iTech: iCSI - Cold Case

Course Evaluation Criteria

Y3: We would expect all children in Y3 to attain statements 1-4. If any of statements 5-8 are attained, those pupils are exceeding expectations.

Y4: We would expect all children in Y4 to attain statements 1-5. If any of statements 6-8 are attained, those pupils are exceeding expectations.

Y5: We would expect all children in Y5 to attain statements 1-6. If any of statements 7-8 are attained, those pupils are exceeding expectations.

Y6: We would expect all children in Y6 to attain statements 1-7. If statement 8 is attained, those pupils are exceeding expectations.

1) Pupils know what defines a cold case.
2) Pupils know what skills are need to to become a CSI investigator.
3) Pupils understand what cookies are and how they are used.
4) Pupils can create a digital mind map.
5) Pupils understand the difference between digital and physical evidence.
6) Pupils understand what GPS stands for and how it works.
7) Pupils can explain the safest ways to store passwords.
8) Pupils can choose appropriate data to support an argument.

Course Overview

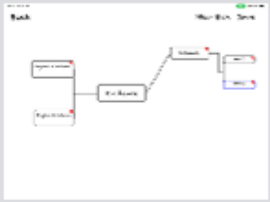
Course overview: iTech is all about exploring how technology can be used in the wider world. Over this course, pupils will look at how technology is used in positive, negative and sometimes illegal ways. Pupils learn about the people who stop cybercrime and what skills / characteristics benefit this line of work. They will examine the skills they use every day in school to see if they are transferable. During iCSI Cold Case the pupils will be introduced to a bank robbery with link to cybercrime. The case presented to them has heavy ties with internet safety and will draw attention to what they give away about themselves every day.

Learning outcome for the course: Throughout iTech Level 3 iCSI pupils will learn how technology is used within the police, cyber units and other specialist departments to help them solve crimes. Pupils will understand the collaboration within technological departments is key. Pupils will understand how Cookies are used, what an IP address is, GPS tracking, click bait, phishing emails/pop ups and facial recognition software. With strong ties to the Teaching online safety in schools (Jan 2023) non-statutory guidance, pupils will leave this course with a strong understanding of how what they do online can directly affect them and their digital safety.

iCSI App

The GPS feature allows us to input coordinates of significant locations relating to the crime.

The mind-map feature allows us to keep track of both the physical and digital evidence.



The judgement feature allows us to select our suspect and explain the evidence that supports our claim.

Apps Used

iCSI JJ

Logo Foundry

Vocabulary Bank

CSI

CSI stands for crime scene investigation.

Cold Case

A cold case is an unsolved criminal investigation.

GPS

GPS stands for Global Positioning System. Satellites send messages to digital devices to locate them.

Cyber Security

Cyber Security is the role protection on devices or networks to prevent cyber attacks.

Phishing

Phishing emails are emails designed to 'bait' the reader into clicking a link that may compromise them.

Cyber Criminal

Someone who commits crimes relating to digital devices or networks.

Physical Evidence

Physical evidence is evidence we can physically see.

Digital Evidence

Digital evidence is evidence that is on digital devices or networks.

Password

A password is a word that is used as a digital key to restrict digital access.

Cookies

A cookie is a file that contains information on where in the world you were when you visited the site and what you look at while you were on it.