

ONLINE SAFETY IN THE CURRICULUM



Rationale:

Astrea Academy Sheffield value Online Safety as a vital mechanism in the development of scholars. Astrea Sheffield aim to provide scholars with bespoke learning opportunities so they can develop an understanding of the dangers when online. This understanding will allow them to make informed choices today, tomorrow and in the future.

Key Stage 3: Online Safety Curriculum

Year 7 will be taught:

1. How to recognise safe and appropriate use of the Internet and technology
2. What the dangers of using technology on the Internet
The dangers explored are: What is inappropriate content (including illegal pornography and content not suitable for age groups), what is fakes news, what is cyber bullying, what are online predators (grooming) how to search the internet effectively, ID theft, social engineering (phishing, pharming, and shouldering).
3. How to report dangers using a range of methods including: How to report to the Academy, How to report to CEOP and How to report to NSPCC
4. What the ethics of using photo manipulation software on society?
5. What Copyright, Designs and Patent act is and how legislation can impact product development using computer systems.

Year 8 will be taught:

1. How to use technology safely, both online and offline.
2. How data is used, collected stored and shared whilst understand how to managing online information
3. What laws and legislation are used when managing data
(Malicious Communications Act 1988 and Data Protection Act)
4. What are the different types of hackers
5. How websites are created for inclusivity
6. How to use technology safely when building and creating websites. Netiquette and W3 standards.

Year 9 will be taught:

1. What the most common online threats are, how to prevent them and how to secure systems.
What the software threats are (Malware) and how to prevent them.
2. *What Ethical and Unethical hacking is*
3. *What the Computer Misuse Act is*
4. What the impacts of gaming online are and how to manage screen time.
5. What micro transactions are and how hidden gambling can take place when playing online games.

Key Stage 4: Online Safety Curriculum in Computer Science

Across the computing curriculum in year 10 and 11, scholars will be taught:

1. How to use abstraction and decomposition to support problem solving using computer systems
2. How data the role of secondary storage and the ways in which data is stored on devices.
(Data Protection Act and General Data Protection Regulation)
3. How cloud technology works and its purpose
4. Understanding of how the internet works
IP addressing, routers, protocols and speed
5. Network security and ways to identify vulnerabilities
(Penetration testing, ethical hacking)
6. Ways to prevent network security vulnerabilities
(Access control, physical security, and firewalls)
7. The legal and ethical issues with the collection of and use of personal data
(privacy, ownership, consent, algorithmic bias and legal liability)
8. Intellectual Property and how to protect
(Copyright, Designs and Patent Act)
9. Understand the threats to digital systems posed by malware.
(Viruses, worms, Trojans and key loggers)
10. How do unethical hackers take advantage of vulnerabilities
(Unpatched software, out of data malware)
11. Social engineering techniques
12. What are the methods to protect digital systems and data?
(The computer misuse act, anti-malware, encryption, acceptable use policies, backup and recovery)

In the Personal development curriculum scholars will be taught:

Year 7

1. Subtopic 1: Staying safe online, about online communication, recognising online grooming in different forms, how to respond and seek support in cases of online grooming.
2. Subtopic 2: Cyber-bullying, recognising and reporting cyber bullying, using social networking sites safely.
3. Subtopic 3: Safer online gaming, being mindful of making comments online and sharing personal information, reporting online abuse, how to protect financial security online, how to assess and manage risks in relation to gambling.
4. Subtopic 4: Biased and misleading online information, how to recognise biased or misleading information online, how to critically access different media sources
5. British Values Subtopic: The Rule of Law, Laws around online behaviour, How laws keep us safe online.

Year 8

1. Subtopic 4: Understanding of what Digital Resilience is, how to develop digital resilience, managing the impact of social media and understanding how this can have a negative effect on our wellbeing

Financial decision making

2. Subtopic 2: Staying in control of your money, Influences on our attitudes to money. For example, peer pressure, marketing, social media, forming good and bad habits with money, recognising persuasive advertising throughout society and how to critically assess this.
3. Subtopic 3: Keeping finances secure, recognising different types of fraud and scams e.g. phishing, smishing, social media scams, ways to safeguard vulnerability to fraud and scams

Year 9

Employability skills

1. Subtopic 2: Managing your online presence. Evaluate how personal online presence is affecting future opportunities, understanding that trends in technology will have implications for future careers
2. Subtopic5: Pornography and Sexting: impact of pornography on relationships, mental health, unrealistic expectations and risks and implications of sexting

Year 10

Healthy relationships

1. Subtopic 2: Impact of Pornography, Impact of pornography on people's understanding and expectations of consent, Challenge inaccurate and dangerous messages perpetuated by pornography about sexuality, gender, and consent
2. Laws relating to pornography and sharing explicit images

Finances

1. Subtopic 2: Cybercrime, causes of cybercrime, Impact of cybercrime and strategies to avoid or exit risky situations relating to cybercrime
2. Subtopic 3: Online fraud and money mules, identifying online fraud, explain risks of becoming a money mule including financial and legal consequences, evaluate ways to prevent being drawn into fraudulent actions support available for online fraud.

Online Safety and Assemblies

Assemblies this academic year 2023-2024 are responsive to the most common Online Safety instances identified through the academies reporting process and use of the Net Support DNA the monitoring and filtering system.

Parental Newsletters and Online Safety

Online Safety updates to be sent out monthly to include the most up-to-date Online Safety Advice.