

Data Security and Protection eLearning – Leads

Update notice October 2026

Content updates

Module 1: Data protection rights and responsibilities

Section	Original content	Updated content
Do you have what you need?	Scenario: Alex needs more help and support	Link to local support partners updated to https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/better-security-better-care/local-support-partners/
Additional resources	Link to local support partners under Sources of additional support and information	Link updated to https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/better-security-better-care/local-support-partners/

Module 2: Keeping data secure

Section 2.1 Managing data

Section	Original content	Updated content
Sharing	Messaging apps	Section updated to include reference to photos
	Generative AI	Section renamed to Open AI tools and content and images updated. Link to

Section	Original content	Updated content
		Digital Care Hub guidance on the use of AI in social care. New scenario added about use of open AI tools. Alex is the Data Security and Protection Lead for Acer Homecare. Alex finds out that a senior care worker is using ChatGPT to write care plans. What should Alex do? New section Closed AI tools. Definition, controls and risks. New section New AI features. Guidance.
Destruction	Advice on retention	New central paragraph added: Your retention timetable should include digital records as well as paper records. It should also consider the places where personal data might be stored, for example photos or downloaded documents on phones.

Section 2.2 Managing risks

Section	Original content	Updated content
Owning the risk assessment process	Exercise: Do you need to complete a DPIA?	New option added: Migrating from one electronic care records system to another? Answer = Yes. This type of change can pose a risk to individuals' rights and freedoms. A DPIA will help you to understand and plan for the potential risks.

Section	Original content	Updated content
	When to carry out a DPIA – link to ICO guidance	Link updated to: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
Additional resources	Link to Information about Data Protection Impact Assessments	Link updated to: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

Module 3: Threats to data security

Section	Original content	Updated content
The cyber security threat	Statistical context "The 2024 National Cyber Security Breaches Survey found that half of businesses had a cyber security breach or attack in the last year."	Text updated: "The 2025-2026 National Cyber Security Breaches Survey found that 43% of businesses had a cyber security breach or attack in the last year."
Preparing for cyber threats	Backups	New item added: Check supplier backups If you're relying on your IT system supplier to make backups of your data, check their arrangements including what they do to test the restore process.
Prevention of cyber threats	Anti-virus software:	Advice updated to:

Section	Original content	Updated content
	"For example, Windows 10 has a product called 'Defender' which will help make your computer safer from malware: ensure it's turned on. There are many anti-malware products available to download on a paid for basis and some are even free. McAfee, Norton and Sophos are just a few well-known names."	"Windows 11 includes 'Microsoft Defender' antivirus software: make sure it's turned on if you don't have any other antivirus installed. There are other free and paid for antivirus/anti-malware products available to download. Bitdefender, Malwarebytes, McAfee, Norton and Sophos are just a few well-known names."
Digital devices	Implementing Bring Your Own Device (BYOD) link to Cyber Essentials guidance	Link updated to: https://ce-knowledge-hub.iasme.co.uk/space/CEKH/2651652226/Guidance+to+BYOD
The digital supply chain	Page title: The digital supply chain Introduction Working with external suppliers Due diligence on your digital supply chain ISO	Page title updated to: IT Suppliers and images updated. Introduction updated to include examples of systems and legal responsibilities. Section renamed to: How to manage your suppliers. Text updated to include links to Digital Care Hub supplier list template and third-party contracts. Section renamed to: IT supplier due diligence Heading updated to: ISO27001

Section	Original content	Updated content
	Data security and protection toolkit Scenario: Assessing technology suppliers	Links added: UK's CertCheck https://certcheck.ukas.com/ and CertSearch https://www.iafcertsearch.org/ Heading updated to: NHS Data security and protection toolkit Information added on the NHS Assured Solutions List Link added to Digital Care Hub guidance on managing suppliers Scenario revised to Alex checks an IT system supplier. Alex is the Data Security and Protection Lead for Acer Homecare. Alex discovers that one of Acer's IT systems suppliers does not have any cyber security certification. What should Alex do? New section Think about the risks Risks your organisation could face if it doesn't check an IT supplier before using them
Additional resources	Link to Guidance on allowing employees to use their own devices for work purposes (Bring Your Own Device)	Link updated to: https://ce-knowledge-hub.iasme.co.uk/space/CEKH/2651652226/Guidance+to+BYOD

Module 4: Data breaches

Section	Original content	Updated content
What is a data breach?	What is the biggest cause of data breaches? "The most common reason for a data breach in 2023 was 'data emailed to the incorrect recipient' "	Text updated to: "In 2025 a quarter of all data breaches were 'data emailed to the incorrect recipient'. "
Minimising the risk of data breaches	Introduction "There were 2236 reported to the Information Commissioners' Office (ICO) in 2023 by the health and social care sectors. This is an increase of 14% compared to 2022."	Text updated to focus on the social care sector specifically: "There were 479 reported to the Information Commissioners' Office (ICO) in 2025 by the social care sector. This is an increase of 21% compared to 2024."
Responding to a data breach	How to respond to a data breach, step 4, link to National Cyber Security Centre guidance on data breaches	Link updated to: https://www.ncsc.gov.uk/sites/default/files/documents/ncsc-data-breaches-infographic.pdf
Additional resources	Additional information and guidance about responding to a data breach, link to National Cyber Security Centre guidance on data breaches	Link updated to: https://www.ncsc.gov.uk/sites/default/files/documents/ncsc-data-breaches-infographic.pdf

Assessment

- **New Assessment module added**, 20 multiple choice questions, learner must achieve 80% correct answers or more to pass and download a certificate

Other updates

- 'That's not quite right' title in module question responses, where the learner would have chosen at least one correct option, reworded to 'That's not quite right'
- Minor corrections e.g. typos