

Don't Share Personal Information Online

40 minutes

Cyber Safety

WHAT THIS LESSON DOES

In this lesson, you'll explore why sharing personal information online can be risky. Learn about identity theft, cyberbullying, unwanted contact from strangers, and phishing scams, and discover practical steps to protect yourself and stay safe online.

WHAT STUDENTS SHOULD BE ABLE TO DO

- Understand what constitutes personal information and the potential risks associated with sharing it online.
- Identify and comprehend the various risks of sharing personal information online, including identity theft, cyberbullying, unwanted contact from strangers, and phishing scams.
- Recognize the implications of identity theft and how sharing personal information online can lead to such a situation.
- Understand the concept of cyberbullying and how sharing personal information online can make one more vulnerable to it.
- Learn how to avoid unwanted contact from strangers by being cautious about sharing personal information online.
- Understand what phishing scams are and how they can be avoided by not sharing personal information online.

BEFORE THE LESSON

- Open the lesson and test each interactive in turn: the activity, the drag and drop, and the chat simulator all need to load and respond before you rely on them.
- Devices ready, one per pupil or per pair. This lesson is on-screen throughout with no printed element.
- Have your own short example of personal information versus safe-to-share information ready, so you can model the difference before pupils sort their own.

Don't Share Personal Information Online

HOW THE LESSON RUNS

Understanding Personal Information
Risks of Sharing Personal Information
Identity Theft
Activity
Cyberbullying
Drag and Drop
Avoiding Unwanted Contact from Strangers
Chat Simulator
Beware of Phishing Scams
Conclusion

TEACHING MOVES

- 1. Understanding Personal Information. Build the list of personal information with the class rather than reading it out. Ask what a stranger could do if they knew each item, so the category means something before you name the risks.
- 2. Risks of Sharing Personal Information. Preview the four risks as headings only. Tell pupils each one gets its own section, so they know this is a map, not the detail, and do not switch off.
- 3. Identity Theft. Keep this concrete. Someone pretending to be you to open an account or buy things in your name. Anchor it in the personal information list from step 1.
- 4. Activity. Let pupils attempt the activity before you intervene. Circulate and check the confusion is about the content, not the interface, before you explain.
- 5. Cyberbullying. Draw the link explicitly: sharing your school or location gives a bully more to use. Keep the focus on the information angle, not bullying in general.
- 6. Drag and Drop. Model one card first, thinking aloud about why it goes where it does. Then let pupils sort the rest and check answers against a partner.
- 7. Avoiding Unwanted Contact from Strangers. Name the everyday places this happens: gaming platforms, forums, social media. Ask what a posted photo can reveal about where someone is right now.
- 8. Chat Simulator. Set the frame before pupils start: they are deciding what is safe to reply. Afterwards, ask what each choice would have told the stranger.
- 9. Beware of Phishing Scams. Show pupils the tell: an unexpected message pushing them to click or share quickly. Practise the safe habit of stopping rather than reacting.
- 10. Conclusion. Ask the class to name the four risks and one safe action for each from memory before revealing the summary. Use it to check what landed.

WHAT TO WATCH FOR

- Pupils think personal information only means obviously private things like a bank number, and do not count their school name, a photo showing where they are, or their date of birth. Point at each item from step 1 and ask what a stranger could work out from it. The photo and school name are usually the ones they underestimate.
- Pupils believe a message or website is safe simply because it looks official or uses a familiar logo. Use the phishing section to show that looking real is exactly the trick. Teach the rule that an unexpected message asking you to act fast is the warning sign, not the logo.
- Pupils think privacy risks only apply to strangers, not to people they chat with online in games. In the chat simulator, remind them they often do not truly know who is on the other side. Judge the safety of the reply, not the friendliness of the message.

DIFFERENTIATION

- Emerging: Sit with them for the drag and drop and sort the first two cards together, talking through why each belongs where it does. Give a shorter question: for any piece of information, ask only 'safe to share or keep private?' before adding the risk names.
- Developing: Have them explain their chat simulator choices back to you or a partner, saying why each reply is safe or unsafe. Ask them to add one more example to each risk category that the lesson did not mention.
- Proficient: Ask them to write or say a short warning they would give a younger child about one of the four risks, in their own words. Challenge them to spot which single piece of personal information appears across the most risks, and explain why.