PSHE Association Quality Assured Resource

Cyber Detectives

Teacher Guidance

Year 5/6
Key Stage: 2

LLOYDS BANKING GROUP

CITY OF LONDON POLICE

This guidance has been written to accompany the City of London Police and Lloyds Banking Group fraud prevention series of two lessons. The lessons raise awareness of online fraud and its associated risks, ensuring that pupils have the skills to stay safe online and protect their personal information. Please read and consider this guidance first, before delivering the lessons. The two lessons are both aimed at upper Key Stage 2 pupils in Years 5 and 6 and could be taught consecutively or at different times within a planned Personal, Social, Health and Economic education programme.

Preparing to teach

Why teach about fraud prevention in the primary phase?

The City of London Police and Lloyds Banking Group are working to protect businesses, organisations and individuals from the threat of cybercrime and online fraud. Victims of fraud are becoming younger, and children can be particularly vulnerable, especially when using platforms or sites which are designed for use by older children (e.g. on social media or age-rated gaming). It is therefore important that children learn how to identify fraudulent activity, protect their personal data and report concerns if they are worried about anything they have seen or experienced online. Helping pupils to understand how to protect themselves from online fraud e.g. keeping data safe, and being aware of trustworthy and untrustworthy sources online can support and reinforce other online safety work.

Links to the PSHE Association Programme of Study

These lessons should be taught within the context of a planned series of lessons which explore either economic wellbeing, digital literacy or online safety. It is important that pupils in upper Key Stage 2 are able to identify examples of online fraud and that they understand that there are risks in different contexts. Pupils should be equipped with strategies to help protect themselves, including their identity and personal information, from potential online fraud.

The table below shows the learning opportunities from the relevant core themes of the PSHE Association Programme of Study[1] at KS2 which are met by these lessons. It also highlights where elements from the statutory guidance for Relationships Education and Health Education[2] are met through the lesson content. Learning should always take place within a spiral programme of knowledge, skills and attribute development, where prior learning is revisited, reinforced and extended in developmentally-appropriate contexts.

1 https://www.pshe-association.org.uk/curriculum-and-resources/resources/programme-study-pshe-education-key-stages-1%E2%80%935

2 https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

Programme of Study Core theme	Learning Opportunity from Programme of Study	Department for Education statutory guidance
Relationships	**R23:** about why someone may behave differently online, including pretending to be someone they are not; strategies for recognising risks, harmful content and contact; how to report concerns	**Relationships Education** **Online relationships** • the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them • how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met • how information and data is shared and used online **Health Education** **Internet safety and harms** • how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private • why social media, some computer games and online gaming, for example, are age restricted
Health and Wellbeing	**H37:** reasons for following and complying with regulations and restrictions (including age restrictions); how they promote personal safety and wellbeing with reference to social media, television programmes, films, games and online gaming **H42:** about the importance of keeping personal information private; strategies for keeping safe online, including how to manage requests for personal information or images of themselves and others; what to do if frightened or worried by something seen or read online and how to report concerns, inappropriate content and contact	
Living in the Wider World	**L11:** recognise ways in which the internet and social media can be used both positively and negatively **L12:** how to assess the reliability of sources of information online; and how to make safe, reliable choices from search results **L22:** about risks associated with money (e.g. money can be won, lost or stolen) and ways of keeping money safe	

Creating a safe learning environment

A safe learning environment helps pupils feel comfortable with sharing their ideas, values and opinions without attracting negative feedback, and will help teachers to manage sensitive issues confidently. It is good practice for teachers to:

- work with pupils 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 a right to pass.
  - We won't judge or make assumptions about anyone
- offer opportunities for pupils to discuss issues in small groups as well as sharing views with the class
- make boxes available in which pupils can place anonymous questions or concerns, to avoid having to voice them in front of the class
- be sensitive to the needs and experiences of individuals – some pupils may have direct experience of some of the issues covered
- distance the learning from pupils to discourage personal disclosures in the classroom and to keep the learning environment safe
- always work within the school's policies on safeguarding and confidentiality
- link PSHE education into the whole school approach to supporting pupil welfare
- make pupils 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 (www.pshe-association.org.uk).

Developing subject knowledge

Notes on terminology

Fraud prevention education is likely to include some specialist language and terms that pupils may be unfamiliar with prior to these lessons. To support you in establishing the accurate use of language, we recommend using the key terms below:

Key term	Definitions used in the lesson plan
Fraud	Deliberately deceiving someone, or doing something that is designed to take someone's private information or money without their permission
Personal information	Information about an individual to identify them e.g. name, address, date of birth, phone number/email address, school/workplace, bank account details, account information
Identity fraud	Using someone else's personal information to access a product or service so they don't have to pay for it themselves
Hacking	When someone tries to get into another person's computer by using harmful software such as a virus or by guessing passwords. This can be used to take personal information without permission. For example, name, address, bank details
Scam email	Attempting to gain personal information or persuade someone to do something through the use of email
Pop-up fraud	Fraudulent messages that 'pop up' when users are online. If clicked viruses can be installed or the computer hacked
Pharming	Users are directed to a fraudulent website without their knowledge to steal personal information and/or money
Geo-tagging	A way to track the location of a photo online. This is done by attaching coordinates to the photo, so it can be found on a map

Signposting support

It is important to ensure that pupils know where they can seek help and further advice, both now and in the future, if they are concerned about online fraud or any aspect of online safety. Remind pupils that they can always share concerns with their parents or with trusted adults at school, such as their teacher. Pupils can also seek support from Childline: www.childline.org.uk / 0800 1111 – for general advice about concerns.

Further support for teachers:

For further guidance on the issue of online fraud, teachers can visit:

www.cityoflondon.police.uk
Advice and information about online fraud and cybercrime

www.lloydsbank.com
Information about online fraud and advice on how to stop it

www.actionfraud.police.uk
Information about fraud prevention and how to report fraud

www.victimsupport.org.uk
Help and support for people affected by crime

www.cifas.org.uk
Not-for-profit membership association for fraud prevention

Information and guidance for parents and carers

Schools may want to support their parent community to discuss the issue of online fraud with their children at home. This information and guidance will not only help parents and carers to stay informed about how online fraud could affect their child, but also provide practical tips and advice on helping them to keep safe.

How online fraud can happen to children

Victims of fraud are becoming younger, and children can be particularly vulnerable. Young people are growing up in a digitalised world; the rise of technology such as social media and online gaming mean that fraud prevention education has never been more important. Although sharing their lives online can be the norm for many, this puts young people at risk of online fraud – for example, fraudsters can gain access to personal information and use this to sign up for new accounts, products or services in their name. Ways to target young people are constantly evolving and online fraud is on the increase for this age group. Staying up to date with the latest trends can be challenging, but it can help to protect young people from being targeted.

Talking to your child about staying safe online

It is really beneficial to talk to your child about their internet use and helping to keep themselves safe. Maintaining an open dialogue will enable your child to come to you with any issues or worries they might have, including about online fraud. The following questions may be helpful to provide insight into their habits and internet use:

- What are your favourite websites and online games?
- What's the best way to stay as safe as possible online?
- What is safe to share online and what isn't?
- How can we keep our personal information safe?

Agreeing on privacy settings and parental controls can improve your child's safety online, as well as ensuring they know how to block and report users or content. Finally, remind your child that if they are worried they have come across anything suspicious, or that online fraud has happened, they should tell you or another trusted adult as soon as possible.

Gaming and online fraud

If your child spends time online playing games, helping them to stay safe including complying with age restrictions can prevent online fraud occurring. Lots of games have communication features so that players can talk to each other but this can put young people at risk of complying with requests for their personal information. Often this feature can be turned off, and players can block other users if they feel unsafe or uncomfortable.

Age ratings: Most games will have an age rating depending on their theme and content. PEGI provides an age rating for individual games so that you can make decisions about which games are suitable for your child. The PEGI age ratings are 3, 7, 12, 16 and 18.

Social media and sharing photos

Social media platforms can be ways for young people and adults to stay connected with family and friends, and find new ways to express themselves. However, there are risks when using social media to communicate. Posts, profile information or photos could expose personal information and put them at risk. Sharing photos of children is common among parents, but once a photo is online it can be hard to control who it is seen by and how it's used. There may be information or visual clues in photos such as names, location (via geo-tagging), age, school etc. which could be used to exploit young people, or make them more vulnerable to crimes such as online fraud. Furthermore, any photos shared online add to the child's digital footprint and so it's important to seek children's permission as they get older before sharing. Internet Matters provide information for parents about protecting children when sharing images of them online as well as guidance on social media age restrictions, with the most common being 13 years old and upwards.

How to get help and report concerns

If you suspect that either you or your child has been a victim of online fraud, the organisations below can provide information and support:

www.actionfraud.police.uk

www.getsafeonline.org

www.citizensadvice.org.uk

www.victimsupport.org.uk

Further advice

www.cifas.org.uk

www.actionfraud.police.uk

www.cyberaware.gov.uk

www.lloydsbank.com

www.met.police.uk / www.cityoflondon.police.uk

Cyber Detectives

LLOYDS BANKING GROUP

CITY OF LONDON POLICE