|  |  |  |  |
| --- | --- | --- | --- |
| **Learner Name:**  |  | **Assessor:**  |  |
| **Centre Name:**  |  | **Internal Verifier (if applicable):**  |  |
| **BCS ID / ULN:**  |  |  |  |
| **Unit Information Summary** |
| **Approximate Guided Learning Hours: 20** | **Unit Number: H/502/9154** |
| **QCF Credit Value: 3** | **Learning Outcomes (Number): 4** |
| **Examples of Context:*** How to deal with cyberbullying.
* Keeping software applications up to date, and enabled (i.e. firewall and virus checking software).
* Keeping personal information private.
 | **Learning Materials Available:**e-safety online materials include lesson plans, class activities, teachers guidance and notes. |
| **Suggested Assessment Methods:**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 fully met* Scenario
* Coursework
* Portfolio of Evidence – classroom or work-based
* Practical Demonstration
* Assignment
* Task-based Controlled Assessment
* Professional Discussion
* Observation
* Witness Statement
 |

| **Ofqual Learning Outcome** | **Assessment Criteria** | **Examples of Content***The examples given are indicative of the learning content at each level and are not intended to form a prescriptive list for the purpose of assessment* | **Evidence Location** |
| --- | --- | --- | --- |
| **1 Understand the risks that can exist when using the Internet** | 1.1 | Identify risks to user safety and privacy | *User safety: abusive behaviour [“cyber bullying”], inappropriate behaviour and grooming, abuse of young people, false identities, financial deception* |  |
| 1.2 | Identify risks to data security | *Data security: theft of data, hacking, accidental deletion or change to data, Trojans, spyware, adware, phishing, identity theft, avatars, mobile technology – wireless and Bluetooth, default passwords, portable devices – USB devices* |  |
| 1.3 | Identify risks to system performance and integrity | *System performance: unwanted email – 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 risks: virus-checking software, anti-spam software, firewall, treat messages files software and attachments from unknown sources with caution, internet settings, block sites, parental controls* |  |
| 1.5 | Outline factors that affect the reliability of information on websites | *Information 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 | *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 of information, confidentiality content filtering, proxy servers, monitoring and reporting user behaviour* |  |
| 2.2 | Protect personal information online | *Protection: 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* |  |
| 2.3 | Carry out checks on others' online identity |  |  |
| 2.4 | Describe the forms and features of cyber bullying | *Forms of cyber bullying: chat rooms, email and instant messaging* |  |
| 2.5 | Identify when and how to report online safety issues | *Online safety issues: abusive behaviour [“cyber bullying”], inappropriate behaviour and grooming, abuse of young people, false identities, financial deception* |  |
| 2.6 | Identify where to get online help and information on e-safety | *Online help: service provider, legal system, parental controls* |  |
| **3 Take precautions to maintain data security** | 3.1 | Take appropriate precautions to maintain data security | *Precautions for data security: use access controls, configure anit-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 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 | *Precautions for system performance: set passwords, physical access controls – 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 | *Browser settings: autofill, cookies, security, pop-ups, appearance, privacy, search engine, toolbars, personalisation, accessibility, software updates, temporary file storage* |  |
| 3.4 | Use appropriate client software safety and security settings |  |  |
|  |  |  |  |  |
| **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 | *Legal constraints: relating to copyright, software download and licensing, digital rights, IPR, Health and Safety, Children Legislation, Data Protection* |  |
| 4.2 | Identify legal constraints on online behaviour |  |  |
| 4.3 | Correctly observe guidelines and procedures for the safe use of the Internet | *Guidelines and procedures: set by employer or organisation relating to Health and Safety, security, equal opportunities, disability* |  |

|  |
| --- |
| **Assessment Report** |
| **Assessor feedback / comments** (continue on additional sheet / assessment report if necessary) |
| **Internal Verifier actions / comments / feedback**  |
| **Assessor signature:**  |  | **Assessment date:** |  | **Reason for IV:****New Assessor** [ ] **Random Sample** [ ] **New Unit/Qualification**  [ ] **Other**  [ ]  |
| **IV signature:** |  | **IV date:** |  |