



# CIFAS ANTI-FRAUD EDUCATION: TEACHER GUIDANCE

This guidance has been written to accompany the Cifas fraud prevention series of four lessons. The lessons aim to 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. Teachers should read and consider this guidance first, before delivering the lessons. This suite of four lessons is divided into two lessons for key stage 3 and two lessons for key stage 4 and have been designed in line with the key principles of effective prevention education.

[www.pshe-association.org.uk/curriculum-and-resources/key-principles-effective-prevention-education](http://www.pshe-association.org.uk/curriculum-and-resources/key-principles-effective-prevention-education)

---

## Preparing to teach

---

**These lessons should be taught within the context of a planned series of lessons looking at issues around economic wellbeing, risk management or online safety. It is important that young people are able to identify instances of fraud, and that they understand the consequences of both becoming a victim of, and participating in, fraudulent activity. Young people should be equipped with the skills and habits to protect themselves, their identity and their online information from potential fraudulent 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 curricular.**

### Why fraud prevention education?

Cifas is the UK's fraud prevention service. We lead the fight against fraud by sharing data, intelligence and learning. For over 30 years we have worked to protect businesses, charities, public bodies and individuals from financial crime. Fraud and cyber crime are the fastest growing crimes in the UK, accounting for one in every two crimes committed. Victims of fraud are also becoming younger, with fraudsters targeting under 21 year olds; an age group which saw 2788 individuals recorded to the Cifas National Fraud Database as victims of fraud in 2021<sup>[1]</sup>. 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 commonplace<sup>[2]</sup>. This means young people are not only more likely to become victims of fraud, but also to unknowingly engage in fraudulent conduct themselves. They therefore need to be equipped with the skills to recognise fraudulent conduct, to protect their personal data and to seek help in the case of becoming a victim of fraud.

### Links to PSHE Association Programme of Study

Each of the three core themes of the PSHE programme of study contains suggested learning opportunities which provide the context through which students can develop knowledge, essential skills and attributes. The learning opportunities should be used flexibly according to student's development, readiness and needs, and taking account of prior learning, experience and understanding. The table below shows the learning opportunities from the relevant PSHE education core themes at KS3 and KS4 which are met by these lessons. Learning should always take place within a spiral programme of knowledge, skills and attribute development, where prior learning is revisited, reinforced and extended in age- and stage-appropriate contexts.

---

<sup>1</sup> Cifas Strategic Intelligence Assessment March 2022

<sup>2</sup> Qualitative research with 16-19 year olds, March 2016, Cifas & Britain Thinks

	<b>PSHE Association Programme of Study</b>	<b>DfE statutory Relationships, Sex and Health Education</b>
<b>Key Stage 3</b>	<p>R42. to recognise peer influence and to develop strategies for managing it, including online</p> <p>L15. to assess and manage risk in relation to financial decisions that young people might make</p> <p>L17. to manage emotions in relation to money</p> <p>L18. to evaluate social and moral dilemmas about the use of money, including the influence of advertising and peers on financial decisions</p> <p>L19. to recognise financial exploitation in different contexts e.g. drug and money mules, online scams</p> <p>L21. to establish personal values and clear boundaries around aspects of life that they want to remain private; strategies to safely manage personal information and images online, including on social media</p> <p>L27. to respond appropriately when things go wrong online, including confidently accessing support, reporting to authorities and platform</p>	<p><b>Relationships and Sex Education: Online Media</b></p> <ul style="list-style-type: none"> <li>• about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.</li> <li>• not to provide material to others that they would not want shared further and not to share personal material which is sent to them.</li> <li>• what to do and where to get support to report material or manage issues online.</li> <li>• how information and data is generated, collected, shared and used online.</li> </ul> <p><b>Health Education: Internet safety and harms</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>Key stage 4</b>	<p>R38. factors which contribute to young people becoming involved in serious organised crime, including cybercrime</p> <p>L17. how to effectively make financial decisions, including recognising the opportunities and challenges involved in taking financial risks</p> <p>L18. to recognise and manage the range of influences on their financial decisions</p> <p>L20. the skills to challenge or seek support for financial exploitation in different contexts including online</p> <p>L25. how personal data is generated, collected and shared, including by individuals, and the consequences of this</p>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

## 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 teachers to manage discussions on sensitive issues confidently. It is good practice for teachers to:

- |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Work with students to establish ground rules about how they will behave in discussion, such as:               <ul style="list-style-type: none"> <li>- everyone has the right to be heard and respected;</li> <li>- we will use language that won't offend or upset other people;</li> <li>- we will use the correct terms, and if we don't know them, we'll ask the teacher;</li> <li>- we will comment on what was said, not the person who said it;</li> <li>- we won't share our own, or our friends', personal experiences;</li> <li>- we won't put anyone on the spot and we have a right to pass, and;</li> <li>- We won't judge or make assumptions about anyone.</li> </ul> </li> <li>• Offer opportunities for students to discuss issues in small groups as well as sharing views with the class</li> <li>• Make boxes available in which students can place anonymous questions or concerns, to avoid having to voice them in front of the class</li> </ul> | <ul style="list-style-type: none"> <li>• Provide balanced information and differing views to help students clarify their own opinions</li> <li>• Be sensitive to the needs and experiences of individuals – some students may have direct experience of some of the issues</li> <li>• Distance the learning from students to discourage personal disclosures in the classroom and to keep the learning environment safe</li> <li>• Always work within the school's policies on safeguarding and confidentiality</li> <li>• Link PSHE education into the whole school approach to supporting student welfare</li> <li>• Make students aware of sources of support, both inside and outside the school</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Further guidance on creating a safe learning environment is available from the PSHE Association.

## Developing fraud understanding

### Notes on terminology

When discussing PSHE issues, it is essential to be clear about the precise and accurate use of language in order to avoid misconceptions. In particular, fraud prevention education is likely to cover specialist language and terms that are unfamiliar to students. To support teachers in their accuracy and clarity, we recommend using the key terms and definitions below:

KEY TERM	DEFINITION
<b>Cyber crime</b>	A type of crime that is committed using information technologies such as a computer and a network
<b>Firewall</b>	A network security system designed to prevent unauthorized access to or from a network
<b>Fraud</b>	Illegal deception intended for financial or personal reward
<b>Identity fraud</b>	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
<b>Malware</b>	Software which is specifically designed to disrupt or damage a computer system
<b>Money laundering</b>	The process of transferring money earned through criminal activity from one account to another in order to make it seem legal
<b>Money mule</b>	A person who (intentionally or unintentionally) transfers money acquired illegally, usually through their own bank account, on behalf of others
<b>Social engineering</b>	A method of manipulating people to reveal personal information about themselves or to persuade them to do something they would not otherwise do
<b>Phishing</b>	<i>Social engineering technique:</i> An attempt to gain personal information (or persuade someone to do something) through the use of email communications. A more sophisticated and targeted version of this is sometimes referred to as 'Spear Phishing'
<b>Smishing</b>	<i>Social engineering technique:</i> An attempt to gain personal information (or persuade someone to do something) through the use of text messages, often implanted into pre-existing conversations with known contacts
<b>Vishing</b>	<i>Social engineering technique:</i> An attempt to gain personal information (or persuade someone to do something) over the phone
<b>Target</b>	Throughout these lessons, we have chosen to use the word 'target' rather than the word 'victim' as the word victim can imply associations of vulnerability, blame or powerlessness.

## Examples of fraud

For many topics in PSHE, examples can bring learning to life and students are likely to have lots of 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 throughout these lessons.

FRAUD OR SCAM	DEFINITION	EXAMPLE
<b>False Application</b>	When an application for a product or service is made with material falsehoods, often using false supporting documents.	<i>Sarah applies for a mortgage but she lies about her income and her address history in order to obtain the mortgage.</i>
<b>Misuse of Facility</b>	The fraudulent misuse of an account, policy or product – for example, allowing criminal funds to pass through your account or paying in an altered cheque.	<i>Mandy takes out a mobile phone contract but purposely doesn't pay the monthly payments. Fred has a bank account and he allows a fraudster to pay money obtained from fraud into his account. Fred then transfers the money into another account, keeps a small sum for himself as payment.</i>
<b>Identity Fraud</b>	When a fraudster abuses personal data to impersonate an innocent party, or creates a fictitious identity, to open a new account or product	<i>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.</i>
<b>Facility Takeover</b>	When a fraudster abuses personal data to hijack an existing account or product, e.g. a bank account or phone contract.	<i>Sean impersonates Sophie and is able to access her retail account, Sean changes the password and address details and orders products using Sophie's account.</i>
<b>Asset Conversion</b>	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.	<i>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.</i>
<b>False Insurance Claims</b>	False insurance claims occur when an insurance claim, or supporting documentation, contains material falsehoods.	<i>Dan and his associates purposely crash their car into another car and then make multiple claims to the insurance company.</i>
<b>Internal Fraud</b>	Fraud or theft committed by an employee of the company or an individual applying to work for a company.	<i>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.</i>

## Consequences of committing fraud

A key area of learning in PSHE is to enable young people to develop an understanding of the consequences of their actions. In the case of fraud prevention education, it is important to allow young people to consider both the consequences of committing a fraudulent act and of being a target of fraud. Below are some of the likely consequences in each case:

FOR THE VICTIM	FOR THE PERPETRATOR
<ul style="list-style-type: none"> <li>• It can cause a great deal of emotional turmoil</li> <li>• It can be very stressful and take a lot of time to rectify what has happened</li> <li>• It can cause lasting reputational damage for a person who has been a target of fraud</li> <li>• If money is taken from a person's bank account, it can be very difficult to get it all (or any of it) back</li> </ul>	<ul style="list-style-type: none"> <li>• May get a criminal record</li> <li>• In severe cases can lead to imprisonment</li> <li>• Markers will be placed on a person's credit details so that banks and other financial organisations know their history of fraudulent conduct</li> <li>• A previous fraud conviction can mean a person is unable to get a bank account, to take out loans or mobile phone contracts</li> <li>• It may also result in the person's job opportunities being drastically limited</li> <li>• Those people that recruit others into fraudulent acts (such as money muling) are often also involved in organised crime, which can lead to violence from gangs, extortion or being drawn into more serious crime</li> </ul>

## Signposting support

It is important to ensure that 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 wishing to seek further guidance on the issue of fraud and cybercrime can visit:

[www.cifas.org.uk](http://www.cifas.org.uk)

[www.takefive-stopfraud.org.uk](http://www.takefive-stopfraud.org.uk)

[www.cyberaware.gov.uk](http://www.cyberaware.gov.uk)

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

[www.victimsupport.org.uk](http://www.victimsupport.org.uk)

[www.barclayslifeskills.com](http://www.barclayslifeskills.com)

[www.moneymules.co.uk](http://www.moneymules.co.uk)

[www.nscs.gov.uk](http://www.nscs.gov.uk)

Teachers can also find more guidance for teaching aspects of online safety from:

[www.gov.uk/government/publications/teaching-online-safety-in-schools](http://www.gov.uk/government/publications/teaching-online-safety-in-schools)

[www.gov.uk/government/publications/education-for-a-connected-world](http://www.gov.uk/government/publications/education-for-a-connected-world)