Scope**

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

### **3. Guidance**

#### **3.1 Training Requirements**

Annual IG Training is a mandated requirement of the DSPTK. All Line Managers must ensure that staff are compliant:

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

New starters complete IG training on appointment as part of their induction. This training will be supplemented by IG Training Seminars and attendance at staff meetings by the IG Manager.

### **How to complete Information Governance Training:**

The Data Security Awareness Level 1 e-learning package is live on [Consult OD](#) All staff must undertake this training on an annual basis and pass the mandatory test. The training is easy to follow with a short assessment at the end of each module. It should take approximately 1 hour to complete.

#### Annual IG audits

The Information Governance Lead with the approval of the Oxfordshire CCG Information Governance Group (IGG) 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.

Training requirements for specialist IG roles are outlined in appendix 1

## **3.2 Responsibilities**

### 3.2.1 The IG Lead will:

- Issue prompts and updates to all staff via email, intranet, team meeting briefings and newsletters regarding completion of annual mandatory Information Governance Training. Consult OD will also send reminders to staff to complete IG training when their training is due.
- Monitor staff completion of Information Governance Training.
- Update the Information Governance Group, Line Managers and Directors as appropriate.

### 3.2.2 Line Managers are responsible for:

- Confirming and monitoring that their staff have completed the relevant annual mandatory Information Governance Training via the appraisal process.
- Agreeing actions and associated timescales with staff that have not completed their identified training.

### 3.2.3 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.

### **3.3 Implementation and compliance**

3.3.1 The Department of Health will review compliance via access to the Information Governance Training Tool and Data Security and Protection Toolkit Submissions by the CCG.

## Appendix 1

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

#### Training Requirements 2018/19

Modules	Data Security Awareness Lv1 e-LfH modules Consult OD link	The Role of the Caldicott Guardian - Workbook	Introduction to Risk Management for SIROs and IAOs	Access to Health Records - Workbook
Senior Information Risk Owner	<b>Mandatory</b> To all existing staff or contractors	<b>Recommended</b>	<b>Mandatory Annual</b>	Recommended
Caldicott Guardian	<b>Mandatory</b> To all existing staff or contractors	<b>Mandatory Annual</b>	Recommended	Recommended
Data Protection Officer	<b>Mandatory</b> To all existing staff or contractors	<b>Recommended</b>	<b>Mandatory 3 yearly</b>	Recommended
Executive Team & Lay Members	<b>Mandatory</b> To all existing staff or contractors		Recommended	Recommended
Information Asset Owners	<b>Mandatory</b> To all existing staff or contractors		<b>Mandatory 3 yearly</b>	Recommended
Data Custodians/Information Asset Administrators	<b>Mandatory</b> To all existing staff or contractors		Recommended	Recommended
All Staff	<b>Mandatory</b> To all existing staff or contractors			<b>Mandatory</b> (if the team manages records)

Colour code: **Complete once** – **Complete annually** – **Complete every 3 years**