Data Protection: e-learning training course

This e-learning course is intended to emphasise the importance of processing information effectively, securely and according to set policies and procedures. Learners will explore the different ways in which they process data through the course of their work and identify the reasons why it must be handled and managed correctly. They will also be given the opportunity to familiarise themselves with, and gain a better understanding of, the guidelines, policies and legal requirements in place which set out how information must be governed in their workplace.

The online materials include quizzes and exercises to help reinforce learning.

There is also an online assessment to test students' understanding of the topic on completion of the course.

Unit Titles and Descriptions

Unit 1 – How to use the course

Unit 2 - An Introduction to Information Governance

This unit emphasises the importance of building and maintaining an effective information governance framework. After completing this unit learners will understand that organisations handling personal information belonging to service users and personnel must handle it securely and appropriately at all times and have a clear management accountability structure in place. The unit goes on to inform learners what their responsibilities are under the Data Protection Act, Freedom of Information Act and Caldicott principles.

Unit 3 - The Legal Framework

This unit explains how to comply with various legal requirements as stipulated by the Information Commissioner's Office (ICO). After completing this unit, learners will understand the definition of 'personal data' and how the legal framework affects the way organisations handle and manage this type of information.

Unit 4 - Maintaining Confidentiality

This unit helps learners focus on how they can contribute to maintaining confidentiality during the course of their everyday work. Learners will look at:
1. what makes information confidential
2. how staff can safeguard against breaching confidentiality and consider the consequences of people failing to comply with the policies and procedures in place
3. the purpose of a Confidentiality Statement.

Unit 5 - Information Security and Communication Policy

The purpose of this unit is to help learners familiarise themselves with their organisation's Information Security and Communication Policy. The unit explains why all staff need to understand and comply with its requirements and that failure to do so could lead to disciplinary action.

Topics covered include:
- how changes in service provision and technology have had an impact on information governance and data protection
- the purpose of an Information Management Policy
- definitions of the terms 'processing', 'confidential', 'personal' and 'sensitive' in relation to data
- the purpose and requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000
- staff and service users' rights under the Data Protection Act
- an introduction to and explanation of the Caldicott principles
- the purpose and content of an organisation's Confidentiality Statement and Information Security and Communication Policy and the consequences of failing to comply with them.