Name:

Information Technology: Initiate and Plan 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | | **Phases of a Project Life Cycle** | | **Input** | | **Output** | |
| 1 | **Initiation** | | Consideration of user or client’s requirements, and a decision of whether to take the job | 1 | User requirements | 1 | Feasibility report |
| 2 | User constraints | 2 | Legislation implications |
| 3 | Next Steps |
| 4 | Phase review |
| 2 | **Planning** | | Coming up with ideas of solutions, how they will be tested, what resources they will require, and how they will be achieved | 1 | Feasibility report | 1 | Project and test plans |
| 2 | Legislation implications | 2 | Constraints list |
| 3 | Next Steps | 3 | Phase review |
| 3 | **Execution** | | Putting the plan into effect, making the product, and testing | 1 | Project and test plans | 1 | Deliverable product |
| 2 | Constraints list | 2 | Test results |
| 3 | Phase review |
| 4 | **Evaluation** | | Checking the final product with the requirements, constraints and assessing the plan against the execution | 1 | Deliverable product | 1 | Release of deliverable product |
| 2 | Test results | 2 | User documentation |
| 3 | Final evaluation report |

|  |  |  |
| --- | --- | --- |
| **B** | **Key Vocab** | |
| **Phase review** | | Assessment at the end of a phase of what went well and what could have been improved with reference to the requirements and plans |
| **Iterative review** | | Assessment after each repetition of a stage of development. |
| **Next Steps** | | Brief outline of what to do next, in the absence of a full plan. |
| **Feasibility** | | How easy to achieve something is |
| **User requirement** | | Something that is needed. *ie the product must appeal to 20-30 year olds* |
| **Constraint** | | Something that must not or cannot happen. *ie the project must not cost more than £8,000* |
| **Objective** | | A specific planned outcome, which may be a small step in an overall project |
| **Success Criteria** | | The things you need to accomplish to know that the product is successful, written during the planning phase and checked in the evaluation phase |

Name:

Information Technology: Initiate and Plan 2

|  |  |  |  |
| --- | --- | --- | --- |
| **B** | **SMART Objectives** | **Example** | **Non-example** |
| **S** | Specific | Learn 7x tables | Get better at tables |
| **M** | Measurable | Get 80% in test | Do well in test |
| **A** | Achievable | Beat my PB | Set world record |
| **R** | Relevant | Learn C=πD | Learn π to 100dp |
| **T** | Time-based | …by 21/11/29 | …as soon as possible |

|  |  |  |  |
| --- | --- | --- | --- |
| **D** | | **Planning Tools** | |
| **1** | **Gantt** | | Horizontal bar chart used as a production control tool |
| **2** | **PERT** | | Program Evaluation Review Technique. A graphic illustration of a project, showing dependencies |
| **3** | **Critical Path** | | The sequence of stages determining the minimum time needed for a project |
| **4** | **Visualisation diagram** | | A sketch of a the final product, with annotations about how it will be used |
| **5** | **Flow chart** | | A diagram showing the sequence of events (or workflow) in a process |
| **6** | **Mind map** | | A diagram representing ideas relevant to an issue. Ideas are represented in nodes and sub-nodes, with links between them |
| **7** | **Task list** | | A list of tasks to be completed |

|  |  |  |
| --- | --- | --- |
| **A** | **Key Vocab** | |
| **Dependent** | | Can only be started once another task is completed |
| **Serial tasks** | | Dependent asks which must be performed one after the other |
| **Parallel tasks** | | Independent tasks which can be performed at the same time |
| **Dummy activity** | | Activity in a PERT diagram which takes no time, but connects a dependent task |
| **Milestone** | | An activity which takes no time and marks significant events |
| **Contingency** | | Planned time for if things do not go according to plan |
| **Risk mitigation** | | Systematic planning to reduce risks |
| **Node** | | An idea in a mind map |
| **Sub-node** | | A node which is linked to another node which is closer to the central node |
| **Link** | | Connection between nodes, denoting a connection of ideas |

|  |  |  |  |
| --- | --- | --- | --- |
| **C** | | **Software Used** | |
| **1** | **DTP** | | Desktop Publishing. eg MS Publisher, |
| **2** | **Project management software** | | eg MS Project |
| **3** | **Spreadsheet** | | eg MS Excel, Google Sheets |
| **4** | **Word processor** | | eg MS Word, Google Docs |

Information Technology: Data Collection

Name:

|  |  |  |  |
| --- | --- | --- | --- |
| **A** | **Key Vocab** | | |
| **Data** | | Unprocessed values (numbers, letters, graphics or sound) with no meaning | |
| **Information** | | Data which has meaning from its context or structure | *information = data + structure + context + meaning* |
| **Data type** | | eg number, alphanumeric, currency, Boolean, Date/time, limited choice | |
| **Alphanumeric** | | Combination of letters, symbols and numbers | *eg AjeY6&9Ed* |
| **Integer** | | Whole number | *eg 1960* |
| **Decimal** | | Number with a decimal point. Decimal places can be specified | *eg 22.75* |
| **Limited choice** | | Restricted to a specific set of options | *eg Drop-down list, radio buttons, check boxes* |
| **Boolean** | | True or False (or Yes/No) | *eg Are they eligible for a discount?* |

|  |  |  |
| --- | --- | --- |
| **B** | **Data Collection** | |
| **Questionnaire** | | A series of questions sent out to multiple people |
| **Survey** | | Same as a questionnaire |
| **Question Types** | | Closed question; Open question; Rank order; Rating |
| **Email** | | Surveys can be sent as attachments or embedded in an email |
| **Attachment** | | A file attached to an email which needs to be opened to be viewed |
| **Sensor** | | Electronic device which collects data from changes in eg motion, light, pressure or heat |
| **Interview** | | Questions asked in conversation, one-to-one |
| **Consumer panel** | | Dedicated group of product users who answer questions about their experience with the product |

|  |  |  |
| --- | --- | --- |
| **C** | **Data Collection** | |
| **Loyalty scheme** | | Customers agree to data being collected about their spending habits in return for discounts and promotional offers |
| **Primary source** | | Data collected by the person using it |
| **Secondary source** | | Data collected by someone else, and then published for general use |
| **Statistical report** | | Information gathered, structured and presented by someone else |
| **Barcode** | | Series of lines of different width which can be read by a scanner as a number |
| **Web survey** | | Questionnaire on the internet |
| **Wearable technology** | | A device which is worn and which can collect data |
| **Mobile technology** | | Any device that can be transported by a user, like a phone, tablet or GPS |

|  |  |  |
| --- | --- | --- |
| **D** | **Threats to data** | |
| **Physical** | | The device storing the data could be stolen or lost |
| **System** | | Data could be *lost*, *manipulated*, *modified* or *stolen* through hacking attempts |
| **Environmental** | | Natural disasters, such as earthquakes or floods. These could affect the data systems, backups and power supplies |

|  |  |  |
| --- | --- | --- |
| **C** | **Types of social engineering** | |
| **Social Engineering** | | Manipulating people so they give up confidential information |
| **Phishing** | | Directing a user to a malicious website from a bogus email where they will, eg, enter their bank details |
| **Pretexting** | | Pretending to confirm someone’s identity in order to get the information they provide |
| **Baiting** | | Users can get free goods (eg downloads) in return for their confidential details |
| **Quid pro quo** | | Users can get free services (eg IT assistance) in return for their confidential details |
| **Tailgating/ Piggybacking** | | Gaining entry to a room or building by following someone else in who holds the door open |
| **Shoulder surfing** | | Getting access to confidential information by watching someone enter it (eg at a cash machine) |

|  |  |  |
| --- | --- | --- |
| **B** | **Types of malware** | |
| **Adware** | | Software which displays advertising |
| **Bot** | | A computer program which operates by itself |
| **Botnet** | | A large collection of bots, working together |
| **Ransomware** | | Malware which disrupts the use of a system until a ransom has been paid |
| **Rootkit** | | Modifies operating system to avoid detection |
| **Spyware** | | Gathers and reports data from the host |
| **Trojan** | | Poses as legitimate software and must be installed by the user. Does not self-replicate |
| **Virus** | | Hidden in an executable and self-replicates |
| **Worm** | | Malware which self-replicates but does not require an executable file |

|  |  |  |
| --- | --- | --- |
| **A** | **Types of attack** | |
| **Hacking** | | Accessing someone else's data without consent |
| **White hat** | | Hacking but with consent. Generally this is to test for weaknesses and is legal |
| **Grey hat** | | Hacking without consent, and without intent to do damage. |
| **Black hat** | | Hacking with malicious intent |
| **Denial of Service (DoS)** | | An attack which aims to stop a server working by using up all its bandwidth |
| **Pharming** | | Directing a user to a malicious website by an attack on the DNS server |
| **Phishing** | | Directing a user to a malicious website from a bogus email |

|  |  |  |
| --- | --- | --- |
| **A** | **Types of attack** | |
| **Hacking** | | Accessing someone else's data without consent |
| **White hat** | | Hacking but with consent. Generally this is to test for weaknesses and is legal |
| **Grey hat** | | Hacking without consent, and without intent to do damage. |
| **Black hat** | | Hacking with malicious intent |
| **Distributed Denial of Service (DDoS)** | | An attack which aims to stop a server working by using up all its bandwidth. Requests are sent to the server by several different clients at once, sometimes by using a botnet |
| **Pharming** | | Redirecting a user to a malicious website when the follow a link from a legitimate one |

Information Technology: Data Threats

Name:

|  |  |  |
| --- | --- | --- |
| **C** | **Secure Destruction of Data** | |
| **Overwriting** | | Destroying data by putting different data in the memory. This can be meaningless data |
| **Magnetic Wipe** | | Using a magnet to remove all data stored on a device |
| **Physical Destruction** | | The storage device is destroyed by eg shredding, incineration, hammer etc |

|  |  |  |
| --- | --- | --- |
| **B** | **Prevention Measures: Key Vocab** | |
| **Access Rights** | | Given to people who have permission to look at or modify certain stores of data |
| **Permissions** | | What a user can do with their access rights (eg read, write, edit, comment or delete) |
| **Two Factor Authentication** | | A type of authentication which requires two different proofs of ID (eg knowing a password and receiving a text) |
| **Encryption software** | | A program which encrypts data to make it unreadable |
| **Encryption key** | | A passcode which is used to encrypt or decrypt data |

|  |  |  |  |
| --- | --- | --- | --- |
| **A** | | **Prevention Measures** | |
| **Physical Prevention Measure** | | | Prevention measure which does not use software or programs |
| **1** | **Biometric Prevention Measure** | | Prevention measure which uses a physical characteristic, eg fingerprint, eye scan or voice |
| **2** | **RFID** | | Radio Frequency ID. Tags which transmit data to a computer system. |
| **3** | **Physically securing** | | Locking a room, bolting equipment to desks, closing windows and blinds etc |
| **4** | **CCTV** | | Cameras which are used for security |
| **Logical Prevention Measure** | | | Prevention measure which uses software or programs |
| **1** | **Authentication** | | Logging on (normally with a username and password) to make sure you are the right person |
| **2** | **Anti-virus software** | | A program which protects against viruses |
| **3** | **Encryption** | | Making the data unreadable without a key |
| **4** | **Secure Backup** | | A copy of important files in case they get lost |

Name:

Information Technology: Data Security

|  |  |  |  |
| --- | --- | --- | --- |
| **A** | | **DPA** | |
| **DPA** | | | Data Protection Act, 1998 |
| **GDPR** | | | General Data Protection Regulation |
| **Data Subject** | | | The person the data is about |
| **Data User** | | | The person or using the stored data |
| **Data Controller** | | | The person in a company who is in charge of data and compliance with DPA |
| **Information Commissioner** | | | The person in government who enforces DPA |
| **Personal data** | | | Data about someone which allows them to be identified. (DPA only applies to personal data) |
| **Eight Principles of DPA** | | | |
| **1** | Personal data must be fairly and lawfully processed | | |
| **2** | Personal data must be processed for limited purposes | | |
| **3** | Personal data must be adequate, relevant and not excessive | | |
| **4** | Personal data must be accurate and up to date | | |
| **5** | Personal data must not be kept for longer than is necessary | | |
| **6** | Personal data must be processed in line with the individual’s rights | | |
| **7** | Personal data must be kept secure | | |
| **8** | Personal data must not be transferred to other countries outside the EEA | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **B** | | **CD&PA** | |
| **CD&PA** | | | Copyright, Designs and Patents Act, 1988 |
| **Intellectual Property** | | | Non-physical created works (eg music, poems etc) which belong to someone |
| **What it does** | | | Makes it illegal to copy, modify or sell intellectual property without permission from the owner |
| **Three ways to break CD&PA** | | | |
| **1** | Use software without the correct licence | | |
| **2** | Download files from the internet | | |
| **3** | Copy or share music, movies or software | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **C** | | **CMA** | |
| **CMA** | | | Computer Misuse Act, 1990 |
| **Hacking** | | | Unauthorised access to computer material |
| **What it does** | | | Makes hacking and malware illegal |
| **Three things CMA does** | | | |
| **1** | Prevents unauthorised access to computer material | | |
| **2** | Prevents any access to computer material if there is intent to commit further offences | | |
| **3** | Prevents acts which have the intent to impair the operation of a computer | | |

|  |  |  |
| --- | --- | --- |
| **D** | **FoI** | |
| **FoI** | | Freedom of Information Act (2000) |
| **Public Authority** | | Any branch of the government |
| **What it does** | | Public authorities are required to publish certain information and the public may request information from the public authority |

Name:

Information Technology: Legislation

|  |  |  |
| --- | --- | --- |
| **C** | **Prevention Measures** | |
| **Physical** | | Protecting against attacks with physical means |
| **Biometric protection** | | Reading data about someone’s body to verify their identity. Eg fingerprint, retina scan, DNA |
| **Locks** | | Securing the doors and windows to rooms with data storing machines |
| **CCTV** | | Security cameras |
| **Bolting down** | | Attaching computing equipment to a desk |
| **Logical** | | Protecting against attacks with non-physical means |
| **Access rights** | | Permissions for different users to be able to look at and edit different data |
| **Authentication** | | Making sure a user is the right person by eg username and password |
| **Two-factor** | | Authentication which asks for two proofs of ID, eg a password and a texted code |
| **Anti-malware software** | | Software which stops viruses and other malware getting into a system |
| **Encryption** | | Data is stored as an incomprehensible code until it is decrypted with a key |
| **Secure backup** | | A copy of important data, preferably kept away from the original data |

|  |  |  |
| --- | --- | --- |
| **C** | **Consequences of Disruption** | |
| **Disruption** | | When a cyber-security attack interrupts the normal running of a business |
| **Operational** | | A website or computer system can be stopped from working |
| **Financial** | | Money can be lost through loss of customers, compensation claims and the time spent fixing the disruption |
| **Commercial** | | When sales cannot be made |
| **Safety** | | Disruption of the running of, eg, a power plant would pose a threat to health of the public |

|  |  |  |
| --- | --- | --- |
| **B** | **Consequences of Data Loss** | |
| **Financial loss** | | If invoices are lost, income may be lost. If personal data is lost, compensation may be paid |
| **Time** | | Loss of data will mean any work done to make the data will have to be done again. |
| **Reputation** | | A data breach will undermine public confidence in the company which is attacked |

|  |  |  |
| --- | --- | --- |
| **A** | **Threats to Data** | |
| **Destruction** | | Data is lost and cannot be recovered |
| **Manipulation** | | Data is changed from its original form |
| **Modification** | | Another way of saying manipulation |
| **Theft** | | Data is stolen |
| **Identity theft** | | Stolen data is used to impersonate someone |

Information Technology: Risk Mitigation with Data

Name: