Complete Scheme of Work for Cyber Play (Weeks 1 to 8)

Target Audience: KS4 (Year 9/10)
Duration: 8 weeks (2 lessons per week)

Week 1: Introduction to Digital Privacy

Lesson Title: Avatar Creation and Data Privacy

Learning Objectives:

- I can understand what personal data is and why it is valuable.
- I can recognise the risks associated with sharing personal information online.
- I can explain how digital footprints affect my online presence.

Outcomes:

- All: Describe basic personal data and explain why it should be protected.
- Most: Identify key privacy risks online and explain how to manage digital footprints.
- Some: Analyse the implications of oversharing data and develop strategies to minimise online risks.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will create avatars and explore what types of personal data are shared when creating online profiles. They will evaluate how this data is used and the potential risks.
- Activity:
  Students will analyse their own digital footprints by searching for themselves online and reflecting on the information that is publicly available. They will then research ways to manage and minimise their online footprint.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will create a Digital Privacy Guide aimed at social media users. This guide will highlight best practices for managing personal data and minimising privacy risks.

Digital Competence Framework (DCF) References:

1. Progression Step 3:
    - Online behaviour: "I can demonstrate appropriate online behaviour and apply a range of strategies to protect myself and others from possible online dangers, bullying, and inappropriate behaviour, e.g., turn off comments on digital media, reporting, block users."
    - Understanding personal data: "I can understand the risks and legal consequences of sending intimate images and content/sexting."
2. Progression Step 4:
    - Appropriate online behaviour: "I can act appropriately online, keeping myself safe and behaving in a responsible manner."
    - Understanding digital footprint: "I can understand the implications of online actions, including my digital footprint and the legal implications of sharing inappropriate material."

Week 2: Understanding Phishing and Social Engineering

Lesson Title: Phishing and Email Scams

Learning Objectives:

- I can identify phishing attempts in emails and online communications.
- I can explain how social engineering manipulates individuals into sharing sensitive information.
- I can develop strategies to protect against phishing and fraud.

Outcomes:

- All: Recognise basic phishing indicators and describe the concept of social engineering.
- Most: Explain how phishing tactics work and apply strategies to avoid falling victim.
- Some: Analyse phishing techniques and create comprehensive strategies for phishing prevention.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will take on the role of cybersecurity analysts tasked with investigating a phishing attack at their school. They will analyse actual phishing emails, identify red flags, and create a report of their findings.
- Activity:
  Students will research the anatomy of a phishing attack, studying how phishing emails trick people into sharing sensitive information. They will discuss how social engineering tactics such as impersonation, urgency, and fear are used to manipulate people.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will create an Anti-Phishing Campaign for their school, which includes infographics, email templates, and strategies to help peers recognise and avoid phishing attacks. The campaign will be included in their portfolio.

Digital Competence Framework (DCF) References:

Progression Step 3:

- Online behaviour: "I can demonstrate appropriate online behaviour and apply a range of strategies to protect myself and others from possible online dangers, bullying and inappropriate behaviour, e.g. turn off comments on digital media, reporting, block users."
- Understanding personal data: "I can understand the risks and legal consequences of sending intimate images and content/sexting."

Progression Step 4:

- Appropriate online behaviour: "I can act appropriately online, keeping myself safe and behaving in a responsible manner."
- Digital footprint: "I can understand the implications of online actions, including my digital footprint and the legal implications of sharing inappropriate material."

Week 3: Network Security and Traffic Analysis

Lesson Title: Network Traffic and Data Breaches

Learning Objectives:

- I can analyse network traffic to identify abnormal patterns.
- I can explain how data breaches occur and how attackers exfiltrate data.
- I can use network logs to trace cyber threats.

Outcomes:

- All: Understand basic network traffic patterns and recognise signs of irregularities.
- Most: Analyse traffic logs to detect suspicious activity and understand the role of data breaches.
- Some: Investigate advanced network threats and create protocols to prevent data breaches.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will act as network administrators investigating suspicious network traffic in an organisation. They will analyse traffic logs to detect unauthorised access and create a report detailing their findings.
- Activity:
  Students will research famous data breaches and explore how network traffic analysis can help prevent these types of attacks. They will discuss the steps organisations can take to secure their networks.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will develop a Network Security Report that outlines how to monitor and secure network traffic to prevent data breaches. This report will be included in their portfolio.

Digital Competence Framework (DCF) References:

Progression Step 3:

  - Online behaviour: "I can demonstrate appropriate online behaviour and apply a range of strategies to protect myself and others from possible online dangers, bullying and inappropriate behaviour, e.g., turn off comments on digital media, reporting, block users."

- Collaboration: "I can work with others to create an online collaborative project for a specific purpose, sharing and appropriately setting permissions for other group members, e.g. editing, commenting, viewing."
- **Planning**: "I can independently create and plan work before beginning a digital task."
- **File management**: "I can manage files and folders locally or online, e.g. move files to a folder."

Progression Step 4:

- Appropriate online behaviour: "I can act appropriately online, keeping myself safe and behaving in a responsible manner."
- Collaboration tools: "I can independently select and use a range of online collaboration tools to create a project with others in one or more languages, e.g. making use of online technology to share and present ideas to others."
- **Planning techniques**: "I can select and effectively use a variety of planning techniques."
- **File management techniques**: "I can use appropriate advanced file management techniques, e.g. version history, restore previous version, tagging, compression."

Week 4: Digital Footprints and Online Safety

Lesson Title: Managing Your Digital Footprint

Learning Objectives:

- I can understand what a digital footprint is and its implications.
- I can analyse the potential long-term impact of one's online activity.
- I can develop strategies to manage and minimise my digital footprint.

Outcomes:

- All: Explain what a digital footprint is and why it matters.
- Most: Discuss the impact of a digital footprint on privacy and how to manage it.
- Some: Analyse case studies related to digital footprints and recommend strategies for minimising online risks.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will investigate the digital footprints of various individuals and analyse how their online presence has impacted their personal or professional lives. They will evaluate both the positive and negative effects of maintaining a digital presence.
- Activity:
  Students will search for information about public figures and examine how their digital footprints have influenced their careers. They will discuss the importance of managing online information and privacy settings.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will create a Digital Footprint Management Plan, which will include strategies for monitoring, controlling, and minimising their own online presence. This plan will be added to their portfolio.

Digital Competence Framework (DCF) References:

Progression Step 3:

- Online behaviour: "I can demonstrate appropriate online behaviour and apply a range of strategies to protect myself and others from possible online dangers, bullying and inappropriate behaviour, e.g., turn off comments on digital media, reporting, block users."
- Understanding digital footprint: "I can understand the risks and legal consequences of sending intimate images and content/sexting."
- File management: "I can manage files and folders locally or online, e.g., move files to a folder."
- Collaboration: "I can work with others to create an online collaborative project for a specific purpose, sharing and appropriately setting permissions for other group members, e.g., editing, commenting, viewing."

Progression Step 4:

- Digital footprint awareness: "I can understand the implications of online actions, including my digital footprint and the legal implications of sharing inappropriate material."
- Tracking and informed decisions: "I can understand that photographs, locations and tags can be tracked and can make informed decisions accordingly."
- File management techniques: "I can use appropriate advanced file management techniques, e.g., version history, restore previous version, tagging, compression."
- Online collaboration: "I can independently select and use a range of online collaboration tools to create a project with others in one or more languages, e.g., making use of online technology to share and present ideas to others."

Week 5: Cybersecurity and Encryption

Lesson Title: Introduction to Encryption

Learning Objectives:

- I can explain what encryption is and why it is essential for cybersecurity.
- I can understand how encryption protects sensitive information online.
- I can evaluate the different types of encryption and their uses.

Outcomes:

- All: Define encryption and explain its basic purpose in protecting data.
- Most: Discuss how encryption protects data in transit and at rest.
- Some: Analyse different encryption methods and evaluate their strengths and weaknesses.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will act as security consultants advising a company on how to secure its sensitive data. They will explore various encryption methods (e.g., symmetric and asymmetric encryption) and recommend the best options for the company's needs.
- Activity:
  Students will research real-world examples where encryption either protected or failed to protect sensitive data. They will present their findings on how encryption plays a vital role in securing communications and transactions online.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will create an Encryption Best Practices Guide for companies and individuals to use. The guide will detail the importance of encryption, types of encryption, and how to implement it effectively. This guide will be included in their portfolio.

Digital Competence Framework (DCF) References:

Progression Step 3:

- Encryption awareness: "I can manage files and folders locally or online, e.g. move files to a folder."
- Collaboration: "I can work with others to create an online collaborative project for a specific purpose, sharing and appropriately setting permissions for other group members, e.g., editing, commenting, viewing."
- **Planning and organisation**: "I can independently create and plan work before beginning a digital task."
- **Encryption knowledge**: "I can show an understanding of the importance of the order of statements within algorithms."

Progression Step 4:

- Encryption knowledge: "I can show an awareness of simple encryption and its purpose, e.g. to send sensitive data more securely."
- Collaboration tools: "I can independently select and use a range of online collaboration tools to create a project with others in one or more languages, e.g. making use of online technology to share and present ideas to others."
- **Advanced encryption techniques**: "I can use appropriate advanced file management techniques, e.g. version history, restore previous version, tagging, compression."

Week 6: Malware and Cyber Attacks

Lesson Title: Understanding Malware and Its Impact

Learning Objectives:

- I can explain what malware is and the different types of malware (e.g., viruses, ransomware, spyware).
- I can understand the consequences of a malware infection on personal and organisational systems.
- I can identify methods to prevent and respond to malware attacks.

Outcomes:

- All: Identify different types of malware and explain their basic function.
- Most: Discuss how malware infects systems and its impact on individuals and organisations.
- Some: Analyse real-world malware cases and evaluate the effectiveness of different prevention and response strategies.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will take on the role of cybersecurity professionals responding to a malware outbreak in a company's network. They will analyse the type of malware involved and recommend steps to contain and eliminate it.
- Activity:
  Students will research famous malware attacks, such as the WannaCry ransomware attack, and explore how these attacks affected various organisations. They will discuss the long-term consequences of malware infections and how they could have been prevented.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will create a Malware Prevention and Response Guide that outlines steps for protecting systems from malware and how to respond effectively if an infection occurs. This guide will be included in their portfolio.

Digital Competence Framework (DCF) References:

Progression Step 3:

- Online behaviour: "I can demonstrate appropriate online behaviour and apply a range of strategies to protect myself and others from possible online dangers, bullying and inappropriate behaviour, e.g., turn off comments on digital media, reporting, block users."
- File management: "I can manage files and folders locally or online, e.g. move files to a folder."
- Planning and organisation: "I can independently create and plan work before beginning a digital task."
- Collaboration: "I can work with others to create an online collaborative project for a specific purpose, sharing and appropriately setting permissions for other group members, e.g., editing, commenting, viewing."

Progression Step 4:

- Advanced file management: "I can use appropriate advanced file management techniques, e.g. version history, restore previous version, tagging, compression."
- Encryption knowledge: "I can show an awareness of simple encryption and its purpose, e.g. to send sensitive data more securely."
- File management and encryption: "I can manage links to files, taking permissions and file locations into account, e.g. some file storage systems will utilise dynamic hyperlinks so that if a file location is changed the links remain intact, whereas changing file location could result in a broken hyperlink."
- Online collaboration: "I can independently select and use a range of online collaboration tools to create a project with others in one or more languages, e.g., making use of online technology to share and present ideas to others."

Week 7: Social Engineering and Online Scams

Lesson Title: Preventing and Identifying Social Engineering Attacks

Learning Objectives:

- I can explain what social engineering is and how it manipulates individuals to share sensitive information.
- I can identify different types of social engineering attacks (e.g., phishing, baiting, pretexting).
- I can develop strategies to protect myself and others from falling victim to social engineering scams.

Outcomes:

- All: Identify basic social engineering techniques and explain how they deceive individuals.
- Most: Discuss how social engineering attacks are executed and the psychological principles behind them.
- Some: Analyse case studies of social engineering attacks and recommend effective prevention strategies.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will take on the role of cybersecurity consultants tasked with identifying potential social engineering vulnerabilities within an organisation. They will simulate various attack scenarios and suggest prevention methods.
- Activity:
  Students will research famous social engineering attacks, such as the Twitter hack of 2020, and examine how attackers were able to manipulate employees. They will discuss how organisations can improve training and security to mitigate these risks.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will create a Social Engineering Awareness Campaign for their school or community, which will include posters, presentations, and tips for

recognising and preventing social engineering attacks. This campaign will be included in their portfolio.

Digital Competence Framework (DCF) References:

Progression Step 3:

- Online behaviour: "I can demonstrate appropriate online behaviour and apply a range of strategies to protect myself and others from possible online dangers, bullying, and inappropriate behaviour, e.g., turn off comments on digital media, reporting, block users."
- Collaboration: "I can work with others to create an online collaborative project for a specific purpose, sharing and appropriately setting permissions for other group members, e.g., editing, commenting, viewing."
- **Planning and collaboration**: "I can independently create and plan work before beginning a digital task."
- **Understanding digital dangers**: "I can understand the risks and legal consequences of sending intimate images and content/sexting."

Progression Step 4:

- Appropriate online behaviour: "I can act appropriately online, keeping myself safe and behaving in a responsible manner."
- Advanced file management: "I can use appropriate advanced file management techniques, e.g., version history, restore previous version, tagging, compression."
- **Online collaboration tools**: "I can independently select and use a range of online collaboration tools to create a project with others in one or more languages, e.g., making use of online technology to share and present ideas to others."
- **Encryption and file management**: "I can show an awareness of simple encryption and its purpose, e.g., to send sensitive data more securely."

Week 8: Final Review and Escape Room Challenge

Lesson Title: Cybersecurity Escape Room

Learning Objectives:

- I can apply all learned concepts from previous lessons.
- I can collaborate to solve cybersecurity challenges in a simulated environment.
- I can reflect on the importance of cybersecurity in daily life.

Outcomes:

- All: Apply basic cybersecurity knowledge to solve simple challenges in a collaborative environment.
- Most: Work collaboratively to solve intermediate cybersecurity problems using knowledge from previous lessons.
- Some: Analyse and resolve complex cybersecurity issues, demonstrating critical thinking and leadership during the Escape Room Challenge.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students participate in an Escape Room-style challenge where they must solve a simulated cybercrime scenario using knowledge gained from previous weeks. Challenges will include identifying malware, securing a network, and detecting phishing attempts.
- Activity:
  Students will work in teams to solve various cybersecurity challenges in a timed environment. Upon completion, students will reflect on their performance and how the concepts they've learned can be applied in real-life situations.

Portfolio-Building Activity (Lesson 2):

- Task:
  After completing the Escape Room Challenge, students will engage in peer assessment, providing feedback to their classmates on their problem-solving and teamwork skills. Students will also write a reflection on the importance of cybersecurity in daily life and how the skills they've learned will help them stay secure online.