

Why We Shouldn't Share Personal Information Online

40 minutes

Cyber Safety

WHAT STUDENTS SHOULD BE ABLE TO DO

- Identify types of personal information and recognise the importance of keeping it private.
- Understand key online risks associated with sharing personal information, including identity theft, cyberbullying, unwanted contact, and phishing scams.
- Apply safety strategies such as STOP, THINK, CHECK and BLOCK, REPORT, TELL to protect against online threats.
- Evaluate scenarios involving strangers or suspicious requests and select appropriate safe responses.
- Develop a cautious attitude towards online interactions to prioritise personal safety and seek help when needed.

BEFORE THE LESSON

- Open and test the lesson on the projector, then click through the drag-and-drop sort and the chat simulator yourself so you know how they behave before pupils reach them.
- Devices per pupil or per pair, with the interactive activities loading correctly on your school network in case a filter blocks them.
- Decide in advance how you will handle a pupil who says they have already met cyberbullying or a suspicious message. Know your school's own reporting route so you can name the trusted adults here.

Why We Shouldn't Share Personal Information Online

HOW THE LESSON RUNS

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

TEACHING MOVES

- 1. Understanding Personal Information. Build the list of personal information from the pupils rather than reading it out. Ask what a stranger could do with each item they name, then land the test: if sharing it could help someone find, contact or recognise you, it is private.
- 2. Risks of Sharing Personal Information. Anchor the whole lesson on one line: if you would not tell a stranger in real life, do not tell them online. Stress that things spread fast and are hard to take back.
- 3. Identity Theft. Keep this concrete with the name-tag-and-keys image. Explain that thieves collect small details over time, so no single fact feels risky on its own. That is why we keep the whole picture private.
- 4. Scenario Activity. Let pupils choose before you reveal the feedback, then pause on wrong choices and ask why that response was tempting. The reasoning matters more than the right button.
- 5. Cyberbullying. State plainly that cyberbullying is never the target's fault and that hiding behind a fake name does not make it anonymous to adults who can help. Model don't reply, keep it, tell someone.
- 6. Avoiding Unwanted Contact from Strangers. Warn pupils that unwanted contact often starts friendly: a shared game, a simple hi. Introduce BLOCK REPORT TELL here as the response, not just a slogan to remember.
- 7. Interactive Activity. Before pupils drag, ask them to say aloud whether each card helps someone find, contact or recognise them. Circulate on any card where a table splits, and use disagreement as discussion.
- 8. Beware of Phishing Scams. Teach the tell: phishing rushes you. Point out CLICK NOW and account-will-be-deleted urgency, and that a real logo does not make a message real. The safe move is to slow down and check with an adult.
- 9. Chat Simulator. Play one exchange together on the board first so pupils see how a request can be dressed up as friendly, then let them try it. Ask what the sender was really after.
- 10. Conclusion. Recap the four risks and pair each with its response. Close on the big message: feeling unsure is itself a reason to stop and ask a trusted adult, and doing so is never overreacting.

WHAT TO WATCH FOR

- Pupils think small details are harmless on their own, so a first name, a school or a favourite game feels safe to share. Show how separate details add up. During the sort activity, take two safe-looking cards and ask what a stranger could work out from both together.
- Pupils believe a friendly stranger who shares their interests is not really a stranger. Return to the lesson's line: strangers online are still strangers even when they seem friendly. Point out that a claimed shared interest is a common way in.
- Pupils assume a message must be real if it carries a familiar logo or looks official. Use the phishing step to separate looks from proof. Ask what the message wants them to do and how quickly, and teach checking with an adult before clicking.

DIFFERENTIATION

- Emerging: Pair the pupil with a partner for the drag-and-drop sort and let them talk each card through before dropping it. Give one simple test to lean on for every decision: could this help someone find, contact or recognise me?
- Developing: Have the pupil explain back why one card is private and one is safe, so they are reasoning rather than guessing. Let them attempt the chat simulator once with support, then a second time on their own.
- Proficient: Ask them to write or say a safe reply to the chat simulator's stranger and justify it using BLOCK REPORT TELL. Challenge them to spot which detail in a scenario was the trap and explain what the sender was really after.