OCR
Oxford Cambridge and RSA

Unit Title:	**Internet safety for IT Users**
OCR unit number:	91
Level:	1
Credit value:	3
Guided learning hours:	20
Unit reference number:	H/502/9154

Unit purpose and aim

This unit is about the skills and knowledge required by the IT user to work safely and responsibly online in the context of activities that are routine and familiar.

As a result of this unit, the candidate will understand the risks of working online and be able to take appropriate precautions to safeguard themselves and others and protect data and IT systems.

Learning Outcomes	**Assessment Criteria**	**Examples**
The learner will:	The learner can:	
1 Understand the risks that can exist when using the Internet	1.1 Identify risks to user safety and privacy	Risks to user safety: abusive behaviour (“cyberbullying”), inappropriate behaviour and grooming; abuse of young people; false identities; financial deception
	1.2 Identify risks to data security	Risks to data security: Theft of data, hacking, accidental deletion or change to data, Trojans, spyware, adware, phishing, identify theft, avatars, mobile technology i.e. wireless and Bluetooth, default passwords, portable devices e.g. USB devices
	1.3 Identify risks to system performance and integrity	Risks to system performance: unwanted e-mail (often referred to as “spam”), worms, viruses, spyware, adware, denial of service, hacking of systems, Trojans, spam
	1.4 Outline how to minimise Internet risks	Minimise risk: virus-checking software, anti-spam software, firewall; treat messages, files, software and attachments from unknown sources with caution, internet settings, block sites, parental controls

Learning Outcomes	Assessment Criteria	Examples
	1.5 Outline factors that affect the reliability of information on websites	Reliability: accuracy, currency, sufficiency, synthesise information from a variety of sources. Recognise intention and authority of provider, bias, level of detail; relevance
2 Know how to safeguard self and others when working online	2.1 Take appropriate precautions to ensure own safety and privacy 2.2 Protect personal information online 2.3 Carry out checks on others' online identity 2.4 Describe the forms and features of cyberbullying 2.5 Identify when and how to report online safety issues 2.6 Identify where to get online help and information on e-safety	Precautions: selection and management of username, password or PIN, including reasons for changing passwords or PINs, length and complexity of passwords; online identity profile, access levels to information, confidentiality, content filtering, proxy servers, monitoring and reporting user behaviour Personal information: username and password/PIN selection and management, password strength, online identity/profile; Real name, pseudonym, avatar; What personal information to include, who can see the information, withhold personal information Cyberbullying: chat rooms, e-mail and instant messaging Safety issues: abusive behaviour (“cyberbullying”), inappropriate behaviour and grooming; abuse of young people; false identities; financial deception E-safety: service provider, legal system, parental controls
3 Take precautions to maintain data security	3.1 Take appropriate precautions to maintain data security	Data security: Use access controls. Configure anti-virus software, 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

Learning Outcomes	Assessment Criteria	Examples
		attachments from unknown sources with caution; proxy servers; download security software patches and updates. Loss or theft of valuable and possibly irreplaceable data, cost of replacing lost data. A range of effective backup procedures
	3.2 Take appropriate precautions to maintain system performance and integrity	System performance: Set passwords, physical access controls i.e. keypads or locks, anti-virus software, adjust firewall settings, carry out security checks, report security threats and breaches, back up data and software and store appropriately, identify and report possible security threats, download and install software patches and updates, treat messages, files, software and data from unknown sources with caution, proxy servers
	3.3 Use appropriate browser safety and security settings 3.4 Use appropriate client software safety and security settings	Settings: autofill, cookies, security, pop-ups, appearance, privacy, search engine, toolbars, personalisation, accessibility; software updates, temporary file storage Security guidelines and procedures: Information security policies, procedures and guidelines set by the centre or organisation, careful disposal of information items, legal requirements, security products Protect systems and data: Access controls: physical controls, locks, passwords, access levels. Security measures: anti-virus software, firewalls, security software and settings. Risk assessment; anti-spam software, software updates

Learning Outcomes	Assessment Criteria	Examples
4 Follow legal constraints, guidelines and procedures which apply when working online	4.1 Identify legal constraints on the uploading and downloading of software and other digital content 4.2 Identify legal constraints on online behaviour 4.3 Correctly observe guidelines and procedures for the safe use of the Internet	Laws: relating to copyright, software download and licensing, digital rights, IPR, Health and Safety, Children legislation, Data Protection Guidelines and procedures: Set by employer or organisation relating to Health and Safety, security; equal opportunities, disability

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.

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. Where candidates are submitting evidence produced having sat an OCR-set WebWise test, there is no need to complete an evidence checklist. 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 links to the IT User National Occupational Standard detailed below:

Occupational standards	Title
IT Users 2009 (e-skills UK)	IT User Fundamentals IT Communication Fundamentals Using the Internet Using Email IT security for users