# EXPLORE BEING CYBERSECURE

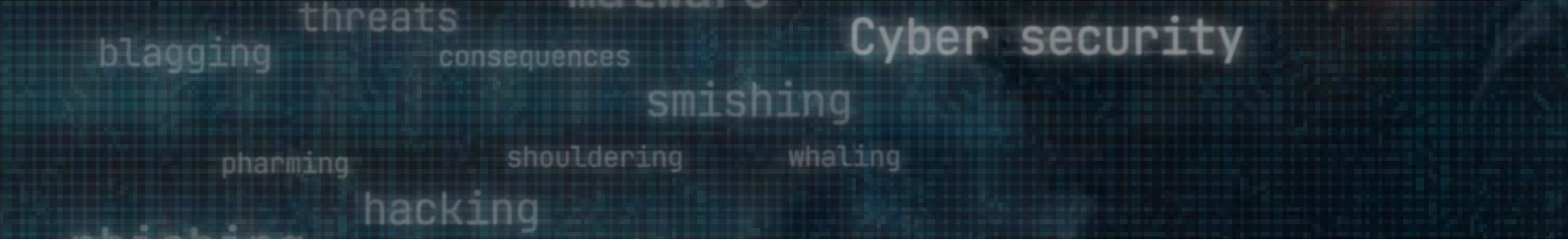
AGES 11-14

Information and guidance for practitioners

## ://CYBERFIRST.NAVIGATORS

How to stay secure online (11-14 year olds)

National Cyber Security Centre
a part of GCHQ




## Contents

## 1. What is cyber security and why is it important?

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage.

It's also about preventing unauthorised access to the vast amounts of personal information that is stored on these devices, and online.

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life.

From online banking and shopping, to email and social media, it's more important than ever that everyone is informed about the steps that can be taken to prevent cyber criminals getting hold of accounts, data, and devices.

## 2. What is CyberFirst Navigators?

This is a resource for teachers to be used with students aged 11-14. It focuses on developing knowledge, skills and online behaviours in children and young people, to help keep them cyber secure when they are online.

**This includes:**

- Using and managing passwords effectively
- Protecting devices and accounts
- Managing and reporting suspicious contact and content

## 3. Who are the National Cyber Security Centre (NCSC)?

The NCSC is part of GCHQ and helps to protect the country, individuals, businesses and other organisations against cyber threats.

We support the most critical organisations in the UK, the wider public sector, industry, small & medium size businesses as well as the general public. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

**More specifically, the NCSC:**

- understands cyber security, and distils this knowledge into practical guidance that we make available to all
- responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK
- uses industry and academic expertise to nurture the UK's cyber security capability
- reduces risks to the UK by securing public and private sector networks

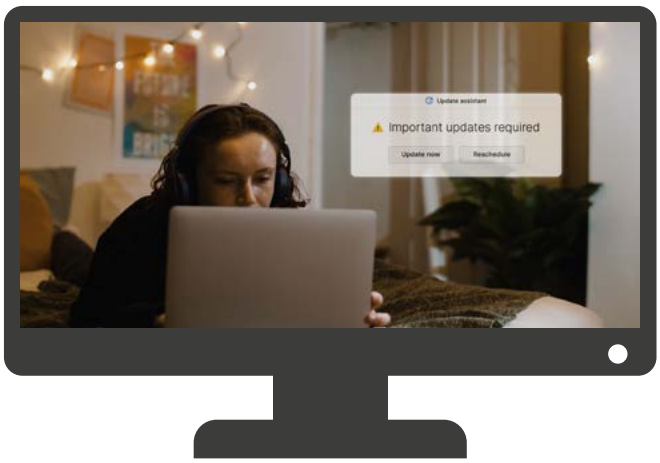

## 4. How to use this resource

This resource has been created to be used with students aged 11-14 and to support the PSHE education curriculum across three lessons (see curriculum mapping for all 4 nations).

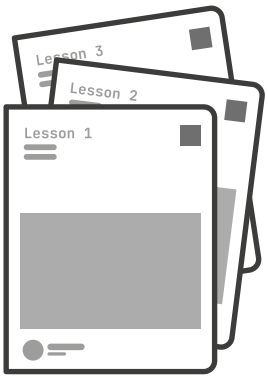
**It consists of:**

1. Factsheets for practitioners
2. The film, which is shown at the start of the first lesson
3. Three lesson plans for 11-14 year olds
4. A PowerPoint presentation for each lesson
5. Printable resources for each of the lessons


Factsheets




The Film




Lesson Plans


Printable Resources


PowerPoint Presentations

# 5. Learning outcomes

**The lessons cover the following themes:**

## Lesson 1 - Protecting personal information online

Students will learn about the risks to personal information online, and how to protect personal information

**Learning outcomes**

- I can identify a range of cyber security risks and threats
- I can explain how activities online might be subject to cyber threats
- I can demonstrate ways to protect personal information to reduce the risk of being hacked

## Lesson 2 - Managing devices and accounts

Students will learn how to keep accounts and devices safe, and what to do if security is breached

**Learning outcomes**

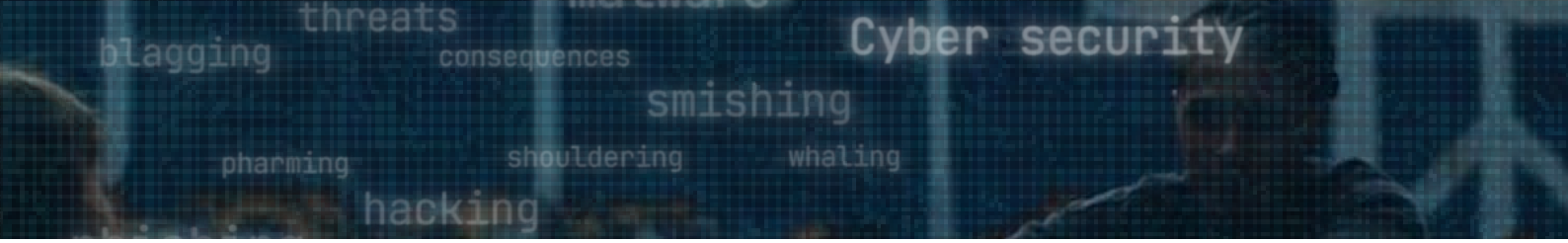
- I can demonstrate what a safe and secure password looks like and highlight why they are important to keep cyber secure
- I can explain the different ways to keep accounts and devices safe, and demonstrate the skills needed to do so
- I can identify how to recover an account and device

## Lesson 3 - Identifying scams and sources of support

Students will learn how to identify signs of online scams, where to report cyber security incidents and what happens when reporting

**Learning outcomes**

- I can identify signs of online scams and the measures needed to stay secure online
- I can explain a range of sources of support and reporting channels, when reporting account or device compromise
- I can offer advice about how to effectively respond to account or device compromise




## 6. Before you start

Familiarise yourself with the resources and the lesson plans before beginning to teach the topic. The resource covers sensitive topics and it's important that students have a safe space in which to explore the issues. The film explores issues around hacking, cyber threats and the loss of money. It is important to recognise that some students may have experienced these issues, or someone in their family may have.

**You will want to consider the following:**

- Talking with colleagues to advise that you are going to be covering this topic and identifying any potential issues beforehand
- Letting students know that you are going to be covering the topic beforehand
- Ensuring that you use distancing techniques e.g. using the characters in the film to help the conversation – what do they think? How are they feeling? What do you think happened to them?
- Ensuring that you give students the option of an 'exit pass' if they need to leave the lesson for any reason
- Ensuring that there is effective support in place – signposting support is included in each of the lessons, but will be most effective if it is tailored to your school and local area.

Also be aware that teaching in relation to the use of social media under the age of 13 (when students are allowed to sign up) should be done with caution. Whilst we know that young people under the age of 13 do use social media, it is important not to give the message that this is universal, and something that they are expected to do.

## 7. Ground rules

When discussing any PSHE topic, it is important to set ground rules so that all students feel comfortable in discussing the topics covered. It is recommended that you set up ground rules in collaboration with the students themselves, but you might have a pre-prepared set of expectations to save time.

**While you will already have classroom behaviour expectations in place, key rules to consider highlighting before these lessons include:**

- Showing respect and listening to others
- The use of language – making sure that it doesn't upset or offend anybody
- Asking students to explain their points, and if disagreeing with something, to comment on the argument not the person
- Making the point that the discussion in the classroom should stay in the classroom, unless the young person is at risk, in which case safeguarding procedures will be followed
- Including effective signposting, to reduce public disclosures. If a young person is worried about themselves or someone else make sure they know where to go for support after the lesson
- Encouraging students to ask for time out if they feel upset or worried at any point in the lesson

You can never be sure that a student or a member of their family has not experienced a cyber security incident, so it's important to not personalise the experience, e.g. avoid saying things like, 'How do you think you would feel in this situation?'. It's more appropriate to comment in third person by saying things like, "How do you think they feel?", or "How might someone feel?", so questions are directed at the situation rather than the individual.

In each of the session PowerPoint presentations, there is a 'ground rules' slide for you to add your own rules, or adapt the ones above.

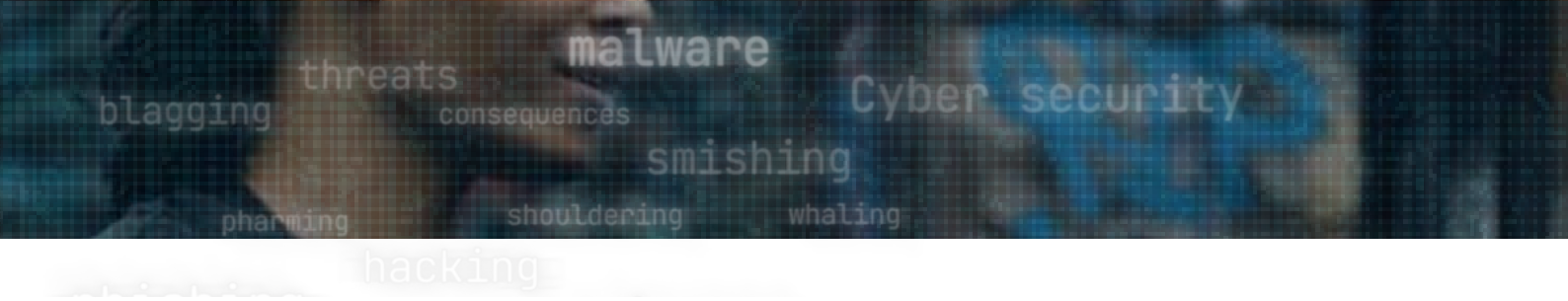
---

## 8. Victim blaming

There is the possibility that young people may express victim blaming attitudes towards some of the characters in the story. This may include statements like, 'they were stupid,' or, 'well what did they expect?'. It's important that these attitudes are challenged in a constructive way.

**You could challenge victim blaming attitudes in one of the following ways:**

- Focus on the unacceptable behaviour of people or organisations that try to hack into devices and steal someone's money or identity. These are criminals who are using malicious intent.
- Explore the impact on individuals who have been subjected to hacking/cyber crime.
- Ensure that young people feel empowered to report incidents and can support one another in managing incidents.
- Unpack victim blaming language – encourage young people to think about the impact that has on someone and highlight that the wrong person is being blamed for the incident.
- Increase empathy and understanding by discussing the reasons why someone may have engaged in the specific behaviour.




# 9. Safeguarding and managing questions and disclosures

Students may have questions about the content of the lessons, and it is useful to have strategies in place to manage this. A question box or 'ask-it basket' should be made available for students in each lesson, providing opportunities for students to ask anonymous questions. Ensuring anonymity encourages students to feel more confident in asking questions, and leaving time to answer questions until the following lesson allows you time to look through the questions and to conduct any necessary research before answering.

Always follow your own safeguarding policies and procedures whatever setting you are in, ensure that you are effectively equipped to manage any disclosures, and that young people know how to disclose safely if needed. There are details in the teachers factsheet about reporting any incidents of cyber crime.

## What do we mean by cyber security?

Cyber security, or online security, is how individuals reduce the risk of a hack (unauthorised access to accounts and devices). Its core function is to protect the devices we all use (smartphones, laptops, tablets, computers and IoT), and the services we access, from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

Smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email, social media and gaming, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices. This information or access in the wrong hands can lead to things such as social engineering, spear-phishing, scamming, and online impersonation.

## Cyber security measures to support online safety

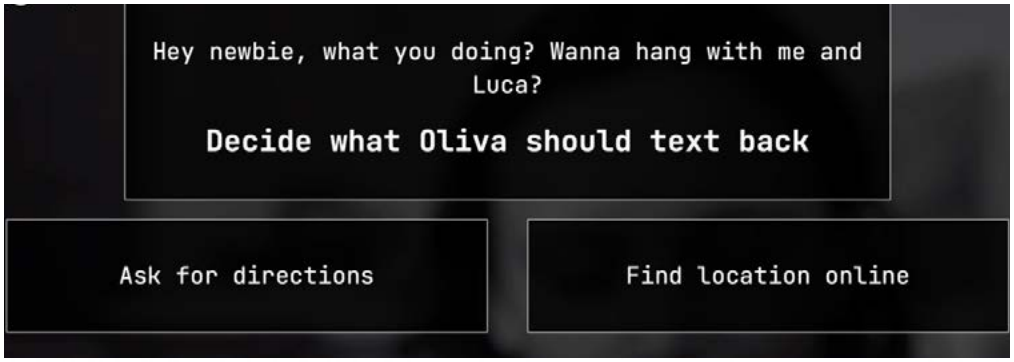
**The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:**

- **Content: being exposed to illegal, inappropriate, or harmful content, for example:** pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact: being subjected to harmful online interaction with other users, for example:** peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct: online behaviour that increases the likelihood of, or causes, harm, for example:** making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

## 10. Watching the film

The interactive film links to the three lesson plans and covers a range of topics related to cyber security. The first lesson includes some time for students to watch the film and consider what happens to the characters. Its three characters, Raheem, Olivia and Luca, are teenagers who experience a range of challenges and are trying to deal with their everyday lives online.

The film is interactive with a range of pop up questions that require responses from the audience. Ideally, this could be used as a whole class teaching tool. The film can be paused and rewound and depending on the answers given there are different pathways through the film so it can be referred back to.




### The plot

The film starts with Olivia who has just moved to the area. She has met a couple of boys and the three of them are friends. They are engaging in life online by playing games, communicating using their devices, and looking at merchandise to buy online. Luca's account gets compromised in the film, which means that the others in the story get messages encouraging them to purchase some headphones. Olivia buys the headphones and her account is hacked. She loses money as a result and has to manage the consequences of this incident.

## 11. Feedback

**Please help us continue to make these resources the best they can be by filling in our feedback form:**

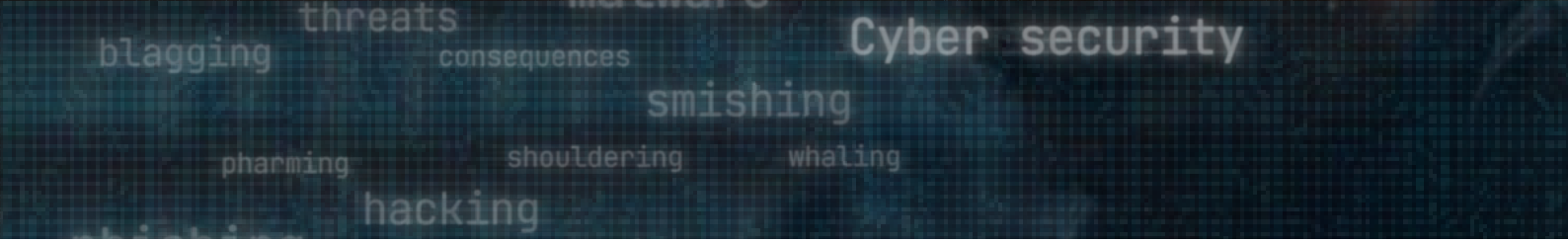
**https://forms.office.com/e/dissCBqkyx**

**There is also an opportunity for students to let us know what they think, we would really value their feedback:**

**https://forms.office.com/e/rCmCWkzN8m**

We would really appreciate you encouraging them to fill this in (no personal data is collected). It is best filled in after the film has been watched and the three lessons completed.

**We thank you for your time.**




# 12. Curriculum Mapping

## England

**Key age ranges:**

- The materials are intended to be used with pupils in year groups 7 to 9, or the age ranges of 11 to 14.
- The resources are designed to support the PSHE curriculum, and link to the following outcomes from the PSHE Association Programme of Study:

**Health and wellbeing:**

- H30. how to identify risk and manage personal safety in increasingly independent situations, including online
- H31. ways of assessing and reducing risk in relation to health, wellbeing and personal safety

**Relationships:**

- R17. strategies to identify and reduce risk from people online that they do not already know; when and how to access help

**Living in the Wider World:**

- L19. to recognise financial exploitation in different contexts e.g. drug and money mules, online scams
- L25. to make informed decisions about whether different media and digital content are appropriate to view and develop the skills to act on them
- L27. to respond appropriately when things go wrong online, including confidently accessing support, reporting to authorities and platforms

**PSHE education**

- Relationships Education, Relationships and Sex Education and Health Education statutory guidance (DfE, 2019).

## Scotland

These resources support the year groups S1 & S2. They align to the Scottish curriculum through Digital Literacy under the curriculum organiser of Cyber Resilience and Internet safety at second level and third level.

Second level Cyber resilience and internet safety: I can explore online communities demonstrating an understanding of responsible digital behaviour and I'm aware of how to keep myself safe and secure.

**TCH 2-03a**

Third level Cyber resilience and internet safety: I can keep myself safe and secure in online environments and I am aware of the importance and consequences of doing this for myself and others.

**TCH 3-03a**

## Wales

**Key age ranges:**
11-14 year olds (Progression Step 4)

**How do these resources support learning outcomes?**

These resources support schools embed digital competence across all areas of learning and support learning through the Health and Well-being area of learning and experience.

Digital competence is the set of skills, knowledge and attitudes that enable the confident, creative and critical use of technologies and systems. Now more than ever, learners need to be adaptable to change, capable of learning new skills throughout life and equipped to cope with new life scenarios.

The resources can be used alongside the Digital Competence Framework (DCF) to support the planning and progression of these skills. The DCF brings together the skills that will help learners thrive in an increasingly digital world, including how to stay safe online and understanding the importance of balancing game and screen time with other parts of their lives.

Learning through the Health and Well-being area of learning and experience provides a holistic structure for understanding health and well-being, developing the capacity of learners to navigate life's opportunities and challenges. Learning in this area is fundamental to developing safe behaviour in relation to digital media and the online world.

These resources relate to the following statements of what matters:

- Our decision-making impacts on the quality of our lives and the lives of others.
- How we engage with social influences shapes who we are and affects our health and well-being.
- Healthy relationships are fundamental to our well-being.

Guidance on how learners should progress within each statement of what matters as they journey through the continuum of learning is provided within the descriptions of learning.

## Northern Ireland

**Key age ranges:** Key Stage 3: 11-14 year olds Supports aspects of Using ICT, which is one of the three Cross-Curricular Skills at the heart of the curriculum. Also supports aspects of the Learning for Life and Work curriculum, under the area of Personal Development.

**How does CyberFirst Navigators support learning outcomes:**

- The Levels of Progression for Using ICT at Key Stage 3 include this statement: 'Pupils should demonstrate, when and where appropriate, knowledge and understanding of e-safety including acceptable online behaviour.'
- Schools should embed e-safety education into teaching and learning in the Areas of Learning through relevant topics. This will give pupils opportunities to develop their knowledge and understanding of e-safety
- Learning for Life and Work is a compulsory Area of Learning at Key Stage 3. It has four subject strands: Employability, Local and Global Citizenship, Personal Development, and Home Economics.

**The Statutory Requirements for Personal Development at Key Stage 3 state that pupils should have the opportunities to:**

- Develop strategies to promote personal safety, for example, developing safe practice in relation to the internet, understanding and managing risk, the place of rules and boundaries etc.

## UKCIS Education for a Connected World

Education for a Connected World is a tool for anyone who works with children and young people. It enables the development of teaching and learning as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world.

The framework aims to support and broaden the provision of online safety education, so that it is empowering, builds resilience and effects positive culture change. The objectives promote the development of safe and appropriate long term behaviours, and support educators in shaping the culture within their setting and beyond.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf

CyberFirst Navigators maps to aspect 7. Privacy and security

- I can explain why someone should use a strong and separate password for their email account, as the gateway to other online accounts.
- I understand the benefits of two factor authentication and use it where available.
- I can explain why backing up data is important and how this can be done.
- I know that accessing some websites or services may increase the risk of encountering viruses and other types of malware.
- I can explain why it's important to know how to recover a device or account if it gets compromised / hacked.
- I know who people can report to if they have experienced a cyber problem (e.g. identity theft, ransomware).

Cyber First

## Information for parents and carers

Below is a set of information that you might want to share with parents/carers:

**You can find more at:**
**www.ncsc.gov.uk/section/information-for/individuals-families**

**We also have resources for 7-11-year-olds.**
**See: www.ncsc.gov.uk/cybersprinters**

# HOW TO STAY SECURE ONLINE

National Cyber Security Centre
a part of GCHQ