Knowledge Organiser for DIT Component 3

Communication technologies: ad hoc networks, open networks, performance issues and network availability

Cloud storage: access rights, synchronisation, availability and scalability

Cloud computing: applications, consistency of versions between users, single shared instances and collaboration tools/features

Selection of platforms and services: complexity of features, paid versus free, interface design and available devices

Using cloud and traditional systems together: device synchronisation, online/offline working and notifications

---

Choosing cloud technologies: disaster recovery policies and security of data

Maintenance, set up and performance considerations: maintenance: updates, downtime and staff expertise and performance: responsiveness, complexity of task and available devices

Collaborative technologies: world teams, multicultural, inclusion, 24/7/365 and flexibility

Using modern technology when managing teams: communication and collaboration tools

Using technology when managing teams: scheduling and planning tools

---

Communication with stakeholders: communication platforms and selection of appropriate communication channels

Accessibility and inclusivity: interface design, accessibility features and flexibility

How modern technologies impact on the organisation: infrastructure, demand, availability, 24/7 access and security of distributed/disbursed data

How technologies impact the way organisations operate: inclusivity, accessibility and remote working

How technology impacts individuals: flexibility, working styles and impact on mental wellbeing

---

Why systems are attacked: fun, challenge, espionage, financial gain, personal attack and disruption, theft

External threats to digital systems and data: unauthorised access, malware, phishing, pharming, social engineering, shoulder surfing and man-in-the-middle attacks

Internal threats to digital systems and data security: unintentional disclosure of data, intentional stealing or leaking of information users overriding security controls, portable devices, downloads from the internet and visiting trustworthy websites

User access restriction: locks, passwords, levels of permitted access, biometrics and two-factor authentication

---

B Cyber security B1 Threats to data B2 Prevention and management of threats to data Cyber Security Challenge Using the Cyber Security Challenge (https://www.cybersecuritychallenge.org.uk) competition in order to reinforce the elements of B is useful for developing learner skills within this area. Teaching Resources https://www.cybersecuritychallenge.org.uk/education/schools/teachers – This website provides specific support for teaching elements of B1: Why systems are attacked, Internal threats and Impact of security breach. External threats:

C1 Responsible use Showcasing social responsibility and shared data: Get learners to think about rules regarding what you should post on social media and how this could impact on you in later life. There has to be consideration given for the blurring of lines between social and business, and how some companies can exploit this. You could get learners to do a personal social media audit and define whether their last 20 posts would be something that a prospective employer in the future would find agreeable with their company's ethos and acceptable standards. This is a good way to teach social responsibility, and can link in well with any tutorial sessions you may be running on how this is managed in life and is not just an IT-related discipline. Interesting way of teaching: Set up something like a mock trial or a mock debate, where each of the learners gets an angle to take. Admittedly this can sometimes look like Lord of the Flies, but because each learner has to challenge their point and showcase why this is the right way to do things, or why something has been done in a certain way, it makes them truly understand their argument and also understand the other side of the debate; they cannot accurately argue why their view is stronger if they haven't looked into the opposing argument. You could write some loopholes or obvious omissions in to this so that learners can use this as a way for getting the person prosecuted or let off, depending on what they spot or what is in the policy. This will meet specific elements of C1 and C2 and could be used for B3 as well. C2 Legal and ethical Showcasing Data protection principles: The GDPR regulations put more responsibilities on employers and could be met by showcasing the following toolkit: http://www.nicva.org/data-protection-toolkit/templates/document-your-processing-activities

D1 Forms of notation There are various ways of showcasing Understand how organisations use different forms of notation to explain systems, and the following resources help with this: https://www.lucidchart.com/blog/data-flow-diagram-tutorial Showcasing Components 1, 2 and 3 together: Inside Learning aim D we have data flow diagrams, flow charts, system diagrams etc. including how we use these to present information and show understanding of a process or a system itself. Again these link really well with Components 1 and 2; for example, in Component 1, showing the steps to navigate through an interface could be done with a flowchart, or, in Component 2, you can use system diagrams to illustrate the types of data taken in, and any manipulation performed on the data in order to have it ready for visualising. As this also covers data interpretation, this again works really well with Component 2 in how we interpret trends and how we look for inaccurate data within a data set. 14 Interesting way of teaching: You can get your learners to flowchart out their route to school, or flowchart a battle plan for a game of Fortnite or Apex Legends. They could even create tabular data of their friends/family and anyone else close to them (for example, dates and places of birth), in order to show how this could be presented in such a way that somebody else could read and understand it.