Lesson Plan: Week 1 (Part 1) – Introduction to Digital Privacy

Lesson Title: Avatar Creation and Data Privacy
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can understand what personal data is and why it is valuable.
- I can identify types of personal data shared online.
- I can begin to explore how personal data contributes to a digital footprint.

Success Criteria:

- All: Can define personal data and list examples shared online.
- Most: Can describe how creating a digital avatar involves sharing personal information.
- Some: Can reflect on how personal data, when combined, forms a digital footprint.

Starter Activity (10 mins):

- Activate prior knowledge and introduce key concepts.
    - Pose the question: "What do you think personal data is?" Have students write down examples of what they might share online (name, location, hobbies).
    - Show a short video or infographic introducing digital footprints—how every interaction online leaves a trace, and that this creates a trail of data.
- Discussion:
    - Ask students: "Have you ever thought about what your online footprint looks like?"

Main Activity: Avatar Creation (25 mins):

- Engage students in creating an online identity to explore how personal data is shared.
  Instructions:

    - Students create an avatar using an online tool (or draw one if internet access is limited). Along with the avatar, they provide personal details such as:
        - Username or Display Name
        - Location
        - Hobbies/Interests
        - Profile Bio (short description)
    - Encourage students to think about what information they are comfortable sharing with others and why.
- Reflection:
    - Ask students to reflect on the process of creating their avatar: "What personal information did you include? What do you think others could learn about you from these details?"

Plenary (10 mins):

- Summarise key points and prepare for the next lesson.
    - Recap the concept of digital footprints and explain how small pieces of personal information, when combined, can reveal more than expected.
    - Explain that in the next lesson (Part 2), the class will use their avatars in a Guess the Person activity to explore how personal data can be used to identify someone.

Resources:

- Internet access or printed avatar worksheets.
- Video/infographic about digital footprints.
- Worksheet for avatar details (username, bio, hobbies, etc.).

Assessment:

- Formative: Teacher observation of student participation during avatar creation and reflection discussions.

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."
    - Understanding digital footprint: "I can understand the implications of online actions, including my digital footprint and the legal implications of sharing inappropriate material."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Present ideas convincingly using techniques such as rhetorical questions or gestures.
    - Year 10: Present ideas that meet the demands of different audiences.

Lesson Plan: Week 1 (Part 2) – Digital Footprints and Privacy Risks

Lesson Title: Guess the Person – Exploring Digital Footprints
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can explain how digital footprints affect my online presence.
- I can analyse how small pieces of data can be combined to reveal personal information.
- I can develop strategies to protect my personal data and minimise online risks.

Success Criteria:

- All: Can recognise that sharing personal information contributes to a digital footprint.
- Most: Can analyse how shared data can reveal more about an individual than intended.
- Some: Can propose strategies for minimising personal data exposure online.

Recap of Part 1 (10 mins):

- Review key concepts from the previous lesson and activate prior knowledge.
    - Recap the Avatar Creation activity from Part 1, where students created digital personas.
    - Discuss how personal data shared through avatars contributes to a digital footprint.
    - Ask: "What types of information did you share in your avatar that could identify you?"

Main Activity: Guess the Person (30 mins):

- Demonstrate the risks of oversharing personal data by identifying classmates based on their avatars.
  Instructions:
    - The teacher will read out the details of anonymous avatars (created in Part 1) without revealing the names. These details may include:
        - Username or display name
        - Location
        - Hobbies or interests
        - Profile bio

    - The class (or selected students) will try to guess who the avatar belongs to based on the information provided.
- Class Discussion:
    - After each guess, discuss:
        - What clues helped identify the person?
        - How do small pieces of data (like hobbies or location) reveal more than expected?
    - Guide the conversation towards understanding how data aggregation leads to revealing personal details.

Extended Activity: Reflect and Respond (15 mins):

- Students reflect on their digital footprints and develop strategies to protect personal data.
  Instructions:
    - Students will write a brief reflection in response to the following questions:
        - How did creating an avatar help me understand the concept of a digital footprint?
        - What surprised me during the Guess the Person activity?
        - What steps will I take in the future to better protect my personal data online?
- Group Discussion:
    - Students will share their reflections in small groups and discuss strategies for protecting their online identity.
    - Encourage students to think of practical steps they can take (e.g., limiting what they share publicly, reviewing privacy settings on social media).

Plenary (5 mins):

- Summarise the key points and provide closure.
    - Recap the key takeaway: Your digital footprint is made up of all the small pieces of information you share online, and it can be more revealing than you expect.
    - Ask: "What's one thing you will do differently online after today's lesson?"
    - Introduce the idea that the next lesson will explore phishing and online scams as further risks to personal data.

Resources:

- List of avatar details from Part 1 (compiled by the teacher).
- Reflection worksheets (or lined paper for writing responses).
- Projector or interactive board for displaying anonymous avatar details.

Assessment:

- Formative:
    - Teacher observation during the "Guess the Person" activity.
    - Participation in group discussions.
- Summative:
    - Student reflections on strategies to protect personal data.

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."
- Understanding digital footprint: "I can understand the implications of online actions, including my digital footprint and the legal implications of sharing inappropriate material."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Take a range of roles in group discussion, including in more formal situations.
    - Year 10: Adapt talk in a range of roles, including in more formal situations and purposes.
- Writing Skills:
    - Year 9: Use a structured and clear explanation in writing.
    - Year 10: Write reflective texts that analyse ideas and offer practical solutions.

Timing Summary:

- Recap: 10 mins
- Main Activity (Guess the Person): 30 mins
- Extended Activity (Reflection): 15 mins

- Plenary: 5 mins
  Total: 60 mins

Lesson Plan: Week 2 (Part 1) – Understanding Phishing and Social Engineering

Lesson Title: Phishing and Social Engineering Tactics
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

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 recognise social engineering tactics when they are used in everyday situations.

Success Criteria:

- All: Recognise basic phishing indicators and describe social engineering tactics like shoulder surfing and blagging.
- Most: Explain how phishing and social engineering tactics work together to deceive individuals.
- Some: Develop strategies for preventing both phishing and social engineering attacks.

Starter Activity (10 mins):

- Introduce key concepts of phishing and social engineering.
    - Show a real-world example of a phishing email and ask students to identify red flags (e.g., spelling mistakes, fake URLs, urgent tone).
    - Introduce social engineering tactics like blagging (pretending to be someone else), shoulder surfing (watching someone's private information), and pretexting (inventing a fake scenario to get information).

Main Activity: Phishing and Social Engineering Simulation (30 mins):

- Engage students in a simulation where they encounter both phishing and social engineering tactics.
  Instructions:

    - Split the class into small groups. Each group will receive two phishing emails to analyse. Alongside this, one student in the class will be secretly assigned as the "Social Engineer."
    - The Social Engineer will have the task of trying to extract information from their peers using strategies like:
        - Blagging: Pretending to need personal information to complete a task.
        - Shoulder Surfing: Peeking at other students' information during the lesson (e.g., usernames or answers).
        - Pretexting: Creating a fake story to gain trust and extract data.
- Student Task:
    - Analyse the phishing emails for red flags and discuss how phishing and social engineering might work together (e.g., a phishing email tricks someone into clicking a link, and a social engineer asks for further details).
- Teacher's Role:
    - Monitor the "social engineering" activity without revealing who the "Social Engineer" is. At the end of the activity, ask students if they can identify the Social Engineer and what tactics were used.

Plenary (10 mins):

- Reflect on phishing and social engineering tactics used during the simulation.
    - Ask: "Who was the Social Engineer? How did they try to manipulate you into giving information?"
    - Discuss how phishing and social engineering work together to compromise personal data.
    - Highlight the importance of being aware of both phishing emails and social engineering attacks in the real world.

Resources:

- Example phishing emails (anonymous).
- A secret "Social Engineer" selected by the teacher.

Assessment:

- Formative: Teacher observation of how students identify phishing tactics and how they handle the Social Engineer's strategies.

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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Take roles in group discussions and respond to the tactics used.
    - Year 10: Adapt responses in different situations, especially when faced with deception.

Timing Summary:

- Starter Activity: 10 mins
- Main Activity (Phishing and Social Engineering Simulation): 30 mins
- Plenary: 10 mins
  Total: 60 mins

Lesson Plan: Week 2 (Part 2) – Anti-Phishing and Social Engineering Campaign

Lesson Title: Creating an Anti-Phishing and Social Engineering Awareness Campaign
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can develop strategies to protect against phishing and social engineering.
- I can design an effective awareness campaign to educate others about phishing and social engineering risks.

Success Criteria:

- All: Create basic anti-phishing and anti-social engineering materials with clear tips.
- Most: Design a campaign with examples of phishing and social engineering tactics, including preventative strategies.
- Some: Develop a comprehensive campaign that includes analysis of phishing techniques and social engineering tactics tailored for different audiences.

Recap of Part 1 (10 mins):

- Review phishing and social engineering concepts from Part 1.
    - Recap the phishing analysis and the Social Engineer activity from Part 1.
    - Ask: "What did we learn about how phishing and social engineering work together to deceive people?"

Social Engineer Warning (2 mins):

- Reinforce the awareness of social engineering tactics.
    - Inform the students: "There is one person in this room who will try to use social engineering tactics to extract information from you throughout this lesson. Be aware and try to avoid falling for it."
    - Encourage students to stay vigilant for tactics like blagging, shoulder surfing, or pretending during the lesson.

Main Activity: Designing an Anti-Phishing and Social Engineering Campaign (38 mins):

- Students create anti-phishing and anti-social engineering materials to help their peers avoid falling for scams.
  Instructions:
    - In groups, students will design an Anti-Phishing and Social Engineering Campaign for their school, which includes:
        - Infographics: Highlighting common phishing and social engineering tactics and how to avoid them.
        - Email Templates: Examples of phishing emails alongside guidance for avoiding scams.
        - Social Media Posts: Tips on how to spot social engineering tactics in online interactions (e.g., fake profiles, scammers asking for personal information).
- Teacher's Role:
    - Guide the students in creating visually appealing materials that are relevant to their peers.
    - Monitor the secret Social Engineer, who will attempt to use deception to extract information from students as they work (e.g., asking for answers, subtly gathering personal details).

Social Engineer Reveal and Discussion (5 mins):

- Reflect on social engineering tactics used during the activity.
    - Ask students if they could identify the Social Engineer during the lesson. What tactics were used, and how did they avoid falling for them?
    - Discuss how being aware of these tactics makes it easier to defend against social engineering attacks in real life.

Plenary (5 mins):

- Summarise the key points and provide closure.
    - Each group presents part of their Anti-Phishing and Social Engineering Campaign to the class.
    - Recap the importance of raising awareness about phishing and social engineering, and the key steps to avoid becoming a victim.

Resources:

- Templates for infographics, email designs, and social media posts.
- Projector for displaying campaign ideas.
- Secret Social Engineer (selected by the teacher).

Assessment:

- Formative: Teacher observation of group work and how well students avoid the Social Engineer's tactics.

- Summative: Completed campaign materials.

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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
  - Year 9: Present ideas and tactics in an anti-phishing campaign format.
  - Year 10: Use persuasive language to engage peers about online safety.

Timing Summary:

- Recap: 10 mins
- Social Engineer Warning: 2 mins
- Main Activity (Campaign Design): 38 mins
- Social Engineer Reveal and Discussion: 5 mins
- Plenary: 5 mins
  Total: 60 mins

Lesson Plan: Week 3 (Part 1) – Cybersecurity War Room: Red Team vs Blue Team

Lesson Title: Cybersecurity War Room: Defending the Network from a Live Attack
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can work with my team to detect and respond to a cyberattack.
- I can analyse network traffic to identify abnormal patterns and respond to them in real-time.
- I can develop strategies to mitigate cyber threats during a network breach.

Success Criteria:

- All: Understand how to monitor basic network traffic and recognise suspicious activity.
- Most: Collaborate effectively to stop an active cyberattack by analysing traffic logs.
- Some: Devise advanced strategies to mitigate the attack and secure the network against future breaches.

Welcome to the War Room: The Cyberattack Begins (5 mins)

Set the stage for an immersive simulation.

- Scenario Setup:
    - "The company network is under attack! You are now part of the company's Cybersecurity War Room, and it's your job to defend the network before the attackers can steal sensitive data or shut down operations."
    - Split the students into two teams: Red Team (Attackers) and Blue Team (Defenders).
- The Drama:
    - Blue Team (Defenders): Their mission is to detect and respond to incoming attacks by monitoring traffic logs and stopping malicious activity.
    - Red Team (Attackers): They will launch cyberattacks by feeding in fake data, inserting anomalies in traffic logs, and tricking the defenders into making mistakes. Their goal is to cause a breach without being caught.
- Tools for Drama:

    - Use sound effects or visual aids (e.g., sirens or breach alerts) to simulate the high stakes of the attack.
    - Introduce a time limit: "The attack will escalate in 45 minutes! Every 10 minutes, the threat grows."

Assigning Roles and Briefing the Teams (10 mins)

Blue Team (Defenders):

- Network Admin: Monitors the network logs and identifies suspicious activity.
- Incident Response Lead: Coordinates the team's response and reports the findings.
- Security Analyst: Verifies whether an IP address or traffic anomaly is truly suspicious.
  Mission:
    - Each role is tasked with analysing traffic logs and identifying anomalies (e.g., unusual IP addresses, traffic spikes).
    - They must collaborate and quickly decide how to stop attacks (e.g., blocking IPs, monitoring specific traffic).
- Guidance:
    - Provide the Blue Team with simplified network logs (pre-prepared) that show a mix of normal and suspicious traffic. The logs will be updated at regular intervals (every 10 minutes) with new threats.

Red Team (Attackers):

- Lead Attacker: Decides the attack strategy (e.g., DoS attack, data exfiltration, ransomware).
- Saboteur: Feeds fake information into the logs to distract the Blue Team.
- Hacker: Simulates network breaches by inserting anomalies (e.g., an unusual IP address or a massive spike in data transfer).
  Mission:
    - Attackers will launch a series of cyberattacks (e.g., data breaches, fake IPs, phishing attempts) by creating traffic anomalies or inserting "attacker" IP addresses into the logs.
    - They must escalate the attack every 10 minutes, increasing pressure on the defenders.

Main Activity: The Cyber War Room Simulation (35 mins)

The Attack Unfolds:

- Teams respond to the attack in real-time, using network traffic logs and problem-solving skills to either attack or defend the network.
  How It Works:

    - Red Team will feed in attack data (fake traffic patterns) into the Blue Team's network logs. This could include:
        - Sudden spikes in outgoing traffic at odd times (suggesting a data breach).
        - Unknown IP addresses making requests to the server.
        - A large data transfer to an unknown IP.
    - Blue Team must identify these anomalies using the logs and take immediate action (e.g., block the IP, shut down a specific port, or raise an alert).

Real-Time Updates:

- Every 10 minutes, the teacher will simulate an escalation in the attack:
    - "You've just noticed a spike in data transfers at 2 AM to an unknown IP address!"
    - "An unknown IP address is trying to connect to the internal server!"
- How Blue Team Reacts:
    - They must collaborate, analyse the logs, and make decisions quickly (e.g., blocking traffic from certain IPs, isolating certain sections of the network).
    - Incident Response Lead will write a brief report for each attack explaining what happened and how they responded.

Red Team's Role:

- Every 10 minutes, they will launch a new phase of attacks. The teacher can assist the Red Team with new instructions or challenge ideas:
    - Phase 1: Insert fake IPs or data spikes (minor disruption).
    - Phase 2: Begin exfiltrating data (simulate outgoing traffic spikes).
    - Phase 3: Trigger a major attack (e.g., DDoS simulation—massive amounts of fake traffic).

Plenary: Debriefing the Cyberattack (10 mins)

Blue Team's Report:

- Incident Response Lead from each Blue Team presents what they found:
    - "We noticed a traffic spike at 3 AM and blocked the suspicious IP."
    - "An unknown IP attempted to connect multiple times, so we isolated it."

Red Team's Debrief:

- Lead Attacker presents the strategy:
    - "We used fake IPs to distract the defenders while launching the real attack."
    - "Our goal was to overwhelm the defenders with multiple small attacks."

Reflection:

- Ask both teams: "What strategies worked? What could have been done differently?"
- Discuss how real-world cybersecurity teams handle these types of threats and why collaboration, quick decision-making, and vigilance are key.

Resources Needed:

- Network Traffic Logs: Printable or digital logs showing normal and suspicious traffic patterns.
- Red Team Attack Instructions: Pre-written scenarios for the Red Team to follow (including fake IPs, data spikes, and escalating attacks).
- Blue Team Role Cards: Clearly define roles for the defenders, so they know exactly what to look for and how to act.
- Problem-Solving Prompts: For both teams to know what questions to ask during each phase of the attack (e.g., "Is this IP legitimate? Is this traffic volume normal?").
- Incident Response Report Templates: A simple form where the Blue Team Incident Response Lead records what happened and how they responded.

Assessment:

- Formative: Teacher observation of how the teams handle the attack, collaboration, and problem-solving.
- Summative: A brief Incident Response Report from the Blue Team explaining what threats they detected and how they responded, plus a Red Team Debrief on how the attack was carried out.

Digital Competence Framework (DCF) Skills:

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."

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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Present findings in group discussions during attack debriefs.
    - Year 10: Present a structured incident response and reflection on team decisions.

Timing Summary:

- Starter Activity: 5 mins
- Assigning Roles and Briefing: 10 mins
- Main Activity (War Room Simulation): 35 mins
- Plenary (Debriefing): 10 mins
  Total: 60 mins

Lesson Plan: Week 3 (Part 2) – Post-War Room: Building a Cyber Defense Strategy

Lesson Title: Creating a Cyber Defense Strategy After a Network Attack
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can reflect on the lessons learned from a simulated cyberattack.
- I can develop a comprehensive Incident Response Plan to prevent future network breaches.
- I can create proactive strategies to strengthen a network against future cyber threats.

Success Criteria:

- All: Reflect on the War Room experience and create basic strategies to respond to similar attacks.
- Most: Develop a detailed Incident Response Plan that outlines how to detect and respond to cyberattacks.
- Some: Propose advanced cyber defence strategies to prevent future breaches and minimise damage during an attack.

Starter: Post-War Room Debrief (10 mins)

Reflect on the War Room simulation and lessons learned.

- Recap: Start with a brief discussion of the War Room simulation.
    - "What was the most challenging part of defending the network?"
    - "How did the attackers manage to get through? What would you do differently next time?"

Group Reflection:

- Split students back into their Blue Teams (defenders from the last lesson) to discuss:
    - What went wrong during the attack?
    - What did they do well?
    - How can they improve their defences for next time?
- Class Discussion: Have each team share one key lesson they learned from the War Room simulation.

Main Activity: Designing an Incident Response Plan (35 mins)

Students create detailed plans for responding to future cyberattacks.

Instructions:

- Each Blue Team will work together to create a comprehensive Incident Response Plan (IRP) for their fictional company based on what they learned from the War Room simulation.
- The plan must include:
    - Preparation: What steps should the company take to ensure it's ready for future cyberattacks? (e.g., regular network monitoring, backup systems, staff training)
    - Detection: How can the team detect unusual network activity earlier? (e.g., using traffic monitoring tools, setting up alerts)
    - Response: What immediate steps should be taken when a cyberattack is detected? (e.g., isolating the affected system, blocking IPs, alerting the security team)
    - Recovery: How should the company recover after an attack? (e.g., restoring data from backups, investigating how the breach happened)
    - Prevention: What long-term steps can the company take to prevent future breaches? (e.g., stronger firewalls, two-factor authentication, regular penetration testing)

Guidance:

- Provide the teams with a simple template for their Incident Response Plan. This can include clear sections with prompts, so they know what to focus on.
- Encourage them to refer back to the War Room simulation to identify weaknesses and suggest improvements.

Optional Twist:

- Red Teams (the attackers from the War Room simulation) can contribute by playing the role of external cybersecurity consultants. They can suggest improvements based on their attack strategy and help identify weaknesses that the defenders missed.

Plenary: Presenting Cyber Defense Strategies (15 mins)

Teams present their Incident Response Plans and receive feedback.

- Each Blue Team presents their Incident Response Plan to the class, focusing on:
    - How they plan to detect and respond to future attacks.

    - What long-term defences they will put in place to prevent similar breaches.
- Class Discussion: After each presentation, open the floor for questions:
    - "What do you think was the strongest part of the plan?"
    - "Are there any weaknesses in the plan that could still be exploited?"
- Feedback: The teacher and classmates provide constructive feedback on each team's Incident Response Plan, discussing how realistic and effective the strategies are.

Resources:

- Incident Response Plan Template: A simple worksheet with sections for Preparation, Detection, Response, Recovery, and Prevention.
- Projector or Whiteboard: For presenting defence strategies.

Assessment:

- Formative: Teacher observation of teamwork and the creation of the Incident Response Plan.
- Summative: Teams will submit their Incident Response Plan, and it will be assessed based on its thoroughness, clarity, and practicality.

Digital Competence Framework (DCF) Skills:

Progression Step 3:

- 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:

- 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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Collaborate to design and present an Incident Response Plan.

    - Year 10: Present a structured defence strategy and respond to feedback.

Timing Summary:

- Starter Activity: 10 mins
- Main Activity (Designing the IRP): 35 mins
- Plenary (Presenting Plans): 15 mins
  Total: 60 mins

Lesson Plan: Week 4 (Part 1) – Digital Footprints and Online Safety

Lesson Title: Investigating Your Digital Footprint
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

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.

Success Criteria:

- 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.

Starter Activity: Uncovering Digital Footprints (10 mins)

Introduce students to the concept of a digital footprint and its implications.

- Begin by asking: “What do you think a digital footprint is?”
- Show a short video clip or infographic that explains the concept of a digital footprint and how every action online leaves a trace (social media posts, comments, purchases, etc.).

Discussion:

- “How many times have you posted something online? Have you ever thought about where that information goes or who might see it?”
- Engage students by asking them to think about what their digital footprint might look like.

Main Activity: Investigating Public Figures’ Digital Footprints (35 mins)

Students analyse how digital footprints can impact a person's life positively and negatively.

Scenario:

- Students take on the role of digital investigators. They will explore the online presence of various public figures and analyse how their digital footprints have influenced their personal or professional lives.

Instructions:

- Divide students into small groups. Each group will select a public figure (e.g., a celebrity, athlete, politician, or influencer) to investigate.
- Provide the groups with guiding questions:
    - What kind of information is publicly available about this person? (e.g., social media posts, news articles, videos)
    - How has this person's digital footprint positively impacted their career?
    - Have there been any negative consequences (e.g., scandals, career setbacks) due to their online presence?

Task:

- Each group will create a Digital Footprint Analysis Report, detailing:
    - Key elements of the person's digital footprint.
    - Examples of positive and negative impacts.
    - Lessons learned from this individual's online activity.

Teacher's Role:

- Circulate around the room, providing guidance and helping students access information if needed.
- Encourage critical thinking: "What could this person have done differently? How could they have protected their digital footprint better?"

Plenary: Digital Footprint Reflection (10 mins)

Reflect on the findings and connect them to students' own online behaviour.

- Ask each group to briefly present one key finding from their analysis.
- Discuss: "What can we learn from these public figures about managing our digital footprints?"
- Introduce the concept of creating their Digital Footprint Management Plan in the next lesson.

Resources:

- Laptops or tablets for researching public figures.
- Infographic/video explaining digital footprints.
- Digital Footprint Analysis Report template.

Assessment:

- Formative: Teacher observation of group discussions and research.
- Summative: Digital Footprint Analysis Report, assessing students' ability to identify the impact of online activity.

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."

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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Present ideas and issues convincingly using a range of techniques for impact.
    - Year 10: Present ideas and issues to meet the demands of different audiences.

Timing Summary:

- Starter Activity: 10 mins
- Main Activity: 35 mins
- Plenary: 10 mins
  Total: 55 mins

Lesson Plan: Week 4 (Part 2) – Digital Footprints and Online Safety

Lesson Title: Creating Your Digital Footprint Management Plan
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can develop strategies to manage and minimise my digital footprint.
- I can understand how to monitor my online presence.
- I can create a plan to protect my identity and personal information online.

Success Criteria:

- All: Understand the importance of managing a digital footprint.
- Most: Create a detailed plan to monitor and control online activity.
- Some: Analyse and propose advanced strategies for maintaining a safe digital footprint.

Recap and Reflection (10 mins)

Reflect on what students learned about digital footprints from the previous lesson.

- Ask students: “What did we learn about the importance of managing a digital footprint?”
- Discuss some of the most interesting case studies from Lesson 1 and how they can relate to students' own online activity.
- Introducing today’s task: Creating a Digital Footprint Management Plan.

Main Activity: Developing a Digital Footprint Management Plan (40 mins)

Students create their own strategies for managing and controlling their digital footprints.

Instructions:

- Provide students with a template for their Digital Footprint Management Plan, which will include:
    - Monitoring: What steps will you take to monitor your online presence? (e.g., Google yourself regularly, check privacy settings)

    - Controlling: How will you control what others can see about you? (e.g., adjusting social media privacy settings, being selective about what you post)
    - Minimising: What actions can you take to reduce your digital footprint? (e.g., deleting old accounts, limiting personal information shared online)

Task:

- Students will work individually to complete their management plans, using what they learned from the case studies to create practical and realistic strategies.
- Encourage them to think critically about their current online activity and what changes they could make to protect their digital footprint.

Plenary: Sharing Strategies (10 mins)

Students share their Digital Footprint Management Plans and reflect on their learning.

- Ask students to share one key strategy they included in their plan with the class.
- Discuss: “Why is it important to manage our digital footprints? How can these strategies help us stay safe online?”

Resources:

- Digital Footprint Management Plan template (printable or digital).
- Projector/whiteboard for sharing strategies.

Assessment:

- Formative: Teacher observation and individual feedback during the planning process.
- Summative: Completed Digital Footprint Management Plans will be added to each student’s portfolio.

Digital Competence Framework (DCF) References:

Progression Step 3:

- 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:

- 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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Present ideas and issues convincingly using a range of techniques for impact.
    - Year 10: Present ideas and issues to meet the demands of different audiences.

Timing Summary:

- Recap and Reflection: 10 mins
- Main Activity (Digital Footprint Management Plan): 40 mins
- Plenary: 10 mins
  Total: 60 mins

Lesson Plan: Week 5 (Part 1) – Cybersecurity and Encryption

Lesson Title: Encryption Methods: Group Exploration and Demonstration
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can explain what encryption is and why it is essential for cybersecurity.
- I can explore different encryption methods and how they work.
- I can demonstrate and explain an encryption method to my peers.

Success Criteria:

- All: Define encryption and demonstrate a simple encryption method.
- Most: Explain how encryption protects data in transit and at rest.
- Some: Analyse encryption methods and evaluate their practical applications in the modern world.

Starter Activity: Introduction to Encryption (5 mins)

Quickly review the concept of encryption and set up the group activity.

- Ask students: “What do we know about encryption?”
- Briefly review that encryption is scrambling data so that it can only be read by someone with the correct key.
- Explain that today they will be working in groups to learn different encryption methods, practise them, and teach them to the rest of the class.

Main Activity: Group Encryption Exploration (40 mins)

Students work in groups, exploring and experimenting with different encryption methods.

Group Setup:

- Divide students into four groups, assigning each group an encryption method.
- Give them 20 minutes to learn the method, practice encoding and decoding messages, and discuss its strengths and weaknesses.
- After 20 minutes, each group will prepare a 3-minute presentation to teach their encryption method to the class.

Encryption Methods for Group Exploration:

Group 1: Caesar Cipher

- Description: Students use Caesar Cipher to shift letters by a set number.
- Task:
    - Encode and decode messages using a Caesar Cipher wheel (or a digital tool).
    - Example: Shift by 3 (A → D, B → E, C → F, etc.).
- Discussion:
    - Why is Caesar's Cipher easily broken?
    - What are its historical uses, and why is it now obsolete?

Group 2: Atbash Cipher (Alternative for XOR)

- Description: Atbash is a substitution cipher where the alphabet is reversed (A → Z, B → Y, etc.).
- Task:
    - Use an Atbash Cipher key to encode and decode messages.
    - Example: "HELLO" becomes "SVOOL".
- Discussion:
    - How does this method work, and why is it easy to break?
    - What historical uses did Atbash have?

Group 3: Vigenère Cipher (Alternative for Symmetric Key Encryption)

- Description: A polyalphabetic cipher using a repeating keyword to encode and decode messages.
- Task:
    - Use the Vigenère Cipher table and a keyword to encrypt and decrypt messages.
    - Example: Keyword "KEY" is repeated for the length of the message "HELLO" (K → H, E → E, Y → L, K → L, etc.).
- Discussion:
    - Compare with Caesar's Cipher and discuss why Vigenère is harder to crack.
    - What are the pros and cons of using a keyword in encryption?

Group 4: Substitution Cipher

- Description: A substitution cipher where each letter is substituted with a different symbol or letter.
- Task:
    - Create your own cipher key (e.g., A → %, B → @, C → , etc.).
    - Use this to encrypt and decrypt messages.
- Discussion:
    - How does the custom cipher work?

    - Why is it more secure than Caesar's Cipher but still breakable?

Group Presentations (20 mins)

Each group has 3-4 minutes to present their encryption method to the class:

- How it works (e.g., how to encode/decode messages).
- Example demonstration (one or two examples of encoding and decoding a message).
- Strengths and weaknesses of their encryption method (e.g., ease of breaking, historical uses, modern relevance).

Teacher's Role:

- Guide the presentations, asking follow-up questions like:
    - "What would happen if the key fell into the wrong hands?"
    - "Why is your method stronger or weaker than others?"

Plenary: Reflecting on Encryption (5 mins)

Reflect on how encryption methods compare and connect to modern encryption.

- Class Discussion:
    - "Which encryption method was the strongest, and why?"
    - "How do modern encryption methods, like AES or RSA, improve on these historical methods?"
- Wrap-Up: Discuss how encryption is essential for online safety, particularly for things like banking, emails, and online shopping.

Resources:

- Caesar Cipher wheel or digital tool.
- Atbash Cipher key (alphabet reversed) handouts.
- Vigenère Cipher table and keyword instructions.
- Substitution Cipher worksheets.
- Projector/whiteboard for presentations.

Assessment:

- Formative: Teacher observation of group discussions and presentations.
- Summative: Group presentations will be evaluated based on:
    - Accuracy of explanation.
    - Effectiveness of demonstration.
    - Depth of understanding of strengths and weaknesses.

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."

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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Explain and demonstrate encryption methods in group presentations.
    - Year 10: Present strategies for protecting data using different encryption methods.

Timing Summary:

- Starter Activity: 5 mins
- Main Activity (Group Exploration): 40 mins
- Group Presentations: 15 mins
  Total: 60 mins

Lesson Plan: Week 5 (Part 2) – Encryption Best Practices

Lesson Title: Creating an Encryption Best Practices Guide
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can develop practical strategies for using encryption in real-world scenarios.
- I can create an encryption guide that explains the importance of protecting sensitive information.
- I can evaluate different encryption methods and recommend their best uses.

Success Criteria:

- All: Understand the importance of encryption and how it protects data.
- Most: Create a clear and well-organised guide outlining best practices for encryption.
- Some: Recommend advanced encryption strategies and evaluate their effectiveness in different contexts.

Recap and Reflection (10 mins)

Review key learnings from the previous lesson and transition into creating the Encryption Best Practices Guide.

- Recap: Ask students to briefly explain the encryption methods they explored last lesson. Highlight the strengths and weaknesses of each (Caesar Cipher, Atbash, Vigenère, and Substitution).
- Discussion:
    - Why is encryption so important for online safety and data protection?
    - How do modern encryption methods build on the concepts we explored?
- Introduce the task for today: Each student will create an Encryption Best Practices Guide for individuals and businesses, focusing on how to protect sensitive data.

Main Activity: Developing the Encryption Best Practices Guide (40 mins)

Students create a practical guide explaining encryption and how to implement it effectively.

Instructions:

- Provide students with a template or guiding questions to structure their guides.
- The guide should cover the following sections:

Section 1: What is Encryption?

- Define encryption in simple terms.
- Explain why encryption is important for securing data online and offline.
- Provide real-world examples (e.g., securing bank transactions, emails, messaging apps).

Section 2: Types of Encryption

- Students will describe the different encryption methods they explored (Caesar, Atbash, Vigenère, Substitution) and briefly explain how each one works.
- They should discuss the advantages and disadvantages of each method, focusing on real-world relevance.
    - Caesar Cipher: Easy to understand but insecure by today's standards.
    - Atbash Cipher: Simple but too easy to break.
    - Vigenère Cipher: Stronger than Caesar, harder to crack with repeating patterns.
    - Substitution Cipher: Customisable, but predictable if patterns are spotted.

Section 3: Modern Encryption Methods

- Research and briefly explain modern encryption methods like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).
- Explain how these methods are used today to secure everything from bank transactions to emails.

Section 4: Best Practices for Encryption

- Practical advice for businesses and individuals:
    - Always use strong encryption (e.g., AES) for sensitive data.
    - Keep encryption keys secure (never share publicly).
    - Use encryption for both data at rest (files on a hard drive) and data in transit (emails, internet communications).
    - Regularly update encryption protocols to stay protected against evolving threats.

Section 5: Case Study

- Students will research a real-world example of encryption either succeeding or failing. Examples could include:
    - Success: WhatsApp encryption protecting messages.

    - Failure: Yahoo data breach (where encryption was insufficient or improperly applied).
- They should summarise what happened, how encryption was used (or misused), and what lessons can be learned.

Task:

- Students will work individually on their guides, using their notes and additional research to create a comprehensive, easy-to-understand guide.

Teacher's Role:

- Circulate and provide support where needed, especially when students are explaining modern encryption methods.
- Encourage students to be as clear and concise as possible while ensuring their guide is practical and useful for non-experts.

Plenary: Sharing Key Insights (10 mins)

Students share important points from their guides and reflect on their learning.

- Ask each student to share one key takeaway from their guide (e.g., an encryption method or best practice that surprised them).
- Discuss as a class:
    - "What encryption method do you think is the most important for protecting personal information?"
    - "How can we apply these encryption strategies in our everyday lives?"

Resources:

- Encryption Best Practices Guide template (digital or printed).
- Laptops or tablets for research and writing.
- Projector/whiteboard for sharing insights.

Assessment:

- Formative: Teacher observation of students' individual work during the guide creation process.
- Summative: Completed Encryption Best Practices Guides will be assessed based on:
    - Clarity of explanation.
    - Accuracy of encryption methods.
    - Practicality of the best practices recommended.

Digital Competence Framework (DCF) References:

Progression Step 3:

- 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 and security: "I can show an awareness of simple encryption and its purpose, e.g. to send sensitive data more securely."
- Advanced encryption techniques: "I can use appropriate advanced file management techniques, e.g. version history, restore previous version, tagging, compression."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
  - Year 9: Explain encryption strategies clearly in class discussions.
  - Year 10: Present findings on encryption use in a clear, concise format.
- Writing Skills:
  - Year 9: Use structured writing to create an encryption guide.
  - Year 10: Write organised and detailed reports with accurate information.

Timing Summary:

- Recap and Reflection: 10 mins
- Main Activity (Best Practices Guide): 40 mins
- Plenary: 10 mins
  Total: 60 mins

Lesson Plan: Week 6 (Part 1) – Malware Prevention and Response Guide

Lesson Title: Malware Outbreak Simulation – Defend the Network
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

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 in real-time.

Success Criteria:

- All: Identify different types of malware and explain their basic function.
- Most: Recognise malware activity and simulate a response plan for containing the attack.
- Some: Analyse the effectiveness of different malware prevention strategies and develop a rapid response protocol.

Starter: Malware Alert! (10 mins)

Introduce the challenge and get students ready for the simulation.

- Start by giving the class an urgent scenario:
  "The school network has been infected by malware! Your job is to stop the attack before it spreads and affects critical data."
- Briefly explain what malware is and the types that are likely involved in the outbreak. The focus will be on viruses, ransomware, and spyware.
- Introduce the Malware Outbreak Simulation:
  - The classroom will be transformed into a cybersecurity war room where students will play the role of cybersecurity specialists tasked with analysing and containing a malware attack.

Main Interactive Challenge: Malware Outbreak Simulation (40 mins)

Students work in groups to simulate the process of identifying and responding to a malware attack on a fictional network. They must take action, communicate effectively, and stop the attack before the time runs out.

The Setup:

- Split the class into two or three teams (depending on class size). Each team represents a cybersecurity team tasked with stopping the malware.
- Each team will have:
    - A malware scenario (ransomware, virus, spyware) to solve.
    - A series of clues and puzzles they need to decode to stop the malware.
    - A time limit (e.g., 30 minutes) to solve the challenge before the malware spreads and "locks" important files.

Challenge Flow:

1. Malware Infection Reports (5 mins):
    - Each team receives an alert about suspicious activity on the network.
    - They are provided with initial clues, such as strange email attachments, sudden file encryption, or unusual network traffic.
2. First Task – Identify the Malware (10 mins):
    - Teams must analyse the clues (provided by the teacher) to determine what type of malware they are dealing with.
    - This could involve fake email alerts, network logs showing suspicious activity, or even encrypted files (represented by locked folders on a USB drive or code puzzles).
3. Second Task – Contain the Attack (10 mins):
    - Once they identify the malware, teams need to develop and simulate a containment strategy.
    - For example, they might have to "disconnect" certain parts of the network (represented by sections of the classroom) to stop the spread of the virus or ransomware.
    - They also need to decide on what tools to use (e.g., antivirus software, backup systems) to protect other machines.
4. Final Task – Restore Systems and Analyse the Attack (15 mins):
    - Teams must now work on restoring files and fixing the damage done by the malware.
    - They can present how they would use backup systems or decryption tools to get systems back up and running.
    - Teams also prepare a report outlining:
        - How the malware attack happened.
        - What damage was caused.
        - What steps should be taken in the future to prevent such an attack?

Twists for More Excitement:

- Hidden Clues: Throughout the challenge, hide additional clues around the classroom that students need to find. These clues could contain encryption keys or instructions for how to stop the malware.
- Live Malware Activity: Randomly introduce new challenges throughout the simulation. For example:
    - Suddenly inform one group that the ransomware has spread to another system, and they need to react quickly.
    - Provide a clue that shows a "phishing email" was the source of the malware infection, and teams need to re-evaluate their containment strategy.
- Time Pressure: Add a countdown timer on the board. If the time runs out before they solve the challenge, the malware will “lock” more systems or "steal" important data.

Plenary: Malware Impact Reflection (10 mins)

Summarise key takeaways from the simulation and reflect on how real-world malware attacks unfold.

- Debrief: Discuss with the class:
    - “How did you identify the malware?”
    - “What was the most challenging part of containing the malware?”
    - “How would you improve your response strategy in a real situation?”
- Highlight the real-world importance of being prepared for malware attacks and knowing how to respond quickly to limit damage.

Resources:

- Printed clues, fake network logs, and email alerts that students need to analyse.
- USB drives or printed folders representing encrypted files.
- Fake encryption keys or decryption puzzles for them to solve.
- A countdown timer to simulate the urgency of stopping the malware.
- Props for the “cybersecurity war room,” like signs for “isolated systems” or “infected network sections.”

Assessment:

- Formative: Observation of teamwork, analysis of clues, and decision-making during the malware simulation.
- Summative: Final report detailing the malware type, damage caused, and prevention strategies.

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."

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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
  - Year 9: Present findings on how malware spreads and suggest response strategies.
  - Year 10: Lead a discussion on malware prevention and mitigation strategies during group presentations.
- Writing Skills:
  - Year 9: Produce a structured action plan outlining prevention and response strategies for malware attacks.
  - Year 10: Write a detailed analysis of a malware case study, assessing its impact and proposing solutions.

Timing Summary:

- Starter Activity: 10 mins
- Main Activity (Malware Simulation): 40 mins
- Plenary: 10 mins
  Total: 60 mins

Lesson Plan: Week 6 (Part 2) – Malware Prevention and Response Guide

Lesson Title: Creating a Malware Prevention and Response Guide
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can develop practical strategies for preventing malware infections.
- I can create a comprehensive guide that explains how to respond to malware attacks.
- I can evaluate different prevention and response techniques, using real-world case studies.

Success Criteria:

- All: Understand basic strategies to prevent malware infections and respond to them.
- Most: Create a detailed and well-organised guide that explains how to prevent and respond to malware attacks.
- Some: Analyse real-world malware attacks and evaluate the effectiveness of various response methods.

Recap and Reflection: Lessons from the Malware Simulation (10 mins)

Reflect on the key takeaways from the Malware Outbreak Simulation in the previous lesson and introduce the task for today.

- Recap the simulation: Ask students how they felt during the malware attack simulation in Part 1.
    - “What was the most challenging aspect of containing the malware?”
    - “What strategies worked best for stopping the attack?”
    - “What prevention strategies could have stopped the infection before it spread?”
- Connect to today’s task: Explain that today they will use their experience from the simulation to create a Malware Prevention and Response Guide. This guide will serve as a practical resource that could help individuals or companies protect their systems from malware attacks and know how to respond if infected.

Main Activity: Developing the Malware Prevention and Response Guide (40 mins)

Students work individually or in pairs to create a comprehensive guide outlining the steps needed to prevent and respond to malware attacks.

Section 1: What is Malware?

- Define malware and explain the different types (e.g., viruses, ransomware, spyware, trojans).
- Provide real-world examples from the simulation or famous malware attacks (e.g., WannaCry, NotPetya).

Section 2: How Does Malware Spread?

- Describe how malware infects systems (e.g., phishing emails, malicious websites, infected USB drives).
- Discuss the role of social engineering in spreading malware, referencing the tactics seen in the simulation.

Section 3: Malware Prevention Techniques

- Outline key prevention techniques such as:
    - Antivirus software: What it does and why it's important.
    - Regular updates: Keeping operating systems and software up to date to patch vulnerabilities.
    - Safe browsing habits: How to avoid suspicious links, downloads, and phishing emails.
    - Employee training: If aimed at a business, the importance of training staff to recognise potential malware attacks (especially phishing).
- Activity: Have students rank these strategies in order of importance and justify their reasoning in their guide.

Section 4: Responding to a Malware Attack

- Provide a step-by-step guide on how to respond to a malware infection, based on their experience from the simulation.
    - Isolating infected systems to stop the spread.
    - Running antivirus scans to detect and remove malware.
    - Using backups to restore data and mitigate the damage of ransomware.
    - Contacting cybersecurity professionals or law enforcement if necessary.
- Activity: Ask students to include a checklist in their guide for responding to malware, based on what they experienced during the simulation.

Section 5: Case Study

- Choose a real-world malware attack (such as WannaCry or Stuxnet) and briefly explain:
    - How the attack spread.
    - What damage it caused.
    - How it was eventually contained.
    - What prevention strategies could have stopped it before it caused damage.

Teacher's Role:

- Circulate during the activity, providing support where needed.
- Encourage students to think about practical solutions and ensure their guides are clear and easy to understand.

Optional Support:

- Provide templates or guiding questions to help students structure their guides, if necessary.

Plenary: Sharing Key Insights (10 mins)

Students reflect on their guides and share key strategies with the class.

- Have each student or pair present a key prevention strategy they included in their guide.
    - For example: "Why is antivirus software important?" or "How would you respond to a ransomware attack?"
- Wrap-Up:
    - Discuss as a class: "What can individuals and organisations do to ensure they stay safe from malware?"
    - Emphasise that prevention is the best protection, but being prepared to respond is also crucial.

Resources:

- Malware Prevention and Response Guide template (digital or printed).
- Laptops or tablets for research and writing.
- Case studies on famous malware attacks (e.g., articles on WannaCry, NotPetya, Stuxnet).

Assessment:

- Formative: Teacher observation of students' progress during the guide creation process.

- Summative: Completed Malware Prevention and Response Guides will be assessed based on:
    - Clarity of explanation.
    - Practicality of the prevention and response strategies outlined.
    - Depth of analysis in the case study section.

Digital Competence Framework (DCF) References:

Progression Step 3:

- 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:

- 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."

Literacy and Numeracy Framework (LNF) References:

- Oracy Skills:
    - Year 9: Explain key malware prevention and response strategies during group presentations.
    - Year 10: Present a comprehensive guide on how to protect systems from malware in a clear, concise format.
- Writing Skills:
    - Year 9: Write a structured guide outlining how to prevent and respond to malware attacks.
    - Year 10: Develop a detailed and well-organised guide with practical strategies for malware prevention and response.

Timing Summary:

- Recap and Reflection: 10 mins
- Main Activity (Guide Creation): 40 mins

- Plenary: 10 mins
  Total: 60 mins

Lesson Plan: Week 7 – Preventing and Identifying Social Engineering Attacks

Lesson Title: Advanced Strategies Against Social Engineering
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can explain the concept of social engineering and its psychological manipulation techniques.
- I can identify advanced tactics used in social engineering attacks (e.g., vishing, smishing).
- I can develop a comprehensive action plan to protect myself and others from social engineering threats.

Success Criteria:

- All: Describe advanced social engineering tactics and their implications.
- Most: Analyse how these tactics exploit psychological principles.
- Some: Create a detailed action plan with prevention strategies for different scenarios.

Starter Activity (10 mins):

Introduce advanced social engineering tactics.

- Present a scenario involving a vishing (voice phishing) attack and discuss what makes it effective.
- Ask students to brainstorm other forms of social engineering they may have encountered or heard about, such as smishing (SMS phishing).

Main Activity: Tactic Exploration (30 mins):

Dive deeper into various social engineering tactics.
Instructions:

- Divide the class into small groups and assign each group a specific tactic to research (e.g., vishing, smishing, baiting).
- Groups will:
    - Investigate how their assigned tactic works and the psychological principles behind it.
    - Prepare a short presentation or infographic summarising their findings.

Student Task:

- Present their findings to the class, highlighting key characteristics and real-world examples of their assigned tactic.

Teacher's Role:

- Facilitate research, providing resources and guidance.
- Encourage students to think critically about the effectiveness of these tactics.

Action Plan Development (15 mins):

Create a comprehensive action plan against social engineering attacks.

- Ask each group to develop an action plan that includes:
    - Warning signs to look for in their specific tactic.
    - Steps to take if they encounter such an attack.
    - Strategies for educating others about these tactics.

Plenary (5 mins):

Reflect on key learnings and action plans.

- Invite groups to share one key point from their action plan.
- Discuss the importance of vigilance and sharing knowledge to protect oneself and others.

Resources:

- Access to online articles and videos about social engineering tactics.
- Tools for creating infographics or presentations.

Assessment:

Formative: Teacher observation of group presentations and participation in developing action plans.

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."

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."

Timing Summary:

- Starter Activity: 10 mins
- Main Activity (Tactic Exploration): 30 mins
- Action Plan Development: 15 mins
- Plenary: 5 mins
  Total: 60 mins

Lesson Plan: Week 7 (Part 2) – Social Engineering Role Play and Response

Lesson Title: Responding to Social Engineering Scenarios
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

Learning Objectives:

- I can demonstrate effective responses to social engineering attacks through role play.
- I can evaluate the effectiveness of different response strategies in various scenarios.

Success Criteria:

- All: Act out responses to social engineering scenarios accurately.
- Most: Analyse the strengths and weaknesses of different response strategies.
- Some: Propose alternative responses based on situational analysis.

Recap of Previous Lesson (10 mins):

Review key concepts of social engineering.

- Briefly discuss the advanced tactics covered in the previous lesson.
- Ask students to share one new thing they learned about social engineering tactics.

Role Play Scenarios (30 mins):

Practise responding to social engineering attacks.
Instructions:

- Prepare several social engineering scenarios based on tactics like vishing, smishing, and pretexting.
- Divide students into small groups, and assign each group a scenario to act out. Each group will:
    - One student plays the role of the attacker.
    - Another plays the victim.
    - The rest act as observers who provide feedback.

Student Task:

- After each role play, groups discuss the effectiveness of the responses and suggest improvements.

Teacher's Role:

- Monitor the role plays, providing feedback and insights into the effectiveness of the responses.

Discussion and Reflection (15 mins):

Evaluate the effectiveness of response strategies.

- Facilitate a class discussion on the role plays.
- Ask questions like: "What worked well in your response?" and "What could be improved?"
- Discuss how different responses might change depending on the situation.

Plenary (5 mins):

Summarise key points learned from the role plays.

- Highlight the importance of practice in recognising and responding to social engineering threats.
- Encourage students to think about how they can apply these strategies in real life.

Resources:

- Scenario descriptions for role plays.
- Feedback forms for observers.

Assessment:

Formative: Teacher observation of participation in role plays and group discussions on response effectiveness.

Digital Competence Framework (DCF) References:

Progression Step 3:

- 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:

- 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."

Timing Summary:

- Recap: 10 mins
- Role Play Scenarios: 30 mins
- Discussion and Reflection: 15 mins
- Plenary: 5 mins
  Total: 60 mins

Lesson Plan: Week 8 – Cybersecurity Escape Room Challenge

Lesson Title: Cybersecurity Escape Room Challenge
Date: [Insert Date]
Duration: 1 hour
Class: Year 9/10

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.

Success Criteria:

- All: Apply basic cybersecurity knowledge to solve simple challenges collaboratively.
- Most: Work together to tackle intermediate cybersecurity problems using prior knowledge.
- Some: Analyse and resolve complex cybersecurity issues, demonstrating critical thinking and leadership during the challenge.

Introduction to the Escape Room (10 mins):

Set the stage for the challenge.

- Briefly explain the Escape Room concept and its relevance to cybersecurity.
- Discuss the importance of teamwork, communication, and applying learned concepts to real-world scenarios.
- Present the rules and objectives of the Escape Room challenge, emphasising time constraints and the collaborative nature of the activity.

Escape Room Challenge Setup (45 mins):

Engage students in solving cybersecurity challenges.
Instructions:

- Divide students into small teams (4-6 members each).
- Each team will rotate through different challenge stations, each designed to test their knowledge in a specific area:
    - Station 1: Identifying Malware – Analyse sample files and identify malware types.

    - Station 2: Securing a Network – Configure settings to secure a simulated network.
    - Station 3: Detecting Phishing – Review emails to spot phishing attempts.
    - Station 4: Social Engineering Scenarios – Role-play responses to various social engineering tactics.

Student Task:

- Teams will work collaboratively to complete each station, solving problems and answering questions.
- Each challenge will have a time limit, and teams must finish before the timer runs out to earn points.

Teacher's Role:

- Monitor each station, providing hints or guidance as needed.
- Ensure teams stay on track and maintain a collaborative spirit.

Reflection and Debrief (5 mins):

Reflect on performance and learnings.

- Gather students together to discuss their experiences during the challenge.
- Ask guiding questions such as:
    - "What strategies worked well for your team?"
    - "How did you overcome challenges together?"
    - "What concepts from previous lessons were most useful?"

Resources:

- Challenge station materials (sample malware files, network settings, phishing emails).
- Timers for each station.
- Reflection sheets for students to document their thoughts.

Assessment:

Formative: Teacher observation of team dynamics, problem-solving approaches, and participation during the challenge.

Digital Competence Framework (DCF) References:

- Progression Step 3 (Year 9): I can apply problem-solving skills to identify and address cybersecurity threats in a simulated environment.

- Progression Step 4 (Year 10): I can critically evaluate cybersecurity scenarios and develop strategies to resolve complex cyberattacks.
- Progression Step 3 (Year 9): I can work effectively as part of a team to solve problems and achieve a common goal in a digital environment.
- Progression Step 4 (Year 10): I can lead a team in solving complex cybersecurity challenges, ensuring all members contribute and collaborate effectively.

Timing Summary:

- Introduction: 10 mins
- Escape Room Challenge Setup: 45 mins
- Reflection and Debrief: 5 mins
  Total: 60 mins

Portfolio-Building Activity: Peer Assessment and Reflection

Task:
After completing the Escape Room Challenge, students will engage in peer assessment and reflection.

Peer Assessment (20 mins):

Evaluate teamwork and problem-solving skills.

- Students will exchange feedback forms with another team, assessing their collaboration and contributions during the challenge.
- Provide criteria for assessment, including communication, problem-solving skills, and overall teamwork.

Reflection (20 mins):

Reflect on the importance of cybersecurity in daily life.

- Each student will write a short reflection addressing:
    - The importance of cybersecurity.
    - How the skills learned will help them stay secure online.
    - Personal insights gained from the Escape Room experience.

Resources:

- Peer assessment forms.
- Reflection prompts to guide student writing.

Assessment:

Summative: Completed peer assessment forms and reflection pieces, focusing on the insights gained about teamwork and cybersecurity.

Timing Summary for Portfolio Activity:

- Peer Assessment: 20 mins
- Reflection: 20 mins
  Total: 40 mins