Context

The Internet is the world in which young people live. It is therefore important that we prepare them to use the Internet safely and to be able to protect themselves. Interest and aptitude for programming and technology is beneficial for the individual and for society as a whole. We need cyber professionals! However, it is of concern that a number of UK teenagers who would not otherwise be involved in traditional crime are becoming involved in cyber crime. The availability of off the shelf hacking tools and other openly advertised illegal products and many hacking and gaming forums where tips, guides and tutorials are commonplace, can make the line between what is legal and illegal seem unimportant.

In this lesson the experience of one teenager who crosses the line to crime is explored. The film which is the central resource of the delivery tells the story of Jack who was a whiz kid at computing. He enjoyed the challenges of games etc. but soon began to follow a pathway into crime. He first broke the law when he used a friend's password without permission. He began to steal, extort, threaten and hacked into his college IT system – causing mayhem. Jack is caught and receives a criminal conviction. He regrets his actions and the consequences he faces in his future life.

The story is based on a true life case of a young boy in Wales.

Links with PSE & Key Stage 3 Learning Outcomes

Skills → Developing Thinking
— Learners should be given opportunities to: use some prior knowledge to explain links between cause and effect and use a arrange of techniques for personal reflection

Skills → Developing Communication
— Learners should be given opportunities to: communicate confidently personal feelings and views through a range of appropriate methods

Skills → Developing ICT
— Learners should be given opportunities to: use ICT safely and responsibly following safe practices

Skills → Working with Others
— Learners should be given the opportunities to: Work both independently and cooperatively
— Empathise with others experiences, feeling and actions
— Access an appropriate range of sources for help, support and advice

Range → Active Citizenship
— Learners should be given opportunities to: develop respect for themselves and others
— To understand topical local and global issues

Range → Health and Emotional Wellbeing
— Develop positive attitudes towards themselves and others

Range → Moral and Spiritual Development
Learners should be given opportunities to:
— develop an insight into their values
— understand what they believe to be right and wrong, actions and the moral dilemmas in life situations

Range → Preparing for lifelong learning
Learners should be given opportunities to:
— understand their aptitudes and interests in order to make informed choices about learning and future studies

Links with Literacy and Numeracy
Year 7 Oracy across the curriculum
→ Developing and presenting information and ideas → Listening
— respond thoughtfully to others' ideas, asking pertinent questions

→ → Collaboration and Discussion
— make a range of contributions to discussions, e.g. leading, encouraging and supporting others

Links with the Digital Competence Framework
Year 7 Citizenship → identity, Image and Reputation
— Use strategies for guarding against identity theft and scams that try to access their private information online, e.g. safely manage browser history and cookies.

Year 9 Oracy across the curriculum **→ Developing and presenting information and ideas → Listening** — Consider the relevance and significance of information and ideas presented to them	**Year 7 Citizenship → Online behaviour and Cyberbullying** — Demonstrate a basic knowledge of the legal aspects linked to online behaviour, e.g. cyber bullying, harassment, false statement and publishing inappropriate content/images without consent. **Year 8 Citizenship → Health and Wellbeing** — Demonstrate healthy online behaviours (physical and psychological) and identify unacceptable behaviour, e.g. in relation to cyber stalking, harassment, abuse of trust and radicalisation. **Year 8 Citizenship → Online Behaviour and Cyberbullying** — Identify high risk situations and active strategies to avoid them, e.g. critically evaluate behaviour to limit exposure to high risk situations. — Critically evaluate the behaviours of other online and identify how they could be beneficial or damaging.
Links with United Nations Convention on the Rights of the Child (UNCRC) **Article 13:** The right to information **Article 16:** The right to privacy (family, home or correspondence); protection from unlawful attacks on his or her honour and reputation **Article 29:** The right to the development of the child's personality, talents and mental and physical abilities to their fullest potential	**Estyn Common Inspection Framework 2017** This resource supports schools to develop their approaches to Wellbeing and to Care, Support and Guidance.
The Law Computer Misuse Act (1990) Malicious Communications Act (1988)	A Glossary of Terms is provided. See Resource 9.

Learning Aims and Objectives	**We are learning:** — What cyber crime is — What the Law is in relation to cyber crime — How to use digital devices safely and responsibly — Why cyber crime is not a victimless crime — What future opportunities are open to young people with cyber skills — What to do when we need help
Intended Pupil Learning Outcomes	**Outcomes:** — I can explain what cyber crime is — I can identify the steps that could lead to criminal activity online — I know the Law relating to cyber crime — I understand that cyber crime is not a victimless crime — I am aware of the career opportunities that are open to me — I know who to go to for help
Resources	1. PowerPoint 2. Key words display cards 3. Definition of Cybercrime display card 4. *Don't Cross the Line to Cyber Crime* Film (schoolbeat.cymru/cyber-crime-film) 5. Jigsaw mat 5a. Jigsaw statement cards 6. Computer Misuse Act card (Teacher) 7. Consequences scenarios 8. Law information card (Teacher) 9. Glossary
Key Words	cyber crime cyber skills consequences victim
Definition	Cyber crime is committed when digital devices are used illegally against other people and systems

Lesson Outline

	Activity	Description	Timing
The lesson is designed to be 50 minutes long.	**Introduction**	Introductions. Introduce ground rules. Outline aims/objectives key words and learning outcomes	5 mins
	Assess previous knowledge and learning (Activity 1)	Capture pupils' knowledge of the subject/issue through questioning and knowledge finders Refer to previous lessons delivered by School Community Police Officers Ask pupils to tell you what they learnt	5 mins
	Activity 2	Don't Cross the Line to Cyber Crime Film	8 mins
	Activity 3	Jigsaw	12 mins
	Activity 4	Consequences scenarios	10 mins
	Activity 5	What are your cyber skills?	5 mins
	Review and assessment of learning	Summarise and assess pupil progress through peer discussion and questioning Review objectives and assess pupil outcomes	4 mins
	Reflection	Encourage learners to think and reflect upon their learning by completing the sentence "After today's lesson I now know …"	
	Help, support and further information	Teacher, Designated Safeguarding Person, (DSP) School Community Police Officer (SCPO) trusted adult www.schoolbeat.cymru, Action Fraud, Childline MEIC, Fearless (Crimestoppers), Child Exploitation and Online Protection (CEOP) www.ceop.police.uk	1 min

Lesson Plan

Introduction		
	Introduce yourself and tell the pupils why you are delivering the lesson. (See Context above) Remind pupils of the importance of respecting each other's' ideas and opinions and negotiate ground rules. Show the PowerPoint (Resource 1) to support the lesson delivery throughout. Share the aim and learning objectives with the group. Display and read the key words (Resource 2). Ask the pupils to tell you what they already know about the key words. Explain they will be learning about cyber crime by looking at a real life story. Tell them what they will learn (outcomes) by the end of the lesson.	5 mins

Activity 1	Assess previous knowledge and learning	
Knowledge finders	Tell the class they are going to find out about their use of digital devices. The aim of this activity is to quickly determine the learners' understanding of digital/cyber literacy and the Law. Ask the learners to indicate (hands up/thumbs up/green/red cards/stand up) to show if they agree or disagree with the following statements: • It's OK to share your password with close friends. • It's fun to guess someone else's password. • It's funny to post a status on my friend's social media account without them knowing. • The best part of gaming is modifying. • Some cyber crime is harmless. Comment on what the learners have shared and listen to their comments about the statements. This will give you an opportunity to assess pupil knowledge of the topic.	5 mins

Introduce the definition of cyber crime (Resource 3):

'Cyber crime is committed when digital devices are used illegally against other people and systems'

A copy of the definition can be displayed in the classroom.

Mention that the majority of the time online activities are fun and helpful, however, there are occasions when people can be misled and when misuse occurs. Sometimes, the Law is broken.

Teacher Information

The following bullet points provide a guide that may be useful in discussion

For example, Gaming is fun, exciting and challenging but the problems that can emerge are unwanted contact, booting, hacking, threats, addiction.

- Social media e.g. cyberbullying, pop-up advertisements, trolling, upsetting content, fraping
- Shopping e.g. fake websites, spending without permission, fraud
- Homework e.g. fake news, dodgy websites, unreliable sources
- Steaming/downloading e.g. viruses, malware, copyright laws

Activity 2		
Don't Cross the Line to Cyber Crime Film	Introduce the film. Tell the class that the film is the real life story of a boy who knew computers inside and out and who loved playing games and completing challenges. Ask the learners to follow the story carefully to see what happens to Jack. Show the film. (Resource 4: schoolbeat.cymru/cyber-crime-film)	8 mins

Activity 3	Jigsaw activity	
	After the film allow the learners time to think about what they have seen. Open up the discussion by asking what happened to Jack. Accept brief feedback and state that in the film Jack crossed the line to cyber crime. Explain that the following activity will help pupils find out what happened to Jack and when he crossed the line. Divide the class into small groups. Distribute an A3 copy of the jigsaw mat (Resource 5) and a set of jigsaw statement cards (Resource 5a) to each group. Tell the learners to look carefully at the questions posed on the jigsaw mat and to put the statements down on the correct jigsaw piece. Allow time for the learners to complete the activities.	12 mins
	Teacher Information Some statements may be placed in a more than one piece of the jigsaw. However, the statements about breaking the Law are not inter changeable. Jack broke the Law and started on the pathway to serious cyber crime when he used his friend's password without permission. 1. Jack was playing online games with his friends — (Who) 2. Jack committed cyber crime — (What) 3. Jack chose to use cheats to beat the system. It was all about cracking the code — (Choices) 4. Jack joined chat rooms where he learnt tricks from other like-minded people — (Choices) 5. Jack became addicted to online gaming — (Why) 6. Jack believed he would not be found out — (Why) 7. Jack used his friend's password to buy game ammunition — **(Law)** 8. While online, Jack stole his friend's gold — **(Law)** 9. Jack was hacking people's accounts and threatening them to demand money — **(Law)** 10. Jack disabled his school's website which caused mayhem! — **(Law)** 11. Jack was arrested and charged with cyber crime offences. He had lied, had no job and no career — (Consequence) 12. Jack was found guilty of cyber crime offences and given a suspended prison sentence and 150 hours of community service — (Consequence)	

Show the pupils PPT slide 14. Learners can check their answers.

In turn ask each group to discuss, **"When did Jack start to break the Law?"**

Take feedback from each group. It is possible that the learners will disagree but explain that the key point was when Jack used his friend's password to buy ammunition.

Pupils might be surprised to find that Jack crossed the line by using someone else's password. Explain that when he used the password without permission he broke the Computer Misuse Act, 1990.
(For further details of The Computer Misuse Act, 1990, Resource 6 has been provided for teachers.)

Discuss that playing games online is fun and you can learn useful skills such as coding.

Unfortunately, although Jack enjoyed playing games, he had become obsessed and his behaviour had changed. He had to beat the challenges and win *at all costs*, never mind the impact it had on other people.

Activity 4	Consequences scenarios	
	In this activity learners will explore the consequences for Jack and his victims.	10 mins
	Distribute one Scenario Card to each small group of learners. Ask the learners to answer the questions on the Scenario Cards (Resource 7). Teachers can refer to the Law Information Card provided for further detail and explanation (Resource 8).	
	Feedback to the whole class.	
	Point out that protecting yourself from cyber crime is important so that you do not become a victim.	
	Jack thought, 'No-one had a clue who I was', yet he was found out and the Police caught up with him and arrested him. He was found guilty and had to carry out community service.	
	The Law is there to help victims, protect people and keep them safe.	

Activity 5	What are your cyber skills?	
	The focus of this activity is to empower learners to make positive choices and to learn about possible career options. Ask the learners to tell their partner one cyber skill they have. Ask a few pupils to share the skill they told their partner with the whole class. Ask for a show of hands in response to the following questions, Who's good at coding? Who's good at gaming? Who's good at using apps to… create music, make films, create animations, games, puzzles, etc. Ask the class to name some jobs where they could use their cyber skills. Collect answers on the board. Use PowerPoint slide 20 to show how their skills can be used in industry and the services. Show the pupils that there are lots of well paid jobs for young people with cyber skills. There are also ways to begin to use cyber skills in a helpful way. The Cyber Security Challenge website has details of many competitions and learning programmes. The http://dvlacodechallenge.dvla.gov.uk develops coding skills and runs clubs etc.	5 mins

Teacher Information

The jobs revealed on the slide are some of the many available to those with cyber skills. The description for each job is as follows:

Ethical Hacker – £50,000
Someone who hacks into computer networks in order to test or evaluate their security, rather than with malicious or criminal intent.

Games Developer – £55,000
Develops and creates video games. Write code and develop software.

Forensic Investigator – £40,000
A person who investigates digital devices.

Data Miner – £35,000
Analyses data, which could then be used for a whole host of purposes including marketing, threat analysis etc.

Web Vulnerability Analyst – £30,000
Someone who works to identify vulnerabilities on web sites and improve security.

Cyber Crime Analyst – £35,000
Someone who conducts analysis/research in relation to cyber crimes to assist in investigations.

Info Security Manager – £70,000
Responsible for protecting the company/organisation's computers, networks and data against threats (i.e. security breaches, computer viruses or cyber-attacks).

Reflection	Review and assessment of learning	
	To close the lesson ask learners to reflect on what they have learnt. Ask them to think about what they knew about digital devices before the lesson began. Accept a few answers. Invite learners to complete the following sentence, "***After today's lesson I now know …***" Check that the learning outcomes have been achieved.	4 mins

Conclusion	Help and support	
	Finally, ensure that pupils know who they can go to for help if they feel they are losing control online or if they are victims of cyber crime. Remind them who is available to help in school. Teachers and the Designated Safeguarding Person (DSP), the School Community Police Officer, as well as help available online. If you are a victim and need help and support you can call MEIC or Childline. If you need to report a cyber crime or fraud you can call Action Fraud on 0800 123 2040	1 min
	Teacher Information In Wales, the Cyber Crime Prevent Team will also help. They are able to visit the young person and offer advice and diversionary activities in a National Crime Agency supported workshop. Referrals can be made to the team via your School Community Police Officer or DSP.	

Further follow up material for teachers and others is available on www.**SchoolBeat.cymru**