



Ascentis Entry Level Award (Entry 3) in Skills for Digital Transactions Specification

Ofqual Number: 603/4619/X

Ofqual Start Date: 01/06/2019

Ofqual Review Date: 31/07/2027

Ofqual Certification Review Date: 31/07/2028

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 House
Lancaster Business Park
3 Mannin Way
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 ENTRY LEVEL AWARD (ENTRY 3) IN SKILLS FOR DIGITAL TRANSACTION

Introduction	4
Aims	4
Target Group	4
Regulation Codes	4
Rules of Combination	5
Guided Learning Hours (GLH) and Total Qualification Time (TQT)	5
Time Limit for the Process of Credit Accumulation and Exemptions	5
Recommended Prior Knowledge, Attainment and / or Experience	5
Age Range of Qualification	5
Opportunities for Progression	5
Centre Recognition	5
Qualification Approval	6
Registration	6
Status in England, Wales and Northern Ireland	6
Reasonable Adjustments and Special Considerations	6
Enquiries and Appeals Procedure	6

ASSESSMENT AND VERIFICATION ARRANGEMENTS

Assessment	7
Internal Assessment	7
Verification	8
Internal Verification	8
External Verification	8
Knowledge, Understanding and Skills Required of Assessors and Internal Verifiers	8

UNIT SPECIFICATIONS

Entry 3 Digital Technology Fundamentals	9
Entry 3 Transacting Digitally	11
Appendix 1: Summary Record of Achievement	14
Appendix 2: Tracking Sheets	15

ASCENTIS ENTRY LEVEL AWARD (ENTRY 3) IN SKILLS FOR DIGITAL TRANSACTIONS

Introduction

This qualification focuses on the learner's ability to use computing and mobile devices to buy goods and services online and administer and manage transactions and finances online, all whilst staying safe legally and confidently.

The increase in the use of digital technology as a route for engagement and activity across government and business has led to both national and local government making significant investment in enhancing their digital infrastructure and making public services 'digital'. For individuals to actively participate in modern life, work and society it is vital that they acquire the necessary digital skills, and without them they will be at a significant disadvantage and unable to access the best goods and services.

The Ascentis Entry Level Award (Entry 3) in Skills for Digital Transactions has been designed in response to the Essential Digital Skills Framework as a 'taster' qualification which aims to develop and recognise learners' basic digital technology and transacting skills, and their ability to use them in their daily lives.

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

- Unit certification is available for each of the units
- Verification and certification can be offered throughout the year, allowing maximum flexibility for centres
- It can be delivered either as a classroom-based course or as a blended learning programme
- Evidence can be generated within a wide range of organisational contexts, allowing the qualification to meet the specific occupational requirements of the learners

Aims

The aim of this qualification is to enable learners:

1. To develop digital technology and transacting skills necessary for life, work and society
2. To buy goods and services online
3. To complete forms and transactions online
4. To register for online banking services
5. To adhere to online safety and security practices

Target Group

This 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
- Adult learners

Regulation Codes

Ofqual Regulation Number:

Ascentis Entry Level Award in Skills for Digital Transactions (Entry 3): 603/4619/X

Rules of Combination

Learners must complete both units for the Entry 3 Award in Skills for Digital Transactions.

Ascentis Entry Level Award in Skills for Digital Transactions (Entry 3)				
Title	Level	Credit Value	GLH	Unit ref
Digital Technology Fundamentals	Entry 3	1	10	R/617/6239
Transacting Digitally	Entry 3	2	20	H/617/6245

Guided Learning Hours (GLH)

The recommended guided learning hours for this qualification is 30.

Total Qualification Time (TQT)

The total qualification time for this qualification is 30.

Time Limit for the Process of Credit Accumulation and Exemptions

Credit accumulation is usually within the life span of this qualification.

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

Learners may progress from these Awards to Ascentis qualifications in the Digital suite.

Centre Recognition

This qualification can only be offered by centres recognised by Ascentis and approved to run these qualifications. 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 with Ascentis within seven weeks of commencement of a course via the Ascentis electronic registration portal. Late registration may result in a fee; refer to the latest version of the product catalogue.

Status in England, Wales and Northern Ireland

This qualification is available in England. They are only offered in English. If you wish to deliver it in any other nation, please contact development@ascentis.co.uk.

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 reasonable adjustments and special considerations are available from the login 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 login area of the Ascentis website (www.ascentis.co.uk) or through contacting the Ascentis office.

Useful Links

Web links and other resources featured in this specification are suggestions only to support the delivery of this qualification and should be implemented at the centre's discretion. The hyperlinks provided were live at the time this specification was last reviewed. Please kindly notify Ascentis if you find a link that is no longer active.

Please note: Ascentis is not responsible for the content of third-party websites and, whilst we check external links regularly, the owners of these sites may remove or amend these documents or web pages at any time.

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

ASSESSMENT AND VERIFICATION ARRANGEMENTS

Assessment

All units are internally assessed through the learner building up a portfolio of evidence that covers the relevant assessment criteria. They are internally assessed and verified by the centre and then externally verified by Ascentis.

On completion of the learners' evidence for the Award, the assessor is required to complete the Summary Record of Achievement for each learner. The Summary Record of Achievement asks assessors and the internal verifier to confirm that the rules of combination have been followed. This is particularly important in cases where a learner has taken units at different levels. The Summary Record of Achievement form is provided in [Appendix 1](#).

Centres are required to retain all evidence from all learners for external verification and for four weeks afterwards should any appeal be made.

Internal Assessment

Evidence for each unit is through building up a portfolio of evidence to demonstrate that all the assessment criteria within the unit have been achieved. The evidence will be assessed by the assessor at the centre, who may or may not be the tutor teaching the course.

Portfolios of evidence should include a variety of evidence to demonstrate that the assessment criteria for each unit have been met. Examples of evidence that could be included are:

- Observation record
- Questions and discussions
- Photographs
- Video
- Worksheets
- Audio recordings
- Self assessments
- Workbook activities

If the learner fails to meet the assessment criteria on the first attempt at an activity they may redraft the work following feedback given by the tutor. However, tutors must not correct the work of the learner, and all feedback given by the tutor must be included within the learner's evidence.

Learners' portfolio work should include a tracking sheet to show where the evidence for each assessment criterion is to be found. Some activities could produce evidence for more than one unit, which is acceptable as long as there is clear reference to this on the tracking sheet. Examples of tracking sheets are found in [Appendix 2](#).

Verification

Internal Verification

Internal verification is the process of ensuring that everyone who assesses a particular unit in a centre is assessing to the same standards, i.e. consistently and reliably. Internal verification activities will include: ensuring any stimulus or materials used for the purposes of assessment are fit for purpose; sampling assessments; standardisation of assessment decisions; and standardisation of internal verification decisions. Internal Verifiers are also responsible for supporting assessors by providing constructive advice and guidance in relation to the qualification delivered.

Ascentis offer free refresher training in support of this role through an Ascentis Internal Quality Assurance course. The purpose of the course is to provide staff in centres with knowledge and understanding of Ascentis IQA processes and procedures, which will enable them to carry out their role more effectively. To book your place on a course or request further information, please contact the Ascentis Quality Assurance Team (qualityassurance@ascentis.co.uk).

Further information is available from the login section of the Ascentis website: www.ascentis.co.uk.

External Verification

Recognised centres will be visited in accordance with a verification model that is considered most appropriate for the provision. More frequent verifications can be requested from the Ascentis Quality Assurance team, for which there is usually an additional charge. External verification will usually focus on the following areas:

- A review of the centre's management of the regulated provision
- The levels of resources to support the delivery of the qualification, including both physical resources and staffing
- Ensuring the centre is using appropriate assessment methods and making appropriate assessment decisions according to Ascentis' requirements
- Ensuring the centre has appropriate internal quality assurance arrangements as outlined within the relevant qualification specification
- Checking that the centre is using appropriate administrative arrangements to support the function of delivery and assessment

External Quality Assurers will usually do this through discussion with the centre management team; assessment and Internal Quality Assurance staff; verifying a sample of learners' evidence; talking to learners; and reviewing relevant centre documentation and systems.

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 the Ascentis website.

UNIT SPECIFICATIONS

Digital Technology Fundamentals

Credit Value of Unit: 1

GLH of Unit: 10

Level of Unit: Entry 3

Introduction

This unit aims to provide learners with a basic understanding of digital technology and will enable them to use computing and mobile devices to access appropriate websites and apps. The unit will give learners the ability to setup and use methods to connect to the internet and make the best use of tools and techniques to search for useful information and download apps. The final part of the unit will teach learners how to maintain devices and also understand common errors that can occur

Learning Outcomes	Assessment Criteria
The student should be able to	The student can
1. Setup computing and mobile devices to meet needs	1.1 Use correct procedures to start and shut down computing and mobile devices
	1.2 Use standard interface features
	1.3 Use appropriate terminology when describing computing and mobile devices
2. Understand the use of computing and mobile devices	2.1 Get online with an internet connection
	2.2 Store and retrieve data on computing and mobile devices
	2.3 Identify health and safety issues associated with the use of computing and mobile devices
	2.4 Outline the advantages and disadvantages of different computing and mobile devices
3. Use browser tools to navigate websites and download apps	3.1 Use search techniques to locate information
	3.2 Demonstrate how to download apps
4. Maintain the performance of computing and mobile devices	4.1 Identify common device problems
	4.2 Respond to common device problems

Indicative Content

Please be aware that the indicative content supplied below is a suggested guide only.

Setup computing and mobile devices to meet needs

Computing and mobile devices: desktop, portable/hand-held, tablets, smart phones, smart watches, switch on/off, start and shut down, login, enter password, install and/or charge battery, install SIM, update software, lock/unlock, touch screen, keyboard/pad, stylus, voice command.

Interface features: display, desktop, home screen, window, dialogue box, menu, submenu, toolbar, keypad, button, icon, scrollbar, button, drag and drop, pinch, zoom, minimise, maximise, rotate, systems and connectivity.

Appropriate terminology: will vary according to the set up or device, computer, PC, laptop, net book, tablet, smart phone, input device, keyboard, mouse, pointer, processor, output device, screen, touch screen, printer, storage media, cloud storage, app, memory, disk, CD, DVD, data/memory stick, hard drive, network, desktop, window, dialogue box, menu, submenu, toolbar, icon, scrollbar, button, drag and drop, pinch, zoom, minimise, maximise, USB, connectivity, Wi-Fi, Bluetooth, 3G, 4G.

Understand the use of computing and mobile devices

Get online: LAN, VPN, mobile phone, modem, router, wireless, dial-up, broadband, Internet Service Provider (ISP), Wi-Fi (secure vs. public), 3G, 4G, login details, username, password, hardware and software requirements; web browser, e.g. Internet Explorer, Edge, Firefox, Chrome, Safari, Dolphin, Opera; websites, web server, domain; website features, e.g. back, forward, refresh, stop, history, new window, new tab, toolbar, search bar, address bar, home, go to, follow link, URL.

Store and retrieve data: files, e.g. create, name, open, save, save as; folders, e.g. create, name, appropriate filename conventions.

Health and safety issues: accessibility, screen size/resolution, screen time, impact on health and well-being, physical stresses and psychological health risks, parental controls, Health and Safety (Display Screens Equipment) Regulations, security.

Advantages and disadvantages: speed, portability, access, availability of software and apps, compatibility, synchronisation, backup, screen time/health issues, connectivity, bandwidth, risks, personal safety, information security.

Use browser tools to navigate websites and download apps

Search techniques: key words, quotation marks, search within results, 'find' or 'search' tools, turn questions into key words for an online query.

Download apps: 'Trusted Sites', adjust internet settings, app downloading software (e.g. App Store, Google Play), security software (antivirus, malware).

Maintain the performance of computing and mobile devices

Common device problems: program not responding, hang-up/crash, reboot/restart, error dialogue, storage full, software update, connectivity, bandwidth, battery life, application and file use, device maintenance, signal loss/network availability (e.g. interference, distance, location).

Respond to common device problems: Limits of own understanding and skills, help menus, manufacturer's guidelines, how to follow advice, information from experts, user support helpline/websites.

UNIT SPECIFICATIONS

Transacting Digitally

Credit Value of Unit: 2

GLH of Unit: 20

Level of Unit: Entry 3

Introduction

This unit aims to develop learners' ability to use computing and mobile devices to access appropriate websites and apps to carry out online transactions. Learners will make use of tools to purchase goods and services, apply for 'digital' public services and organise own finances. In addition the unit will develop the learner's understanding of how to work responsibly and protect personal information, and will also introduce guidelines and procedures that learners must adhere to whilst completing transactions online.

Learning Outcomes	Assessment Criteria
The student should be able to	The student can
1. Interact with online marketplace services	1.1 Identify secure online marketplace services
	1.2 Understand online payment systems
	1.3 Demonstrate how to buy goods and services online
	1.4 Demonstrate how to make reservations and appointments online
2. Interact with online transactional services	2.1 Demonstrate how to access 'digital' public services online
	2.2 Complete online transactional forms
	2.3 Upload documents and photographs
	2.4 Comply with data validation and verification checks
3. Understand how to manage and organise own finances online	3.1 Register for online and telephone banking
	3.2 Manage own online bank account
4. Understand the need for safety and security practices when online	4.1 Stay safe and work responsibly
	4.2 Keep information secure
	4.3 Configure and use secure ways to access devices and online services
	4.4 Follow guidelines and procedures when transacting online

Indicative Content

Please be aware that the indicative content supplied below is a suggested guide only.

Interact with online marketplace services

Secure online marketplace services: SSL encryption, https, secure certificates, app vs. browser/website, malware-infected websites, public hotspots, https (s for secure), padlock symbol, valid certificate, online marketplaces (e.g. Amazon, eBay, Gumtree).

Online payment systems: credit/debit card, bank transfer, online/telephone banking, mobile payment, digital wallet services, e-money services (e.g. PayPal, Apple Pay).

Buy goods and services: search for goods/services, price, contact details, quantity, shopping basket, checkout, delivery options, payment method, billing information, register account/checkout as guest.

Make reservations and appointments: make reservations online for events (e.g. eventbrite.com, ticketmaster.co.uk), make appointments online at GPs, dentist, hairdressers, etc.

Interact with online transactional services

Digital public services online: transactional services require users to supply information online in multiple steps, following the provided instructions at each step; examples include central government services (e.g. applying for a passport, road tax, television license, benefit calculators, accessing income tax information), local government services (e.g. paying council tax online, requesting collection of household rubbish).

Complete online forms: typically comprise a simple single page form, such as those used to enter name and/or contact details, or to request a service (e.g. collection of household rubbish) or make an appointment; completion online, e.g. timed responses, saving drafts, checking, final submission, cannot be changed after entering data, number of characters, word limits, data validation and verification (refer to AC 2.4).

Upload documents and photographs: save/browse location, file size, appropriate filenames, editable documents (e.g. Word), non-editable documents (e.g. PDFs), common file formats, doc, pdf, jpg/jpeg, gif, png, file resolution, resizing, cropping.

Data validation and verification: data validation (process of comparing data with a set of rules to find out if data is reasonable). Examples of types of data validation include: format check – checks data is in the right format (e.g. date in the format dd/mm/yyyy); presence check – checks that data has been entered into a field; range check – checks that a value falls within the specified range (e.g. GCSE grades can only range between 9-1); type check – ensures the correct data type has been entered (e.g. age should be a number).

Data verification (process of checking that the data entered exactly matches the original source to find out if data is accurate). Methods include: double entry – entering data twice; proofreading data – someone checks the data entered against the original document; echo – system repeats the data being entered.

Accuracy, reliability, personal information, upper/lower case, mandatory fields, CAPTCHA, auto-complete (e.g. postcode/address), data type check (e.g. DOB (00/00/00)), range check (e.g. mobile phone number should have 11 digits and no letters, special characters or spaces), consistency check (e.g. delivery date cannot be before the order date).

Understand how to manage and organise own finances online

Online/telephone banking: register application/account, online account, remote/instant access, protect personal information (refer to AC 4.2, 4.3), online banking apps, automated telephone service, security, two-factor authentication, account number, password, PIN, passcode, online banking simulator: <https://www.moneyinstructor.com/onlinebanking.asp>, Open Banking (technologies and standards which in the future will allow consumers to safely and securely share their account information and take advantage of a number of different services).

Manage bank account: check bank balance at any time, pay bills, transfer money to other accounts, check any linked mortgages, loans, savings accounts or ISAs, bank statements and go paperless (no paper bills is more environmentally friendly), set up or cancel direct debits and standing orders, check on investments.

Understand the need for safety and security practices when online

Stay safe and work responsibly: appropriate language and behaviour, 'netiquette', respect for others, false identities/information, financial deception, fraud, identity theft, disclosure of information, firewall settings, internet security settings, reporting inappropriate behaviour, reporting security threats/breaches, content filtering, avoid misuse of content, physical stresses and psychological health risks.

Keep information secure: protect personal information from fraud and scams (identity theft), 'safe' username and password/PIN selection, passcode, online identity/profile, real name, pseudonym, personal information, who can view, withholding personal information, password protect files, use of passwords and logons, keep passwords safe, don't reveal personal details to unknown sources, secure websites (https) to exchange private information (encryption, reduced risk of intercepted data), security software (e.g. anti-spam, firewall).

Secure access: Multi-Factor Authentication (MFA) adds an extra layer of protection on top of usernames and passwords, Two-Factor Authentication (TFA) adds an extra layer of security that requires not only a password and username but also something that the user has on them, use of safe passwords, use of upper/lower case, numbers and symbols, retrieve forgotten passwords, password reset, security questions, never reveal/write down password/logon details, use different passwords for different devices and accounts, authentication processes, security keys.

Guidelines and procedures: health and safety, GDPR, security, copyright, software downloads and licensing, employer/organisational policies, website and app terms and conditions, electronic contract, consumer rights/protection laws (e.g. Consumer Contracts Regulations, Consumer Rights Act, PayPal Buyer Protection Scheme, eBay Money Back Guarantee).

APPENDIX 1

Summary Record of Achievement

Entry Level Award in Skills for Digital Transactions (Entry 3)

Unit Title	Level	Credit Value	Date completed	Assessor Signature	Internal Verifier Signature (if sampled)
Digital Technology Fundamentals	Entry 3	1			
Transacting Digitally	Entry 3	2			

Learner Name _____

Assessor Signature _____

Internal Verifier Signature (if sampled) _____

APPENDIX 2

Tracking Sheet

Entry 3 Digital Technology Fundamentals

Criteria	Assessment Method	Evidence Details	Portfolio Reference	Completion Date
1.1 Use correct procedures to start and shut down computing and mobile devices				
1.2 Use standard interface features				
1.3 Use appropriate terminology when describing computing and mobile devices				
2.1 Get online with an internet connection				
2.2 Store and retrieve data on computing and mobile devices				
2.3 Identify health and safety issues associated with the use of computing and mobile devices				
2.4 Outline the advantages and disadvantages of different computing and mobile devices				
3.1 Use search techniques to locate information				
3.2 Demonstrate how to download apps				
4.1 Identify common device problems				
4.2 Respond to common device problems				

The above evidence has been assessed against the standards and has been judged for validity, authenticity, currency, reliability and sufficiency.

Learner Signature _____ Date _____

Assessor Signature _____ Date _____

Internal Verifier (if sampled) _____ Date _____

APPENDIX 2

Tracking Sheet

Entry 3 Transacting Digitally

Criteria	Assessment Method	Evidence Details	Portfolio Reference	Completion Date
1.1 Identify secure online marketplace services				
1.2 Understand online payment systems				
1.3 Demonstrate how to buy goods and services online				
1.4 Demonstrate how to make reservations and appointments online				
2.1 Demonstrate how to access 'digital' public services online				
2.2 Complete online transactional forms				
2.3 Upload documents and photographs				
2.4 Comply with data validation and verification checks				
3.1 Register for online and telephone banking				
3.2 Manage own online bank account				
4.1 Stay safe and work responsibly				
4.2 Keep information secure				
4.3 Configure and use secure ways to access devices and online services				
4.4 Follow guidelines and procedures when transacting online				

The above evidence has been assessed against the standards and has been judged for validity, authenticity, currency, reliability and sufficiency.

Learner Signature _____ Date _____

Assessor Signature _____ Date _____

Internal Verifier (if sampled) _____ Date _____