

## Correlation Breakdown by Theme from “Cyber Safety 101 video”:

### Theme 1: Cybersecurity Fundamentals & Device Protection

- **Science & Technology Concepts (from “Cyber Safety 101 video”):**
  - "Cybersecurity" (a field of computer science and information technology)
  - "Computer, smartphone, and other devices" (hardware technology)
  - "Hacked or attacked," "steal your personal information or cause damage" (understanding vulnerabilities in technology)
  - "Strong passwords," "security software" (specific technological tools and applications)
  - "Secure your digital life," "prevent unwanted access" (application of security principles)
- **Real-World Problems Addressed (from “Cyber Safety 101 video”):**
  - Theft of personal information, photos, and documents.
  - Damage to digital devices.
  - Unauthorized access to digital lives.
- **Practical Applications in Occupations/Skilled Trades:**
  - **Cybersecurity Analyst/Specialist:** Applies knowledge of network security, software vulnerabilities, and data protection to prevent attacks. They develop and implement security measures.
  - **IT Support Specialist/Network Administrator:** Configures and maintains secure computer systems and networks. They install security software, manage passwords, and troubleshoot security issues for organizations or individuals.
  - **Software Developer (Security-focused):** Designs and codes security features into software, ensuring applications are built with protection against hacking and data breaches.
  - **Skilled Trade (e.g., Data Cabling Technician, Network Installer):** While not directly "cybersecurity," these trades are foundational. They physically install the infrastructure (cables, routers) that cybersecurity professionals then secure, ensuring data can travel safely.

- **How the “Cyber Safety 101 video” supports A3.1:** The “Cyber Safety 101 video” introduces the fundamental *need* for cybersecurity and basic tools. Students can then explore who builds these tools (developers), who deploys and maintains them (IT specialists), and who monitors the threats (cybersecurity analysts) to keep information safe.

## **Theme 2: Social Media & Online Communication – Benefits & Risks**

- **Science & Technology Concepts (from “Cyber Safety 101 video”):**
  - "Messaging, photos, and videos" (digital communication technologies, multimedia file formats)
  - "Social media" (online networking platforms, internet protocols)
  - "Digital communication tools like text messages" (mobile communication technology)
- **Real-World Problems Addressed (from “Cyber Safety 101 video”):**
  - Sharing too much personal information.
  - Cyberbullying, identity theft, online harassment.
  - Risk from content posted and interactions.
- **Practical Applications in Occupations/Skilled Trades:**
  - **Social Media Manager/Community Manager:** Uses social media platforms for communication and marketing. They address problems of online reputation, engagement, and potential harassment by monitoring content, setting community guidelines, and responding to issues.
  - **UX/UI Designer (User Experience/User Interface Designer):** Designs intuitive and safe interfaces for social media apps/websites, aiming to make privacy settings clear and user interaction positive, thereby mitigating risks of accidental oversharing.
  - **Digital Content Creator/Influencer:** Utilizes platforms to create and distribute content. They address the problem of managing their digital footprint and privacy while engaging with a large audience.
  - **Educator/Digital Literacy Instructor:** Teaches safe and responsible use of digital communication tools to prevent the problems mentioned.

- **How the “Cyber Safety 101 video” supports A3.1:** The “Cyber Safety 101 video” highlights the dual nature of social media. This opens discussion for occupations that leverage these technologies positively (social media managers) and those that mitigate their negative side effects (UX/UI designers, educators).

### **Theme 3: Cyberbullying – Impact & Response**

- **Science & Technology Concepts (from “Cyber Safety 101 video”):**
  - "Technology to harass, intimidate, or hurt someone" (misuse of digital tools)
  - "Anonymously" (understanding how technology can mask identity)
  - "Document the incident" (digital evidence, screenshots, data preservation)
- **Real-World Problems Addressed (from “Cyber Safety 101 video”):**
  - Harmful and long-lasting effects on victims (sadness, anxiety, depression, impact on mental health, schoolwork, social life).
  - Difficulty in identifying perpetrators.
- **Practical Applications in Occupations/Skilled Trades:**
  - **School Counsellor/Social Worker:** Provides support to victims of cyberbullying, helping them cope with mental health impacts. They apply their knowledge of psychology and social dynamics in the digital context.
  - **Law Enforcement Officer (Cybercrime Unit):** Investigates cyberbullying, identity theft, and online threats. They use digital forensics techniques to trace anonymous perpetrators and gather digital evidence ("document the incident").
  - **Digital Forensics Investigator:** A specialized role or skilled trade focusing on retrieving and analyzing digital data to find evidence of cybercrimes, including cyberbullying, by understanding how digital information is stored and recovered.
  - **Online Platform Safety Specialist:** Works for social media companies to enforce policies, review reported content, and ban users engaging in cyberbullying.
- **How the “Cyber Safety 101 video” supports A3.1:** The “Cyber Safety 101 video” details the severe consequences of cyberbullying. Students can then discuss the roles of professionals who intervene to support victims (counsellors), investigate

crimes (law enforcement, digital forensics), and try to prevent such acts on platforms (safety specialists).

#### **Theme 4: General Online Safety Practices**

- **Science & Technology Concepts (from “Cyber Safety 101 video”):**
    - "Reputable websites and apps" (understanding secure vs. insecure platforms, software reliability)
    - "Suspicious emails or links" (phishing, malware, understanding how malicious code is delivered)
  - **Real-World Problems Addressed (from “Cyber Safety 101 video”):**
    - Falling victim to scams, malware, or phishing.
    - Compromising digital identity.
  - **Practical Applications in Occupations/Skilled Trades:**
    - **IT Security Trainer/Consultant:** Educates employees and the public on safe online practices, including identifying phishing attempts and using reputable software.
    - **Web Developer/App Developer:** Builds secure websites and applications, addressing the problem of user trust and data integrity. Their "trade" is to create "reputable websites and apps."
    - **Quality Assurance (QA) Tester for Software:** Tests applications and websites for vulnerabilities and bugs, ensuring they are safe and reliable before release.
  - **How the “Cyber Safety 101 video” supports A3.1:** The final points offer actionable advice. These actions are directly supported by the work of various professionals who design secure systems, educate users, and combat digital threats.
- 

#### **Classroom Application for Outcome A3.1:**

After reviewing the "Digital Safety 101" “Cyber Safety 101 video” with students:

1. **Identify Key Concepts & Problems:** Ask students to highlight or list all the science and technology concepts and real-world problems discussed in the “Cyber Safety 101 video”.

2. **Brainstorm Occupations:** Based on these concepts and problems, guide students to brainstorm different jobs or skilled trades that might be involved in creating, maintaining, securing, or resolving issues related to digital safety. *This is where explicit teaching and examples of careers would be introduced.*
3. **Connect the Dots:** For each identified occupation, ask students:
  - "What specific science or technology concept from the "Cyber Safety 101 video" does this job use?"
  - "What real-world problem does this job try to solve (related to digital safety)?"
  - "How do they apply their knowledge/skills to address this problem?"
4. **Case Study/Research:** Have students research a specific digital safety-related occupation (e.g., a cybersecurity expert, a digital forensics specialist, a school counsellor specializing in online bullying) and report back on how their work directly applies science and technology concepts to solve real-world problems.
5. **Guest Speaker (Optional):** Invite an IT professional, a police officer from a cybercrime unit, or a school counsellor to discuss their work and how it relates to the topics covered in "Digital Safety 101."

By using the "Cyber Safety 101 video" as a springboard, educators can effectively demonstrate how the abstract concepts of science and technology are concretely applied in various professions to tackle critical real-world problems in the digital age, directly addressing Outcome A3.1