# Appendix B
## Promoting Digital Resilience

### What is Digital Resilience?

At Plashet school, the 'Digital Resilience' package is a suite of resources designed to empower students with the resilience to critically evaluate information accessible online. It is also designed to safeguard young people from potentially harmful information or views presented online or through social networking sites such as YouTube, Twitter and Facebook.

### Why do we need it?

If a young person lacks the tools to make sense of their increasingly digital world, it has a direct impact on their vulnerability to exploitation. The Prevent Duty: Departmental advice for schools and childcare providers (2015) states schools have a responsibility to "safeguard children and young people in England from extremists and extremist views in school and in out of school hours learning, and stop young people from becoming radicalised or acting on extreme views.'

In addition, the Common Inspection Framework (Ofsted 2015) requires learners to demonstrate an 'understanding of how to keep themselves safe from relevant risks such as abuse, sexual exploitation and extremism, including when using the internet and social media'.

### Digital Resilience through the Wider School Curriculum.

In line with the school E-Safety Policy, there is an expectation for all users to promote digital resilience. This includes ensuring all e-materials used to teach the curriculum are safe for students to access and will not expose students to dangerous content. Whenever applicable, teachers and support staff should reference e-safety as part of their taught curriculum content. Teachers also develop in students the critical reasoning skills to evaluate information presented online with a specific focus on 'fake-news'.

### Digital Resilience through Student Leadership:

As part of our student leadership programme, students may apply in Year 10 to be a safer school's prefect. As part of this role they will work with a dedicated member of staff to promote digital resilience across the student body.

### Digital Resilience: The Taught Curriculum

Digital Resilience is taught through the Learning for Life and Computing Curriculums.

### The Learning for Life Curriculum (CPSHE)

| **Year 8: Unit of Learning** | **Digital Resilience** |
|---|---|
| 1. What is the Social Networking Revolution and how has this changed the way we communicate?<br>2. What are the dangers of social networking? (Online grooming case-study)<br>3. How can I ensure I keep myself safe while online?<br>4. Students are taught how to use CEOPS 'think you know' website to report online activity that they deem to be a risk to their safety and well-being. | Students will describe some of the problems associated with widespread use of the internet & specifically social media.<br><br>Students will apply their understanding of rights & responsibilities to explain how the dangers of internet use & specifically social networking can be mitigated through safe and responsible use of digital resources.<br><br>Students will know how to report digital material that they deem to be offensive or that poses a risk to their safety and well-being.<br><br>Students will begin to think about the strategy and tactics utilised by those who may wish to groom them to exploit, abuse them or groom them to commit a crime. |

## The Computing Curriculum

**Year 7: Unit of Learning: Digital Resilience**

**Introduction to computing assignment**

- Learn how to use the school network including the importance of good practice in using passwords.

**E-safety assignment**

- CEOP videos about the dangers of meeting up with on-line contacts
- Social networking – digital footprints and privacy
- Internet use – bias, plagiarism

Students undertake an assessed piece of work within both assignments.

Students will also sit a test in these units and have the opportunity to review their answers to address any misconceptions.

**GCSE: KS4 IT (Cambridge Nationals IT)**

Types of digital security threats:

- Malware (e.g. adware and ransomware)
- Social engineering (e.g. phishing)
- Hacking
- Distributed Denial of Service

**All Years: Responsible user agreement**

This document is discussed in the first lesson of the year. If students are seeing it for the first time the discussion is detailed. For subsequent years they are reminded about it.

The Responsible Computer User agreement has two sections. The first section is about rules and guidance within school. The second section is advise to follow outside of school.