



Anti-Fraud Education

Teacher Guidance



QUALITY
ASSURED
RESOURCE
PSHE ASSOCIATION

Context

This guidance accompanies the Cifas fraud prevention series of lessons. The lessons raise awareness of the risks associated with fraud and cybercrime, to ensure young people have the skills to protect themselves and are aware of the consequences of over sharing their personal information and/or engaging in fraudulent activity. Please read and consider this guidance first, before delivering the lessons. This suite of six lessons is divided into two lessons for key stage 3, two lessons for key stage 4, one lesson for key stage 5 and one lesson for pupils with SEND in key stages 3-4.

Preparing to Teach

These lessons should be taught within the context of a planned series of lessons on economic wellbeing, risk management or online safety. The 2025 DfE [statutory guidance for Relationships Education, Relationships and Sex Education and Health Education](#), states that students should learn about:

- 'Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online.' (Online safety and awareness, point 2)
- 'That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion.' (Online safety and awareness, point 14)

It is important that young people can identify instances of fraud, and that they understand the consequences of both becoming a victim of, and participating in, fraudulent activity. Students should be equipped with the skills and habits to protect themselves, their identity and their online information from potential fraud risks. These lessons may also provide PSHE teachers with opportunities to collaborate with their Citizenship and Maths colleagues who may be delivering elements of personal finance education in their curricula.



Why Fraud Prevention Education?

Cifas is the UK's leading fraud prevention service, driving forward the fight against fraud by sharing data, intelligence and learning. For over 35 years, the not-for-profit, member-led organisation has worked to protect hundreds of businesses, charities, public bodies and individuals from fraud and financial crime. Fraud and cybercrime are the fastest growing crimes in the UK. Cifas' National Fraud Database filed over 444,000 cases¹ of fraud in 2025 – this is an unprecedented number of cases, highlighting that fraud shows little sign of abating, as it now accounts for 45% of all crime.

Almost all young people aged 13-18 (96%) buy things online² and UK Finance found that almost half of 18-24-year-olds had been targeted in an impersonation scam, of which half had gone on to provide personal information or send money³. Cifas also reports that nearly 1 in 5 (18%) of money laundering cases involve Under-21s⁴.

Moreover, research conducted by Cifas suggests that young people do not always identify acts such as lying on a CV, using their parents' details to get cheaper car insurance or taking out mobile phone insurance after breaking their phone as 'fraudulent conduct'. Rather, they see these types of behaviours as excusable, victimless and commonplace⁵. This means young people are not only more likely to become victims of fraud, but also to unknowingly engage in fraudulent activities themselves. They therefore need to be equipped with the understanding and skills to recognise fraud, protect their personal data, understand the consequences of being involved in fraud, and to seek help if they have experienced fraud.

¹ Cifas, *Fraudscape*, 2026

² Parent Zone, 'A problem hiding in plain sight', November 2023

³ UK Finance, 'Gen Z more likely to be tricked by criminals and fall for impersonation scams' 2023

⁴ Cifas, *Fraudscape*, 2026

⁵ Cifas, *Is it okay to commit fraud?*, 2024

Using the SEND Lesson Plan

The specific lesson plan for students with SEND is designed for those with Moderate Learning Disabilities, additional learning needs and those on the autism spectrum, for use in special education settings, or for specific groups in mainstream schools. It is intended to be used flexibly, and you are encouraged to adapt it to meet your students' needs and abilities. The SEND lesson plan provides four main activities for you to choose from, which are based on four progression stages outlined in the [PSHE Association's Planning Framework for Pupils with SEND](#):

CORE:
Fundamental learning elements

DEVELOPMENT:
Increasing understanding of learning

ENRICHMENT:
Deepening of application of learning

ENHANCEMENT:
Applying learning in different contexts

The learning outcomes begin at the 'Core' stage, as students working at 'Encountering' or 'Foundation' stage are likely to be taught through sensory experiences and interactions. For students working at these first stages, please refer to the Planning Framework for Pupils with SEND and [Enhancing PSHE for pupils with SEND](#).

In the lesson plan, each progression stage builds on the one before, and each has its own learning outcome and activity. The timings given are for guidance and can be adapted as required. All students should complete the introduction, baseline assessment, signposting support and endpoint assessment, and you should select the relevant main activity depending on the progression stage of each student or group.

Creating a Safe Learning Environment

A safe learning environment helps students feel comfortable with sharing their ideas, values and attitudes without attracting negative feedback, and will help you manage discussions on sensitive issues confidently. It is good practice to:

1. Work with students to establish ground rules about how they will behave in discussion, such as:
 - everyone has the right to be heard and respected
 - we will use language that won't offend or upset other people
 - we will use the correct terms, and if we don't know them, we'll ask the teacher
 - we will comment on what was said, not the person who said it
 - we won't share our own, or our friends', personal experiences
 - we won't put anyone on the spot, and we have the right to pass
 - we won't judge or make assumptions about anyone.
2. Offer opportunities for students to discuss issues in small groups as well as sharing views with the class.
3. Make boxes available in which students can place questions with or without their name on, to avoid having to voice them in front of the class.
4. Provide balanced information and differing views to help students clarify their own opinions.
5. Be sensitive to the needs and experiences of individuals, as some students may have direct experience of some of the issues.
6. Distance the learning from students to discourage personal disclosures in the classroom and to keep the learning environment safe.
7. Always work within the school's policies on safeguarding and confidentiality.
8. Link PSHE education into the whole school approach to supporting student welfare.
9. Make students aware of sources of support, both inside and outside the school.

Further guidance on creating a safe learning environment is available from the [PSHE Association](#).

Developing Understanding of Fraud

When discussing PSHE issues, it is essential to be clear about the precise and accurate use of language to avoid misconceptions. Fraud prevention education is likely to cover specialist language and terms that are unfamiliar to students. We recommend using the key terms and definitions below:

Key Term	Definition
Cybercrime	A type of crime that is committed using information technologies such as a computer, a networked device or a network, either as the target or the tool for the crime.
Firewall	A network security system designed to prevent unauthorised access to or from a network.
Fraud	Illegal deception intended for financial or personal reward.
Identity Fraud	Identity fraud is when a fraudster uses someone else's identity (or creates a fake identity) to access a product or service, so they don't have to pay for it themselves.
Malware	Software which is specifically designed to disrupt or damage a computer system.
Money Laundering	The process of transferring money earned through criminal activity from one account to another, in order to make it seem legal. Laundering the proceeds of crime is a criminal offence under The Proceeds of Crime Act (2002).
Money Mule	A person who (intentionally or unintentionally) transfers money acquired illegally, usually through their own bank account, on behalf of others. Note: this phrase is not used in student-facing materials due to victim-blaming connotations for victims of financial exploitation. The materials use the term 'money laundering' and explain that people can be complicit or exploited to launder money.

Key Term	Definition
Social Engineering	A method of manipulating people to reveal personal information about themselves or to persuade them to do something they would not otherwise do.
Phishing	Social engineering technique: An attempt to gain personal information (or persuade someone to do something) using email communications. A more sophisticated and targeted version of this is sometimes referred to as 'Spear Phishing'.
Smishing	Social engineering technique: An attempt to gain personal information (or persuade someone to do something) using text messages, often implanted into pre-existing conversations with known contacts.
Vishing	Social engineering technique: An attempt to gain personal information (or persuade someone to do something) over the phone.
Quishing	Using a fake or tampered QR code to direct someone to a fraudulent website designed to steal information or prompting malware downloads.
Target*	Throughout these lessons, we have chosen to use the word 'target' rather than 'victim', as the word victim can imply associations of vulnerability, blame or powerlessness.

*Challenging victim blaming

Be vigilant to any potential victim blaming expressed by students during feedback on lesson activities. 'Victim blaming' happens when a target of crime is held partially or fully responsible for it happening to them. This might be expressed explicitly, by stating it was the person's fault; or implicitly, for example, questioning what they could or should have done differently. It can have a significant impact on students with related vulnerabilities and can prevent those affected seeking support.

Research shows that children and young people internalise the 'buyer beware' principle, often blaming themselves when they are scammed or defrauded⁶. Follow the key learning provided in these lessons to reinforce that someone affected by the harms that are explored is not at fault.

If some students use victim-blaming language, this should be challenged in a constructive and supportive way; encouraging the students to consider the impact this language can have on others and empathising with the character.

Keep in mind those with vulnerabilities and the likelihood that some pupils may have had direct experience of these harms, recognising the profound impact this can have, even when the money involved is relatively small. Consider ways to best support them, for example by providing the opportunity to opt out of some or all of the lesson using an 'exit-pass', if it is upsetting for them.

⁶ Parent Zone, 'A problem hiding in plain sight', November 2023

Examples of Fraud

For many topics in PSHE, examples can bring learning to life and students may have questions about how fraud occurs in practice. Therefore, we have provided some real-life examples of the various types of fraud 'in action' for teacher reference.

Fraud or Scam	Definition	Example
False Application	When an application for a product or service is made with deliberately deceptive information, often using false supporting documents.	Sarah applies for a car finance contract, but she lies about her income and her address history to get the contract.
Misuse of Facility	The fraudulent misuse of an account, policy or product – for example, allowing criminal funds to pass through your bank account or paying in an altered cheque.	Mandy takes out a mobile phone contract but purposely doesn't pay the monthly payments. Fred has a bank account, and he allows an acquaintance to pay money into his account, without knowing for certain where the funds were coming from. Fred then transfers the money into another account and keeps a small sum for himself as payment.
Identity Fraud	When a fraudster abuses personal data to impersonate an innocent party, or creates a fictitious identity, to open a new account or product.	Leah uses Claire's personal details and address to fraudulently apply for a credit card. Sandra creates a fictitious name and a false passport in that name to apply for new bank account.
Facility Takeover	When a fraudster abuses personal data to hijack an existing account or product, e.g. a bank account or phone contract.	Sean impersonates Sophie and accesses her shopping account. Sean changes the password and address details and orders products using Sophie's bank details.

Fraud or Scam	Definition	Example
Asset Conversion	The unlawful sale of an asset subject to a credit agreement, e.g. a car bought on finance and sold on before it has been paid off.	Simon gets a car on finance but sells it to an unsuspecting buyer and disappears with the money. The buyer then has the car taken back by the car company as they still own it, and Simon had no right to sell the car.
False Insurance Claims	When an insurance claim, or supporting documents, contains deliberately deceptive information.	Dan and his friends purposely crash their car into another car and then make multiple claims to the insurance company.
Insider Threat	Fraud or theft committed against an organisation by an employee of the company or an individual applying to work for the company.	Amber accesses company data and sends it to a third party in return for a financial reward. Wayne applied for a job but lied about his qualifications and previous employment history on his job application and interview.

Consequences of Committing Fraud

PSHE education can also teach young people to understand the consequences of their actions. In the case of fraud prevention education, allow students to consider both the consequences of committing a fraudulent act and of being a target of fraud.

For the Target	For the Perpetrator
• It can cause a great deal of emotional turmoil. • It can be very stressful and take a lot of time to rectify what has happened. • It can cause lasting reputational damage for a person who has been a target of fraud. • If money is taken from a person's bank account, it can be very difficult to get it all (or any of it) back.	• May get a criminal record. • Bank account may be frozen or closed. • In severe cases, can lead to imprisonment. • Markers will be placed on a person's credit details so that banks and other financial organisations know their history of fraudulent conduct. • A previous fraud conviction can mean a person is unable to get a bank account, to take out loans or mobile phone contracts. • It may also result in the person's job opportunities being drastically limited. • Those people that recruit others into fraudulent acts (such as money laundering) are often also involved in organised crime, which can lead to violence from gangs, extortion or being drawn into more serious crime.

Signposting Support

Ensure students know where they can seek help and further advice, both now and in the future, if they are concerned about data protection or fraud. Teachers wanting further guidance on the issue of fraud and cybercrime can visit:

- www.cifas.org.uk
- www.reportfraud.police.uk
- www.takefive-stopfraud.org.uk
- www.victimsupport.org.uk
- www.nscs.gov.uk
- www.dontbefooled.org.uk
- www.stopthinkfraud.campaign.gov.uk

For more information, lesson plans and online training focused on online financial harms, see the PSHE Association website: www.pshe-association.org.uk/online-financial-harms

Appendix: Curriculum Links

PSHE Association Programme of study	DfE statutory Relationship Education, Relationships and Sex Education and Health Education guidance (2025)
KS3 Online life 10. how to recognise online scams to extort money or information in different contexts; the impact of online scams on individuals and society; ways to protect personal information and finances online Personal safety, risk and influence 7. how to recognise signs that they or others may be being drawn into criminal behaviour (e.g. county lines drug running, money laundering, cybercrime); how to access appropriate support	Online safety and awareness: 1. Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online. 2. Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues. 3. The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online.
KS4 Online life 13. strategies to critically assess bias, reliability and accuracy in online content, including how to analyse and fact check content produced by generative AI Online harms 9. risks and warning signs of online scams, including sextortion, and the harm they can cause; the importance of seeking help swiftly, how to report and who to tell if scammed or involved in sextortion	14. That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion.

KS5

Careers education: aspirations, learning and work

5. how to identify and evidence their strengths and skills when applying and interviewing for future roles and opportunities, recognising that there are different recruitment and selection processes in different industries

7. how to maintain their online presence to maximise career opportunities and mitigate potential reputational risks

9. what is meant by, and the importance of, professional conduct; about workplace cultures and expectations in different industries and organisations; to understand and appreciate the importance of workplace policies and protocols, including health and safety, confidentiality, cyber-security and data protection

SEND

CORE:

- Recognise that not everything we see or read online is trustworthy; that some things that are written about are not real and are fake, edited, or are exaggerated. (The world I live in 2)

- Identify some things online that might seem 'too good to be true' (e.g. competitions, offers, fake websites or adverts). (The world I live in 2)

DEVELOPMENT:

- Identify things that we should never share online without checking with a trusted adult first. (Self-care, support and safety 4)

- Recognise that there are online scams (ways that people may try to trick us online); identify what some of these ways of deceiving people might be (e.g. phishing, fake email addresses). (The world I live in 2)

ENRICHMENT:

- Describe specific ways of keeping ourselves safe online (e.g. secure passwords, never giving out personal details or passwords, covering our computer's camera when not in use). (Self-care, support and safety 6)

- Describe some ways that we might be able to spot that something is a scam, and how we could report a scam if experienced. (The world I live in 2)

ENHANCEMENT:

- Explain what the effects of online scams might be for individuals, and how we could protect ourselves from scams (e.g. through our online behaviours and privacy settings). (The world I live in 2)

- Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond. (Self-care, support and safety 4)

Being safe:

3. How to determine whether other children, adults or sources of information are trustworthy, how to judge when a relationship is unsafe (and recognise this in the relationships of others); how to seek help or advice, including reporting concerns about others, if needed.

Wellbeing online:

3. How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.