

## Embedding Online Safety Threads Throughout the Polaris Computer Science Curriculum

Our Polaris Schools' Computer Science Curriculum map has been updated to better reflect the KCSIE 20205 increased focus on Online Safety

See updated Curriculum Map

### KCSIE-Integrated Online Safety Curriculum summary

| Year Group | Existing Theme                          | Online Safety Integration   | KCSIE 2025 Emphasis                              |
|------------|---|---|--|
| Year 1–2   | Technology & Media Foundations          | Recognise when to ask for help online<br>Name a trusted adult for digital concerns<br>Spot technology that is 'safe' vs 'unsafe'  | Self-image & Identity<br>Online Relationships    |
| Year 3–4   | Developing Programming & Media Literacy | Identify misleading online content<br>Recognise and respond to unkind messages<br>Safe use of devices, gentle rules for responsible tech<br>Understand photos and data, introduce basics of password safety<br>Spot real vs fake digital content, decode respectful messaging<br>Discuss impact of sharing and edited content, intro to image and audio authenticity<br>Discuss why some online content may be altered or false | Online Reputation<br>Managing Online Information |

| Year Group | Existing Theme                        | Online Safety Integration  | KCSIE 2025 Emphasis  |
|------------|---------------------------------------|--|--|
| Year 5–6   | Advanced Media & Data Handling        | <ul style="list-style-type: none"> <li>-Spot misinformation and evaluate website safety</li> <li>Understand personal data protection online</li> <li>Explore footprint, safe sharing, how websites gather data</li> <li>Misinformation recognition, evaluating websites, ownership of personal data</li> <li>Explore implications of fake news &amp; viral trends</li> </ul> | Privacy & Security<br>Online Bullying  |
| Year 7     | Networks & Digital Collaboration      | <ul style="list-style-type: none"> <li>- Apply critical analysis to digital sources</li> <li>Reflect on digital footprint and online persona</li> <li>Identify manipulation tactics in digital communication</li> <li>Identity theft, manipulation online, content credibility</li> </ul>  | Online Behaviour<br>Digital Consent  |
| Year 8–9   | AI, Cybersecurity, and Representation | <ul style="list-style-type: none"> <li>- Describe AI bias and its influence online</li> <li>Algorithm awareness, ethical design principles, responsible media creation</li> <li>Assess ethical sharing of digital media</li> <li>Create secure systems and evaluate digital risks</li> <li>Data cleansing, cybersecurity, peer influences &amp; digital ethics</li> </ul>    | Disinformation & Conspiracy<br>Cybersecurity & Harmful Content<br>Privacy & Security<br>Online Relationships |

KCSIE 2025 emphasises safeguarding against **misinformation, conspiracy theories, and online harms**. To better align we have improved our Computer Science curriculum coverage. WE have also updated our RSHE and PSHE Curriculum maps to ensure pupils are being supported to develop the knowledge and skills they will need in our world of growing technology.

Changes include:

- **KS1–KS3:** Explicit learning objectives around:
  - Recognizing false information online (e.g., “I can spot when something online might be misleading or fake”).
  - Evaluating digital content credibility (“I can ask questions about who made it and why”).
  - Exploring respectful online behaviour and communication.
- **KS4–KS5:** Deepened teaching around:
  - Ethical digital conduct and critical evaluation of online sources.
  - Responsible sharing, image copyright, and implications of digital footprint.
  - AI literacy and algorithmic bias, linking with existing media manipulation themes.



#### **Addressing Harmful Online Trends Explicitly in Upper KS2–KS3**

To reflect current KCSIE themes:

- Curriculum points include:
  - Impact of viral trends, TikTok challenges, “hoaxes” or inappropriate content.
  - Discussions on grooming, radicalization, and how manipulation works.
  - Signposting clear processes to report concerns, both technically and emotionally.



#### **Cross-Curricular Reinforcement and Staff Familiarity**

We have strengthened our already robust whole-school safeguarding culture by:

- Co-planning computing units with PSHE and RSE to embed safeguarding holistically.

- Ensuring we share clear guidance on the curriculum including vocabulary, particularly around online harms—ensuring consistency and preventing ambiguity.
- Prompting pupils to reflect on **digital responsibility**, especially when producing blogs, podcasts, code or digital portfolios.
- *Embedding themes such as* critiquing a range of online sources for reliability and intent, linking to misinformation and conspiracy theory trends.

### **Scaffolding Teaching and Learning around Safeguarding for SEND Learners**

Given our schools' support **pupils with SEND or interrupted educational journeys**, online safety topics are:

- **Adaptable to cognitive readiness:** E.g., use visual cues to identify safe/unsafe online content, explore emotions linked to online interactions.
- Taught with **concrete scenarios:** Simulate texting, gaming chats, and video streaming in safe settings.
- Reinforced with simple, repeatable rules: E.g., “Check with a trusted adult before clicking”.