Information Technology (OCR J808)

	R	A	G
1.1.1 The phases of the project life cycle and the tasks carried out in each phase i.e.			
a. initiation			
b. planning			
c. execution			
d. evaluation			
1.1.2 The advantages of following a project life cycle			
1.2.1 The interaction and iteration between the phases of the project life cycle i.e.			
1. iterative reviews occur throughout the project life cycle at the end of every phase			
2. the output from the reviews are the inputs into the next phase or they inform actions to be implemented within the current phase			
1.4 Initial project considerations i.e.			
1. SMART (Specific, Measurable, Achievable, Realistic, Time) goals			
2. user requirements			
3. success criteria			
4. constraints/limitations i.e.			
a. time			
b. resources			
c. regulations			
d. security/risk management			
e. mitigation of risks			
5. the purpose and importance of setting objectives			
1.5 Planning tools and the software types used to develop project plans i.e.			
1. purpose of planning tools i.e.			
a. Gantt			
b. PERT (Project Evaluation and Review Technique)			
c. critical path			
d. visualisation diagram			
e. flow chart			
f. mind map			
g. task list			
2. components of the planning tools			
3. advantages and disadvantages of different planning tools			
4. software types used i.e.			
a. project management software			
b. spreadsheets			
c. word processors			
d. Desktop Publishing (DTP)			
3.1 Data			
1. what data is			
2. data types and appropriateness of the use of these in a given context i.e.			
a. text			
b. alphanumeric (e.g. combination of letters and numbers)			
c. numeric – integer, real, currency, percentage, fraction, decimal			
d. date/time			
e. limited choice (e.g. drop down lists, radio buttons, tick list)			
f. object			
g. logical/Boolean (e.g. yes/no true/false)			
3.2 Information			
1. what information is			
2. how data and information are related i.e.			
a. data must be processed to become information			
b. information is in context whilst data has no context			
c. information is data which has			
3.3 The methods used to collect data and store data/information, and the appropriateness of the use of these in a given context i.e.			
1. methods to collect and store i.e.			
i. questionnaires / surveys - online and hard copy			
ii. email			
iii. sensors			
iv. interviews			

v. consumer panels			
vi. loyalty schemes			
vii. statistical reports (e.g. Government departments)			
viii. secondary research methods (e.g. search engines)			
2. appropriateness of methods i.e.			
i. suitability			
ii. advantages			
iii. disadvantages			
3. Information Technology (IT) used to support data collection, and the appropriateness of the use of these in context i.e.			
a. barcode/QR code readers			
b. web-based surveys			
c. wearable technology			
d. mobile technologies			
3.4 Different storage methods and the appropriateness of the use of these in context i.e.			
1. cloud			
2. physical devices			
3.5.1 The use of data in a given context including Big Data			
3.5.2 Applications and interaction of data stores i.e.			
a. law enforcement			
b. education			
c. health and fitness			
d. shopping			
e. entertainment / leisure			
f. lifestyle			
3.5.3 Benefits and drawbacks of the use of data			
4.1 Types of threats i.e.			
1. Botnet			
2. Malware i.e.			
a. adware			
b. bot			
c. bug			
d. ransomware			
e. rootkit			
f. spyware			
g. Trojan horse			
h. virus			
i. worm			
3. Social engineering i.e.			
a. Phishing			
b. pretexting			
c. baiting			
d. quid pro quo			
e. tailgating/piggybacking			
f. shoulder surfing			
4. Hacking i.e.			
a. white hat hacking - given permission to hack into systems to identify loopholes and weaknesses			
b. grey hat hacking - hacking into systems for 'fun' or to 'troll'			
c. black hat hacking - hacking into systems with malicious intent to steal, exploit and sell data			
5. Distributed Denial of Service (DDoS)			
6. pharming			
4.2 The vulnerabilities which can be exploited in a cyber-security attack i.e.			
1. environmental - natural disasters			
2. physical - theft of identity, theft of property			
3. system - insecure software applications, weak passwords, insecure modems			
4.3.1 The impacts of a cyber-security attack i.e.			
a. denial of service (DoS) to authorised others			
b. identify theft			
c. data destruction			
d. data manipulation			
e. data modification			
f. data theft			
4.3.2 Consequences of a cyber-security attack			

a. loss			
i. financial			
ii. data			
iii. reputation			
b. disruption			
i. operational			
ii. financial			
iii. commercial			
c. safety			
i. individuals			
ii. equipment			
iii. finance			
4.4 Prevention measures i.e.			
1. physical i.e.			
a. biometric access device			
b. emerging measures			
2. logical i.e.			
a. access rights and permissions including authentication, usernames and passwords			
b. anti-virus software			
c. encryption			
d. secure backups of data			
e. emerging measures			
3. secure destruction of data i.e.			
a. over writing			
b. magnetic wipe			
c. physical destruction			
4.5 Current relevant IT legislation, at time of delivery, its implications and applications i.e.			
1. legal protection of i.e.			
a. individuals			
b. organisations			
c. technological equipment			
d. data			
e. information			
f. intellectual property			
2. ethical and moral i.e.			
a. avoiding defamation of character			
b. misuse of data, information and equipment			
Data Protection Act			
Copyright – including Creative Commons			
Health & Safety			
Computer Misuse			
Freedom of Information			
4.6 The importance of validity, reliability and bias when collecting and using data and information			
6.1 Selection and justification of the appropriate software tools and techniques to process data to meet the defined objectives in a given context i.e.			
1. Tools i.e.			
a. spreadsheet			
b. databases			
6.2.1 Selection of the appropriate software tools and techniques to present information to meet the defined objectives in a given context. Justification of the use of the selected tool and format i.e.			
a. word processor			
b. spreadsheet			
c. databases			
d. desktop publishing (DTP)			
e. presentation software			
6.2.2 The purpose and suitability of methods of presenting information i.e.			
a. target audience			
i. demographics i.e.			
1. gender			
2. age			
3. ethnicity			

4. income			
5. location			
6. accessibility			
ii. visibility			
1. public facing i.e. website			
2. targeted i.e. email			
b. content limitations			
c. availability of information i.e.			
i. real-time (e.g. travel, traffic, weather)			
ii. location			
iii. delay effects			
d. what impact is to be achieved from distributing information			
e. selecting how the information is shared across distribution channels by individuals or organisations i.e.			
i. messaging services i.e.			
1. email			
2. social media for business (e.g. LinkedIn, iMessage, Twitter, Instagram, Facebook WhatsApp)			
3. internal messaging services (e.g. Moodle)			
ii. Websites			
1. Blogs			
2. vLogs			
3. intranet			
4. internet site			
5. internal website			
iii. Voice over Internet Protocol (VOIP) i.e.			
1. Skype			
2. Lync			
3. Podcast			
iv. Multimedia i.e.			
1. YouTube			
2. Web Conference			
v. Cloud Based (e.g. Google Drive, Office 365)			
vi. Mobile Apps (e.g. fitness app, travel app)			
f. selection of presentation method i.e.			
i. report (e.g. formal business report)			
ii. presentation (e.g. presentation to company board, presentation to customers)			
iii. graphs/charts i.e.			
1. pivot			
2. line			
3. bar			
4. pie			
5. dynamic			
iv. tables (e.g. table of results)			
v. integrated documents (e.g. document featuring components from other documents)			
vi. end user documentation i.e.			
1. user guide			
2. installation guide			
6.2.3 The advantages and disadvantages of methods used for presenting information.			
The resources required for presenting information and the appropriateness of the use of these in context i.e.			
1. hardware requirements			
2. software requirements			
3. connectivity requirements			