OCR
Oxford Cambridge and RSA

Unit Title:	**IT security for users**
OCR unit number:	42
Level:	1
Credit value:	1
Guided learning hours:	10
Unit reference number:	R/502/4256

Unit purpose and aim

This is the ability to protect hardware, software and the data within an IT system against theft, malfunction and unauthorised access.

This unit is about the skills and knowledge needed by the IT User to identify day-to-day security risks and the laws and guidelines that affect the use of IT; and use simple methods to protect software and personal data (e.g. risks from people getting access to it who are not authorised, from viruses or from hardware not working properly).

Learning Outcomes	Assessment Criteria	Examples
The learner will: 1 Use appropriate methods to minimise security risks to IT systems and data	The learner can: 1.1. Identify security issues that may threaten system performance 1.2. Take appropriate security precautions to protect IT systems and data 1.3. Identify threats to information security associated with the widespread use of technology 1.4. Take appropriate precautions to keep information secure 1.5. Follow relevant guidelines and procedures for the secure use of IT 1.6. Describe why it is important to backup data securely 1.7. Ensure personal data is backed up to appropriate media	Threats to system performance: Unwanted e-mail (often referred to as "spam"), malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers) and hackers; hoaxes Security precautions: Use access controls: Physical controls, locks, passwords, access levels; Run anti-virus software, adjust firewall settings, adjust internet security settings; carry out security checks, report security threats or breaches; backup; store personal data and software safely; treat messages, files, software and attachments from unknown sources with caution Threats to information security: From theft, unauthorised access, accidental file deletion, use of removable storage media; malicious programs (including viruses, worms, trojans, spyware, adware and

Learning Outcomes	Assessment Criteria	Examples
		rogue diallers), hackers, phishing and identity theft Keep information secure: Username and password/PIN selection, how and when to change passwords; Respect confidentiality, avoid inappropriate disclosure of information Widespread use of technology: Unsecured and public networks, default passwords and settings, wireless networks, Bluetooth, portable and USB devices Guidelines and procedures: Set by: employer or organisation; privacy

Assessment

All ITQ units may be assessed using any method, or combination of methods, which clearly demonstrates that the learning outcomes and assessment criteria have been met. Assessments must also take into account the additional information provided in the unit Purpose and Aims relating to the level of demand of:

- the activity, task, problem or question and the context in which it is set;
- the information input and output type and structure involved; and
- the IT tools, techniques or functions to be used.

See the Assessment and postal moderation section of the ITQ Centre Handbook.

Evidence requirements

Candidates must complete the Evidence Checklist without gaps for this unit. Individual unit checklists are available to download from the qualification webpage (see forms).

Guidance on assessment and evidence requirements

Please refer to the ITQ centre handbook on our webpage.

Details of relationship between the unit and national occupational standards

This unit maps fully to competences outlined in IT User National Occupational Standards version 3 (2009).