Ascentis Level 1 Award in Internet Safety for IT Users Specification

Ofqual Number	**600/3240/6**
Ofqual Start Date	01/11/2011
Ofqual Review Date	31/07/2020
Ofqual Certification Review Date	31/07/2021

ABOUT ASCENTIS

Ascentis was originally established in 1975 as OCNW, a co-operative scheme between Universities and Colleges of Further Education. Ascentis was the first 'Open College' in the UK and served the needs of its members for over 34 years. Throughout this period, OCNW grew yet maintained its independence in order that it could continue to respond to the requirements of its customers and provide a consistently high standard of service to all centres across the country and in recent years to its increasing cohorts of overseas learners.

In 2009 OCNW became Ascentis - a company limited by guarantee and a registered educational charity.

Ascentis is distinctive and unusual in that it is both:

- **An Awarding Organisation** regulated by the Office of Qualifications and Examinations Regulation (Ofqual, England), Council for the Curriculum, Examinations and Assessment (CCEA, Northern Ireland) and Qualifications Wales

and

- **an Access Validating Agency (AVA)** for 'Access to HE Programmes' licensed by the Quality Assurance Agency for Higher Education (QAA).

Ascentis is therefore able to offer a comprehensive ladder of opportunities to centres and their students, including Foundation Learning, vocational programmes and progressing to QAA-recognised Access to HE qualifications. The flexible and adult-friendly ethos of Ascentis has resulted in centres throughout the UK choosing to run its qualifications.

ASCENTIS CONTACT DETAILS

Ascentis
Office 4
Lancaster Business Park
Mannin Way
Caton Road
Lancaster
LA1 3SW

Tel: 01524 845046
www.ascentis.co.uk

Company limited by guarantee. Registered in England and Wales No. 6799564. Registered Charity No. 1129180

TABLE OF CONTENTS

ASCENTIS LEVEL 1 AWARD IN INTERNET SAFETY FOR IT USERS

Introduction

The Ascentis Level 1 Award in Internet Safety for IT Users qualification is designed to give learners the knowledge and understanding of the basic principles of internet safety including understanding the risks associated with using the internet, safeguarding self and others when working online, maintaining data security and following guidelines and procedures.

There are several features of this qualification that make it very appropriate for its target learners

- Assessment and certification can be offered throughout the year, allowing maximum flexibility for centres
- Can be delivered either as a classroom based course or as a blended learning programme
- Assessment is by a multi choice test, offered on screen or paper based. This will normally be taken at the end of the course
- There are online resources that can be used alongside the teaching

Aims

The aims of the qualification are to enable learners

1 To understand the risks that can exist when using the internet

2 To understand how to safeguard self and others when working online

3 To know how to maintain data security

4 To follow guidelines and procedures which apply when working

Target Group

The qualification is aimed at a range of learners, including

- Young people wishing to pick up an award as part of another learning programme
- Young people aged 14 – 19 who are in various learning environments

Regulation Codes

Ofqual Qualification Number (Ofqual/CCEA): 600/3240/6

Award of the Qualification

Learners must complete one unit for the Award in Internet Safety for IT Users. This is a single unit qualification and certification is given for achieving a pass in the external assessment.

Ascentis Level 1 Award in Internet Safety for IT Users				
Title	**Level**	**Credit Value**	**TQT**	**Unit ref**
Internet Safety for IT Users	1	3	31	H/502/9154

Recommended Guided Learning Hours

The recommended guided learning hours for this qualification is 30

Total Qualification Time

The total qualification time for this qualification is 31

Recommended Prior Knowledge, Attainment and/or Experience

No recommended prior learning or experience is required.

Age Range of Qualification

This qualification is suitable for young people aged 14-19 and adult learners.

Opportunities for Progression

The qualification gives the learner an introduction to Internet Safety which can be applied in a wide variety of contexts. Learners may use the qualification as a stand-alone course or as part of a longer vocational or academic programme of study. Learners may also use the qualification as an element of their continuing professional development.

Resources to Support the Delivery of the Qualification

There are online resources available to download to support this qualification.

Centre Recognition

This qualification can only be offered by centres recognised by Ascentis and approved to run this qualification. Details of the centre recognition and qualification approval process are available from the Ascentis office (tel. 01524 845046) or from the website at www.ascentis.co.uk.

Qualification Approval

If your centre is already a recognised centre, you will need to complete and submit a qualification approval form to deliver this qualification. Details of the qualification approval process are available from the Ascentis office (tel. 01524 845046) or from the website at www.ascentis.co.uk.

Registration

All learners must normally be registered within 15 working days of the intended test date for paper based assessment and 5 working days for e-assessment.

Registration is via the Ascentis electronic registration portal.

Re-sits

Learners can re-sit the assessment if they do not achieve a pass but should have sufficient time for additional learning. Re-sits for e-assessment are free of charge, but please refer to the pricing structure for re-sits of the paper based tests.

Status in England, Wales and Northern Ireland

This qualification is available in England and Wales. It is only offered in English. If a centre based overseas (including Scotland and Northern Ireland) would like to offer this qualification, they should make an enquiry to Ascentis.

Reasonable Adjustments and Special Considerations

In the development of this qualification Ascentis has made every attempt to ensure that there are no unnecessary barriers to achievement. For learners with particular requirements reasonable adjustments may be made in order that they can have fair assessment and demonstrate attainment. There are also arrangements for special consideration for any learner suffering illness, injury or indisposition. Full details of the reasonable adjustments and special considerations are available from the Resources/Key Documents area of the Ascentis website www.ascentis.co.uk or through contacting the Ascentis office.

Enquiries and Appeals Procedure

Ascentis has an appeals procedure in accordance with the regulatory arrangements in the Ofqual *General Conditions of Recognition*[1]. Full details of this procedure, including how to make an application, are available from the Resources/Key Documents area of the Ascentis website www.ascentis.co.uk or through contacting the Ascentis office.

[1] In Northern Ireland it is the CCEA General Conditions of Recognition and Qualifications Wales is the Standard Conditions of Recognition.

ASSESSMENT AND VERIFICATION ARRANGEMENTS

Overview

To gain the Level 1 Award in Internet Safety for IT Users all learning outcomes and assessment criteria within the unit must be successfully achieved. The full award consists of one unit.

External Assessment

This qualification is assessed through the completion of an Ascentis devised multiple choice test that is carried out at the completion of the course, available as a paper based test or e-assessment.

The grading of this qualification is pass or did not achieve.

Conduct of Assessment

The assessment is through a 40-minute test paper or e-assessment consisting of 20 multiple-choice questions.

Full details of candidate, Examinations Officer and invigilator instructions are available from the Resources/ Key Documents area of the Ascentis website www.ascentis.co.uk or through contacting the Ascentis office.

Note: Dictionaries cannot be used during the assessment.

Quality Assurance Arrangements

As part of ongoing quality assurance arrangements, Ascentis will carry out quality visits to recognised centres using a risk based approach. The focus of quality visits will normally be

- Review of resources; both physical and staffing
- Observation of assessment practice
- Staff development, if required

Further details will be provided prior to a visit taking place.

Ascentis reserve the right to carry out inspections of assessments taking place without prior notice.

The delivery of the knowledge required within this qualification should be carried out by qualified teachers or those working towards a teaching qualification. Delivery staff should also have a theoretical understanding of IT User Skills.

Results

Provisional results are provided immediately after e-assessment. An hour after the e-assessment the e-assessment achievement list report can be run through QuartzWeb

Knowledge, Understanding and Skills required of Assessors and Internal Verifiers

Centres must ensure that those delivering and assessing Ascentis qualifications are occupationally knowledgeable and competent within the relevant subject area.

Centres are responsible for ensuring that all staff involved in the delivery of the qualification are appropriately qualified. Ascentis will not be held responsible for any issues that relate to centre staffing which could impact on the successful delivery, assessment and internal quality assurance of our qualifications.

Those delivering the qualification should preferably hold or be working towards a recognised teaching qualification. Assessors must be able to make appropriate assessment decisions. Internal Quality Assurers need to have knowledge and experience of the internal quality assurance processes.

Centres are required to ensure that appropriate training and support is in place for staff involved in the delivery, assessment and internal verification of Ascentis qualifications.

Ascentis offers free support for centres. Further information on the support that is available can be found on Quartz Web or the Ascentis website.

Internet Safety for IT Users

Credit Value of Unit 3	GLH of Unit 30	Level of Unit 1

Introduction

This unit gives the learner knowledge and understanding of the basic principles of internet safety including understanding the risks associated with using the internet, safeguarding self and others when working online, maintaining data security and following guidelines and procedures.

Learning Outcomes The learner will be able to	Assessment Criteria The learner can
1 Understand the risks that can exist when using the internet	1.1 Identify risks to user safety and privacy
	1.2 Identify risks to data security
	1.3 Identify risks to system performance and integrity
	1.4 Outline how to minimise internet risks
	1.5 Outline factors that affect the reliability of information on websites
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
3 Take precautions to maintain data security	3.1 Take appropriate precautions to maintain data security
	3.2 Take appropriate precautions to maintain system performance and integrity
	3.3 Use appropriate browser safety and security settings
	3.4 Use appropriate client software safety and security settings
4 Follow legal constraint, 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

Indicative Content
User safety and privacy risks to user safety – fraudulent soliciting for money; harassment and cyber bullying; exposure to inappropriate content; racist or hate material; identity theft **Risks to data security** – spam; adware; spyware; phishing; hoaxes; cookies; social engineering; ways to prevent phishing and scamming; reporting phishing and scamming **Risks to system performance –** malware; firewalls; updating and patching **Protecting computers and data** - practising diligence when using computers; installing appropriate anti-spam software; installing other appropriate security software; turning on firewall; protecting personal information; browser safety; client software **Information on websites** – reliability of information on websites; Wikis; websites; social networking sites **Safeguarding self and others when working online** **Risks and dangers online –** exposure to inappropriate content; age inappropriate content; cyber bullying; befriending unknown people; grooming and sexting; sharing personal information; gambling and debts **Precautions to ensure own safety and privacy –** care with email attachments; not opening pop ups; avoiding emails from unknown sources; not visiting suspect sites **Protecting Personal information** – name; address; email address; bank details; credit card details **Checking others' identity –** Online person search; ask questions; use search engine **Cyber bullying** – effects of cyber bullying on people **Reporting cyber bullying -** When to report; who to report to **Sources of information about cyber bullying** – Specialist websites **Precautions to maintain data security** – beware of phishing; care when giving bank or credit card details; good firewall; regularly updating antivirus software **Precautions to maintain system performance and integrity** – care with email attachments; not opening pop ups; avoiding emails from unknown sources; not visiting suspect sites; anti-malware software **Browser and security settings** – Turn on firewall; spam filter; blocked site list; privacy settings **Client software safety and security settings** – This will alter from package to package but the software instruction manual (paper based or onscreen) should be read to discover which settings are available to change **Legal constraints, guidelines and procedures relevant to working online** **Legal constraints on uploading and downloading software and other digital content** – Copyright; Data Protection Act **Legal constraints on online behaviour** – cyber bullying, protection of children; libellous behaviour; etiquette **Guidelines and procedures for safe use of the internet –** security patches; firewalls; dealing with unexpected emails; use and protection of passwords; blocking websites and web content; chatroom monitoring; backing up data; data encryption **User safety and privacy risks to user safety** – fraudulent soliciting for money; harassment and cyber bullying; exposure to inappropriate content; racist or hate material; identity theft **Risks to data security** – spam; adware; spyware; phishing; hoaxes; cookies; social engineering; ways to prevent phishing and scamming; reporting phishing and scamming **Risks to system performance –** malware; firewalls; updating and patching **Protecting computers and data** - practising diligence when using computers; installing appropriate anti-spam software; installing other appropriate security software; turning on firewall; protecting personal

information; browser safety; client software
Information on websites – reliability of information on websites; Wikis; websites; social networking sites

Safeguarding self and others when working online
Risks and dangers online – exposure to inappropriate content; age inappropriate content; cyber bullying; befriending unknown people; grooming and sexting; sharing personal information; gambling and debts
Precautions to ensure own safety and privacy – care with email attachments; not opening pop ups; avoiding emails from unknown sources; not visiting suspect sites
Protecting Personal information – name; address; email address; bank details; credit card details
Checking others' identity – Online person search; ask questions; use search engine

Cyber bullying – effects of cyber bullying on people

Reporting cyber bullying - When to report; who to report to

Sources of information about cyber bullying – Specialist websites

Precautions to maintain data security – beware of phishing; care when giving bank or credit card details; good firewall; regularly updating antivirus software

Precautions to maintain system performance and integrity – care with email attachments; not opening pop ups; avoiding emails from unknown sources; not visiting suspect sites; anti-malware software

Browser and security settings – Turn on firewall; spam filter; blocked site list; privacy settings

Client software safety and security settings – This will alter from package to package but the software instruction manual (paper based or onscreen) should be read to discover which settings are available to change

Legal constraints, guidelines and procedures relevant to working online
Legal constraints on uploading and downloading software and other digital content – Copyright; Data Protection Act

Legal constraints on online behaviour – cyber bullying, protection of children; libellous behaviour; etiquette

Guidelines and procedures for safe use of the internet – security patches; firewalls; dealing with unexpected emails; use and protection of passwords; blocking websites and web content; chatroom monitoring; backing up data; data encryption

Sample Questions

Level 1 Award in Internet Safety for IT Users

1) Sending threatening or abusive emails to someone is called:

a) danger email
b) cyberbullying
c) just a bit of fun
d) electronic threat

2) Which one of the following is a symptom of spyware?

a) a magnifying glass icon appears on your desktop
b) your keyboard stops working
c) your computer won't switch on
d) internet access is sluggish

3) Using emails and websites to fool people into giving personal information is called:

a) phishing
b) social networking
c) software
d) piracy

4) When leaving your laptop or computer for a short while, you should always:

a) just leave it 'unlocked' and logged on
b) email your friends to tell them you'll be back in a moment
c) use the 'lock' function
d) put a cover over the screen

5) You get an email telling you that you have won a large amount of money. All you need to do is send your bank account details so that you can receive the money. What do you do?

a) Delete the email. This is a fraudulent email
b) You're a winner! Send your details immediately
c) Reply but ask for further information before you send your bank details
d) Send your bank details but keep a record of the email for proof

6) Using copyrighted works online without permission, e.g. copyrighted music, is called:

a) cyberbullying
b) spam email
c) online piracy
d) uploading

7) Which of the following provides you with internet security?

a) a screensaver
b) a webcam
c) an anti-spyware program
d) a social networking website

8) A type of virus designed to use up all of a computer's memory is called a:

a) mega-virus
b) a worm
c) spam
d) a mole

9) How can you prevent having to open and to read so much spam?

a) activate a junk email folder in your inbox
b) send less emails
c) switch off your computer overnight
d) always give out false details

10) Which of the following is a legal way to get music?

a) rip a friend's CD
b) download from a P2P (peer to peer) website
c) buy from a site such as iTunes
d) none of the above