Colton Hills Community School medium term planning – ICT/Computer Science

<table>
<tr>
<td>Topic title:
Cyber Security and Incident Management</td>
<td>Year: KS5 Year 12/13

Term: Year long</td>
<td colspan="2">Why we teach this:
Learners study cyber security threats and vulnerabilities, the methods used to protect systems against threats and how to plan for and manage security incidents.</td>
<td>Why we teach this here:
To help them choose which pathway they will take for further studies.
Insight on cybersecurity university course</td>
</tr>
<tr>
<td colspan="2" rowspan="2">Big questions:
1. What is cyber security?
2. What in the difference between internal/external threats?
3. How can threat impact organisations?
4. What measures can be put in place to protect organisation?
5. What are the different types of networks?
6. What component are needed to make a network?
7. How can threats be classified?
8. How to create an effective plan to make cyber security plan robust?
9. What policies are involved when referring to cybersecurity?
10. How can forensics be gathered to investigate threat.</td>
<td colspan="2">Builds on previous topics:
- How IT is used in different organisations
- BTEC Level 2 learning
- Element of computer science</td>
<td>Links to future topics:
- Further education</td>
</tr>
<tr>
<td colspan="2" rowspan="2">Key knowledge:
A Cyber security threats, system vulnerabilities and security protection methods
⇨ A1 Cyber security threats
⇨ A2 System vulnerabilities
⇨ A3 Legal responsibilities
⇨ A4 Physical security measures
⇨ A5 Software and hardware security measures
B Use of networking architectures and principles for security
⇨ B1 Network types
⇨ B2 Network components
⇨ B3 Networking infrastructure services and resources</td>
<td>Key knowledge continued:
C Cyber security protection plan
⇨ C1 Assessment of computer system vulnerabilities
⇨ C2 Assessment of the risk severity for each threat
⇨ C3 A cyber security plan for a system
D Cyber security documentation
⇨ D1 Internal policies
⇨ D2 External service providers
E Forensic procedures
⇨ E1 Forensic collection of evidence
⇨ E2 Systematic forensic analysis of a suspect system</td>
</tr>
<tr>
<td>Skills developed:
- Basic skills on how to use the school computer systems in an effective manner.
- To be able to use office 365 and the OneDrive to carry out work in school and out of school.
- Make use of Cloud storage to save work.</td>
</tr>
<tr>
<td colspan="2">Mini/Interim assessments:
- Practise mocks using requited templates
- Lesson worksheets
- Lesson Homework sheets
- Kahoot quiz
- Retrieval</td>
<td colspan="2">Independent study tasks/resources:
Risk assessment of the networked system
Cyber security plan for the networked system
Management report justifying the solution
Use of technical language</td>
<td>Key vocabulary 1:
Cybersecurity
Vulnerabilities
Legal
Network types</td>
<td>Key vocabulary 2:
Forensic
Systematic forensic
Penetration testing</td>
</tr>
</table>

- Microsoft Forms tests **Termly summative assessment:** - Exam in May/June	Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident and come to a conclusion about the probable cause(s) of the security incident Review the incident and suggest ways to prevent a similar incident in the future	LAN WAN PAN SAN Infrastructure Matrix Severity	Open Web Application Security Project (OWASP) Software-defined networking (SDN) The Onion Router (Tor) SQL injection
Cultural capital opportunities: - Cybersecurity	**Whole school Curricular Concept links:** Civic Responsibility Cultural Diversity Artistic Creativity		