

Sharp Alert Secure Kind Brave

Be
Internet
Legends.

Teacher guide to pupil safety

Please make sure you read this guide before carrying out any activities with pupils.

Ages

Years 3 and 4 (ages 7-9)
Years 5 and 6 (ages 9-11)

Summary

- Reinforce existing ground rules that have been drawn up with the class.
- Add or emphasise any that are especially relevant to this lesson, e.g. no personal stories, the right to pass.
- Make sure you're familiar with the school's safeguarding policy.
- Consider any sensitivities and your prior knowledge about specific pupils' circumstances. It may be advisable to let relevant staff know that you're covering this subject.
- Local and national support groups or helplines such as the Child Exploitation and Online Protection Command (CEOP), NSPCC, and Childline should be signposted to pupils – as well as adults within school who can support them if they have worries or concerns.
- Invite pupils to write down any questions they have anonymously at any time, and collect them using an 'ask it basket', question box or envelope. This should be accessible both in, during and after the lesson.

Please see individual plans at the back of the booklet on pages 51-74 for information on differentiation and support for pupils.

[g.co/BeInternetLegends](https://www.g.co/BeInternetLegends)

Welcome

Welcome to the Be Internet Legends Scheme of Work, developed by Google in partnership with the educators and online safety experts at Parent Zone. This resource is part of Be Internet Legends, a multifaceted programme designed to teach children the skills they need to be safe and confident online.

The Be Internet Legends programme gives teachers the tools and methods they need to teach online safety fundamentals in the classroom. Inside this booklet you'll find a full set of lesson plans. Two have been written for the younger children in your school (years 3 and 4: ages 7-9), while the rest were created for older children (years 5 and 6: ages 9-11). These plans provide fun, age-appropriate learning experiences around four internet safety pillars:

- **Think Before You Share (Be Internet Sharp)**
- **Check it's For Real (Be Internet Alert)**
- **Protect Your Stuff (Be Internet Secure)**
- **Respect Each Other (Be Internet Kind)**

The fifth pillar brings everything together. It provides interesting and valuable follow-up discussions to have in class or during a regular safeguarding discussion.

- **When in Doubt, Discuss (Be Internet Brave)**

The lessons also feature Interland, a playful browser-based game that makes learning about online safety interactive and fun – just like the internet itself. Using Interland and the complementary programme, teachers can choose the activities that best suit pupils, working through the lessons to ensure their progress. The lessons have been designed to allow you to choose when to deliver the learning, but remember the activities shouldn't be repeated.

At the back of the booklet are two additional resources. Teachers can photocopy these and give them to students to take home and use with their parents (the Be Internet Legends pledge, and the Be Internet Legends certificate). For additional resources from Google, visit [g.co/BeInternetLegends](https://www.google.co.uk/BeInternetLegends)

This scheme of work was developed in partnership with Parent Zone. Parent Zone supports families and schools by creating expert information on all of the issues affecting children and young people that are caused or amplified by the internet.

Table of Contents

Think Before You Share	7
Activity 1: Is it OK to share?	
Activity 2: Whose profile is this, anyway?	
Activity 3: How do others see us?	
Activity 4: Keeping it private	
Activity 5: Interland: Mindful Mountain	
Check it's For Real	16
Activity 1: Don't bite that phishing hook!	
Activity 2: Who are you, really?	
Activity 3: Interland: Reality River	
Protect Your Stuff	29
Activity 1: How to build a strong password	
Activity 2: Shh... Keep it to yourself!	
Activity 3: Taking care of yourself and others	
Activity 4: Interland: Tower of Treasure	
Respect Each Other	39
Activity 1: How can I stand up to others online?	
Activity 2: Turning negative into positive	
Activity 3: Mixed messages	
Activity 4: Reacting to role models	
Activity 5: Interland: Kind Kingdom	
When in Doubt, Discuss	49
Lesson plans and support materials	51
Support worksheets	76
Certificate	85
Pledge	86

Be Internet Legends

Intro letter/email template

Here's a template for a letter (or email). You can customise it to tell parents how new education tools are helping their children learn to make good decisions regarding their online safety and behaviour.



Dear parents,

When our children are young, we do our best to help them get the most out of the internet, while protecting them from the online world's risks and downsides. But as children mature into teenagers, our role shifts to helping them learn to make their own safe and ethical decisions as they navigate their digital lives.

At [school name], we believe this means preparing our [year group or key stage] students to:

- **Think critically** and evaluate online sources.
- **Protect themselves** from online threats, including bullies and scams.
- **Be sharp about sharing:** what, when, and with whom.
- **Be kind and respectful** towards other people and their privacy.
- **Ask for help** from a parent or another trusted adult with tricky situations.

This year these efforts will include Be Internet Legends, a multifaceted programme designed to teach children the skills they need to be safe and smart online. One of the resources, Interland, is a playful browser-based game that makes learning about digital safety interactive and fun — just like the internet itself. Developed by Google in partnership with the educators and online safety experts at Parent Zone, Be Internet Legends provides fun, age-appropriate learning experiences built around five pillars:

- **Think Before You Share**
- **Check it's For Real**
- **Protect Your Stuff**
- **Respect Each Other**
- **When in Doubt, Discuss**

Smart, safe technology usage can help students learn better, and help our schools function better. We believe the Be Internet Legends programme will mark an important step towards our goal of ensuring that all our students at [school name] are learning, exploring, and staying safe online.

If you're interested, we'd be happy to share more information about this new programme, including introductions to some of the resources your children might start using at home. We encourage you to ask them about what we're doing in class; you might pick up a few privacy and security tricks yourselves!

Yours faithfully,



Think Before You Share

Protecting your online reputation

Please read the detailed lesson plans:

- Pages 52-55 for years 3 and 4: Ages 7-9
- Pages 62-64 for years 5 and 6: Ages 9-11

Activities:

- Suitable for both ages 7-9 and 9-11
- Please read the safety guide at the front of the booklet before running any activities with pupils

Lesson summary

Overall aims

Younger children often don't understand that whatever they post online can still be seen by anyone far into the future – this is our 'digital footprint'. As they get older, inappropriate posts or 'digital mistakes' can have a lasting effect on how others see them, or on their online reputation. What may seem like a harmless post today could be misunderstood by different readers in the future.

The activities in this section help pupils develop skills to encourage them to make and maintain a positive online reputation, by managing their privacy and protecting their personal information.

Objectives

Pupils will learn

- ✓ What having a positive digital footprint means.
- ✓ Ways in which they can start to build a positive digital footprint.

Outcomes

Pupils can

- ✓ Explain what it means to have a positive digital footprint, and why it is important.
- ✓ Explain things someone can do to build a positive digital footprint.

Activity guide

- Activity 1: **Is it OK to share? (10 mins)**
- Activity 2: **Whose profile is this, anyway? (10 mins)**
- Activity 3: **How do others see us? (20 mins)**
- Activity 4: **Keeping it private (10 mins)**
- Activity 5: **Interland: Mindful Mountain (20 mins)**

Assessment opportunities

- Assessing pupils' pre-existing knowledge in an introductory activity.
- Think, pair, and share with peers.
- Class discussion and teacher circulation during activities.
- Traffic light assessment after each activity to check understanding and progression (red – not at all confident / amber – quite confident / green – very confident).

Plenary

Pupils reflecting on activities and progress made since introductory activity.

Think Before You Share

Vocabulary



Positive

Something that is good.

Negative

Something that is bad.

Public

When information online is open and anyone can see it.

Private

When information online is closed and you control who sees it. This may be only you, or close friends and family members.

Digital footprint

Your digital footprint is everything on the internet that makes you, you. This could include photos, audio, videos, texts, blog posts and messages that you write on friends' pages.

Personal information

Information about a specific person. Your personal information can be public or private to varying degrees, depending on how sensitive it is.

Settings

The area in any digital service, app, website, etc. where you can define or adjust what you share and how your account is handled.

Personal boundaries

Rules that you make to let others know the safe and acceptable ways for them to behave towards you.

Is it OK to share?

Pupils invent an imaginary character and come up with made-up 'personal' information to start thinking about zones of privacy.



Please read: The detailed lesson plans on pages 52-55 (ages 7-9), and pages 62-64 (ages 9-11).

Activity



1. Invent a character around your age – draw or write the character's name in the middle of a piece of paper, and around the outside, draw or write 'personal' information about this person.
2. Now look at each piece of 'personal' information and identify whether it's OK to share that information online or not. What effect might sharing have on the character's online reputation?

For the differentiation activity, please see lesson plan on page 53.

Let's talk



Why does privacy matter?

Your online persona is everything on the internet that's about you. This could mean photos, audio, videos, texts, your posts on friends' pages, etc. As you get older, a strong online presence can bring with it all kinds of benefits. The internet makes it easy to communicate with family, friends and people who love the same things that you do. We send messages, share pictures and join conversations on social networks, sometimes without giving it a second thought.

But all this online connection can pose various risks. Once something's out there, there's no turning back. A picture or post that you think is funny and harmless today could be seen and misunderstood in the future by people you never intended to see it. Remember:

- Like everything on the internet, your digital footprint could be seen by anyone in the world.
- Once something about you is online, it could be online forever.

That's why your privacy matters. You can protect it by sharing only things that you're sure you want to share – in other words, by being careful about what persona you create online. Knowing when to stay silent and when to speak up is the key to respecting other people's privacy and protecting your own.

Summary

Private information consists of personal details or facts that we might want to keep to ourselves or share only with trusted family or friends. What kinds of information does this include?

- Your home address and phone number.
- Your email and other online passwords.
- Your username.
- Your schoolwork and other documents that you create.
- Your photos, videos, music and other content.

Continued on the next page →

Whose profile is this, anyway?

Pupils study a collection of personal information about a fictitious character to try to deduce things about this person.

Activity



You'll need:

- Various fictitious personal data sources. You can use the handout on the next page, or here are some ideas:
 - Social media accounts, if age appropriate.
 - Printed-out browser history logs.
 - Printed-out list of locations where they 'checked in' (restaurants, coffee shops, Wi-Fi hotspots).
 - Notebooks or devices for a short writing assignment.

1. List at least two pieces of personal information you've found by reading each character's profile.
2. We'll then separate into groups, and each group will write its own quick description of this person. Who do you think they are?
3. How much can we find out about someone just from what they post online, even if we don't know them?

OK, now here's the truth about our character:

- **Gurpreet** is a sixth former. She is going to university next year and hopes to study business, and eventually start her own fashion label. She cares most about: family, volunteering, and pop culture.
- **Mark** is the starting midfielder on the sixth-form football team. He is 16, and lives in Cheltenham. He has an 8-year-old sister. He cares most about: football, design and engineering, playing the guitar, and his friends.
- **Leah** is 17. She just joined the football team and has two cats. She is very good at engineering and likes to build robots at the weekend. She cares most about: technology, her football team, animals and animal rights.

Let's talk



How we know what we (think we) know

There's a lot of personal information to be found on the internet. Some of that information can cause us to make assumptions about people that aren't true. These are the questions that we're going to explore:

- What can we learn about a person from their personal information?
- What can we guess from personal information, even if we aren't sure?
- Do we know how this information was collected in the first place?

That's why your privacy matters. You can protect it by sharing only things that you're sure you want to share – in other words, by being careful about what persona you create online. Knowing when to stay silent and when to speak up is the key to respecting other people's privacy and protecting your own.

Summary

Our assumptions about people aren't always right, but too often we use these inaccurate conclusions to judge or make decisions about someone. Always try to make sure you really know the things about people that you think you know.

Whose profile is this, anyway?

Read each description of a person's online activity below. After each example, write a short description of who you think this person is. What do they like, dislike and care about?

Gurpreet

Mark

Leah

<p>Here are the photos I took of our end-of-year party! Everyone looked good!</p>	<p>Won the game! One more to go before championship. Gotta practice my free kicks</p>	<p> Tokyo Kitchen, Canterbury</p>
<p> Best Ways to Battle Spots</p>	<p>I hate school dances. #ratherbeatarockconcert</p>	<p>Missed the winning goal. ugh. At least we drew.</p>
<p>My little brother Alex is SOO annoying. Maybe he's an alien?</p>	<p> University Academy of Engineering, South Bank, London</p>	<p> 25 Photos of Puppies</p>
<p> Laser Tag Venue, Market Square</p>	<p> 10 Signs Your Parents are Trying to Ruin Your Life</p>	<p> St. Anselm's end of year prom</p>
<p> Young Fashion Design Conference at Sheffield College of Fashion</p>	<p>Fishing this Saturday with my dad at Bristol Water Park! Gonna be fantastic</p>	<p>Hi everyone, check out my friend's website! I wrote all the code for it.</p>
<p>FINALLY SAW THE NEW SPY SQUIRREL MOVIE. Omg obsessed!</p>	<p> Tyler Smith concert at King's Park</p>	<p>Wahoo! Just got my highest score on Confectionary Crunch</p>
<hr/> <hr/> <hr/> <hr/> <hr/>	<hr/> <hr/> <hr/> <hr/> <hr/>	<hr/> <hr/> <hr/> <hr/> <hr/>

How do others see us?

Pupils explore how different types of people – parents, employers, friends, police – would see the character from their previous activity.

Activity



You'll need:

- A copy for each pupil of the fictitious profile from Activity 2, on page 11.

1. Take a new point of view

Now we're going to break into groups, and each group will think about their character from the point of view of one of these types of people:

- Parent
- Teacher
- Friend
- Police
- Advertiser
- Yourself in 10 years

What's important to each of these people? What conclusions would they reach about this profile? Cross out the information that you think your character wouldn't want your group to see or that it would be unwise for them to reveal.

2. Present conclusions

Finally, each group presents its results and explains its privacy choices.

Let's talk



A new point of view

The information in your digital footprint could tell people more about you than you meant to reveal – and the consequences can be significant. Let's take another look at the profile from our character's point of view.

- Do you think he or she wants people to know all this personal information?
- How might this information be used by other people?

Different situations call for different levels of privacy. Seeing the world from someone else's point of view is the key to getting privacy right.

Summary

Different people can see the same information and draw different conclusions from it. Don't assume that people online will see you the way you think they'll see you.

Keeping it private

We're going to review three scenarios and talk about how each one might have a different privacy solution.

Let's talk



You'll need:

- Pictures of each scenario for pupils who need more support (please note example three is different for ages 7-9) on pages 79-80.

Privacy scenarios: What should you do?

Example 1: A child at your school has a really bad haircut and isn't happy with it. Someone takes a picture and shares it online.

- Is it kind to share another person's bad hair day?
- How do you think that person would feel?

Example 2: Someone writes in their diary. Another person copies what they wrote and posts it online.

- Was the other person wrong to post the diary entries?
- How would you feel if someone did this with your diary?

Example 3: Someone posts, 'have a good holiday,' on a friend's social media page.

- Had the friend announced publicly that they were going away?
- Are there more private ways to communicate this message – i.e., sending a private message or text?

Summary

Different situations call for different responses. It's always important to respect other people's privacy choices, even if they aren't the choices that you yourself would make.

Interland: Mindful Mountain

The mountainous town centre of Interland is a place where everyone mingles and crosses paths. But you must be very careful about what you share and with whom. Information travels at the speed of light and there's an oversharer among the Internauts you know.

Open a web browser on desktop or mobile device (e.g., tablet), visit [g.co/interland](https://www.g.co/interland), and navigate to the land called Mindful Mountain.



Please read: The detailed lesson plans on pages 52-55 (ages 7-9), and pages 62-64 (ages 9-11).

Let's talk



After pupils explore Mindful Mountain, these questions will encourage discussion of the game's themes.

- Why is the character in the game called an oversharer?
- How do the oversharer's actions affect the game?
- How has playing the game made you think about what people should share online?
- How can sharing something publicly online instead of just with friends affect someone's online reputation?
- What can someone do, or how can they get help, if they share something they later regret online?

Discussion questions for younger years

- Why is the character in the game called an oversharer?
- How do the oversharer's actions affect the game?
- How has playing the game made you think about what people should share online?
- When is making something public online, instead of just with friends, not a good idea or potentially unsafe?
- What can someone do, or how can they get help, if they share something they later regret online?



Check it's For Real

Staying away from phishing and scams

Please read the detailed lesson plans:

- Pages 52-55 for years 3 and 4: Ages 7-9
- Pages 65-67 for years 5 and 6: Ages 9-11

Activities:

- Suitable for both ages 7-9 and 9-11
- Please read the safety guide at the front of the booklet before running any activities with pupils

Lesson summary

Overall aims

It's important for children to understand that online content isn't always honest or reliable, and is sometimes even deliberately designed to steal personal information. The activities in this lesson help give children the skills to stay safe online by spotting the clues that something may be suspicious, misleading or a scam.

Objectives

Pupils will learn

- ✓ How to be a critical consumer while online.
- ✓ About different online scams, including what 'phishing' means.

Outcomes

Pupils can

- ✓ Describe ways to critically evaluate what we see on social media.
- ✓ Explain how social media can mislead or misrepresent reality.
- ✓ Identify different types of online scams people our age may experience, including 'phishing'.
- ✓ Identify sources of support for someone who is worried about anything online.

Activity guide

Activity 1: **Don't bite that phishing hook! (15 mins)**

Activity 2: **Who are you, really? (20 mins)**

Activity 3: **Interland: Reality River (20 mins)**

Assessment opportunities

- Assessing pupils' pre-existing knowledge in introductory activity.
- Think, pair, and share with peers.
- Class discussion and teacher circulation during activities.
- Pupils acting out scenarios.
- Traffic light cards for measuring progress throughout the lesson and at start/finish.

Plenary

Pupils share advice based on what they've learnt.

Check it's For Real

Vocabulary



Genuine

Something that is real and true.

Honest

Something that is truthful and reliable.

Fraud

A trick to get something from someone.

Unreliable

Something you can't trust. You may be unsure that it's true.

Suspicious

You may feel this way when you don't trust something or someone — or you think information may be fake or dishonest.

Phishing

A phishing attack happens when someone tries to trick you into sharing personal information online. Phishing is usually done through email, ads, or sites that look similar to sites you already use.

Spear phishing

A phishing scam where an attacker targets you more precisely by using pieces of your own personal information.

Scam

A dishonest attempt to make money or gain something else of value by tricking people.

Trustworthy

Able to be relied on to do what is right or what is needed.

Authentic

Real, genuine, true, or accurate; not fake or copied.

Verifiable

Something that can be proven or shown to be true or correct.

Deceptive

Intended to make someone believe something that isn't true.

Firewall

A program that shields your computer from most scams and tricks.

Malware

A term used to refer to a variety of forms of hostile or intrusive software, including computer viruses and other malicious programs.

Encrypted

When information or data is converted into a code.

Don't bite that phishing hook!

A game where pupils study various emails and texts and try to decide which are for real and which are phishing scams.



Please read: The detailed lesson plans on pages 52-55 (ages 7-9), and pages 65-67 (ages 9-11).

Activity



You'll need:

- Support worksheet on page 80.
- Student handout: Phishing examples on pages 20-21.

Answers to student handout: Phishing examples

1. **Real.** The email asks the user to sign in to their account on their own, rather than providing a link that could be malicious.
2. **Fake.** Suspicious and not secure URL.
3. **Real.** Note the https:// in the URL.
4. **Fake.** Suspicious offer in exchange for bank details or other personal information.
5. **Fake.** Not secure and suspicious URL.

1. Group study examples

Let's divide into groups. Each one studies examples of messages and websites.

2. Individuals indicate choices

Select 'real' or 'fake' for each example, and list reasons why below.

3. Groups discuss choices

Which examples seemed trustworthy and which seem suspicious?
Did any answers surprise you?

4. Further discussion

Here are some more questions to ask yourself when assessing messages or sites you find online:

- Does this message look right? What's your first instinct? Do you notice any untrustworthy parts?
- Is the email offering you something for free? Free offers usually aren't really free.
- Is it asking for your personal information? Some websites ask for personal information so they can send you more scams. For example, a 'personality test' could be gathering facts to make it easy to guess your password or other secret information. Most real businesses, on the other hand, won't ask for personal information over email.
- Is it a chain email or social post? Emails and posts that ask you to forward this to everyone you know can put you and others at risk. Don't do it unless you're sure of the source and sure the message is safe to pass on.
- Read the fine print. At the bottom of most documents you'll find the fine print. This text is tiny, and often contains the stuff you're supposed to miss. For example, a headline at the top might say 'you've won a free phone', but in the fine print you'll read that you actually have to pay that company £200 per month.

Note

- For the purposes of this exercise, pretend that Internaut Mail is a real, trusted service.
- Please see lesson plan on page 54 for differentiation activity.

Continued on the next page →

Don't bite that phishing hook!

Let's talk



What is this phishing thing anyway?

Phishing in the online world (not to be confused with 'fishing' with an 'f') is when someone tries to steal information like your login or account details in an email, text, or other online communication by pretending to be someone you trust. Phishing emails – and the unsafe sites they try to send you to or the downloads and attachments they try to get you to open – can also put viruses on your computer that use your contacts list to target your friends and family with more phishing emails. Other scams might try to trick you into downloading malware or unwanted software by telling you that there's something wrong with your device. Remember: A website or ad can't tell if there's anything wrong with your machine!

Some phishing attacks are obviously fake. But others can be sophisticated and convincing. For instance, when a scammer sends you a message that includes some of your personal information, it's called 'spear phishing', and it can be very effective.

It's important to know how to spot anything odd or unusual in emails and texts early, before you click on questionable links or enter your password on risky websites. Here are some questions to ask when you're assessing a message or site:

- Does it include the indicators of a trustworthy site, such as badges?
- Does a site's URL match the name and title you're looking for?
- Are there any pop-ups? (They're often bad news.)
- Does the URL start with 'https://' preceded by a green padlock? (That means the connection is encrypted and secure.)
- What's in the fine print? (That's where they put the sneaky stuff.)

And what if you do fall for a scam? Start with this: Don't panic!

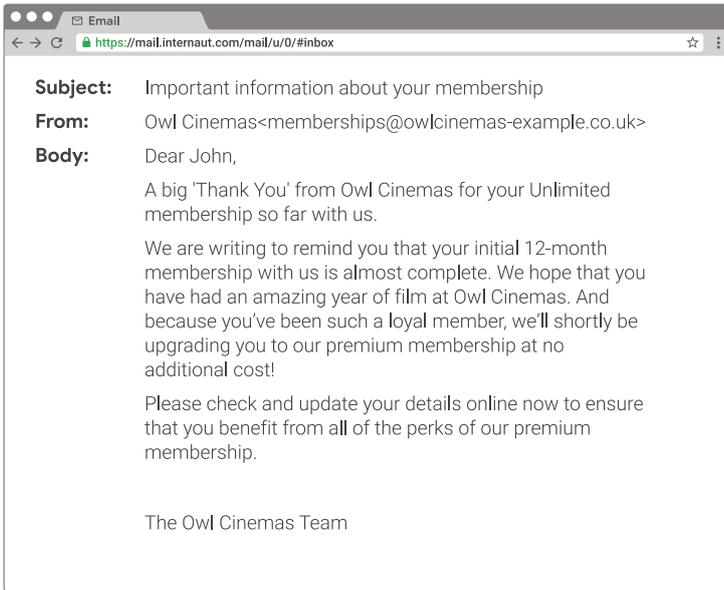
- Tell your parent, teacher, or another trusted adult right away. The longer you wait, the worse things could get.
- Change your passwords for online accounts.
- Let any friends who might be targeted as a result know.
- Use settings to report the message as spam, if possible.

Summary

When you're online, always be on the lookout for phishing attacks in your email, texts, and posted messages – and make sure you tell the right people about it if you do get fooled.

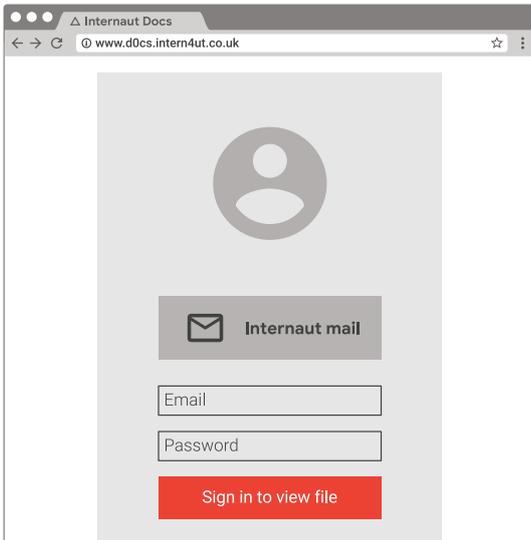
Worksheet: Activity 1

Phishing examples



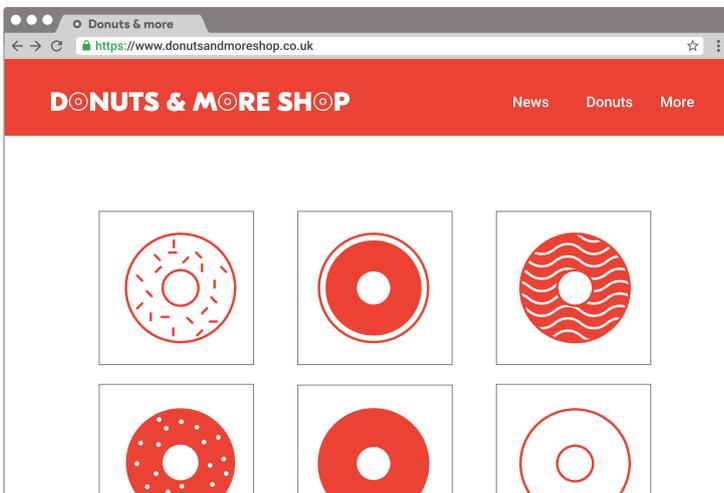
1. Is this real or fake?

Real Fake



2. Is this real or fake?

Real Fake

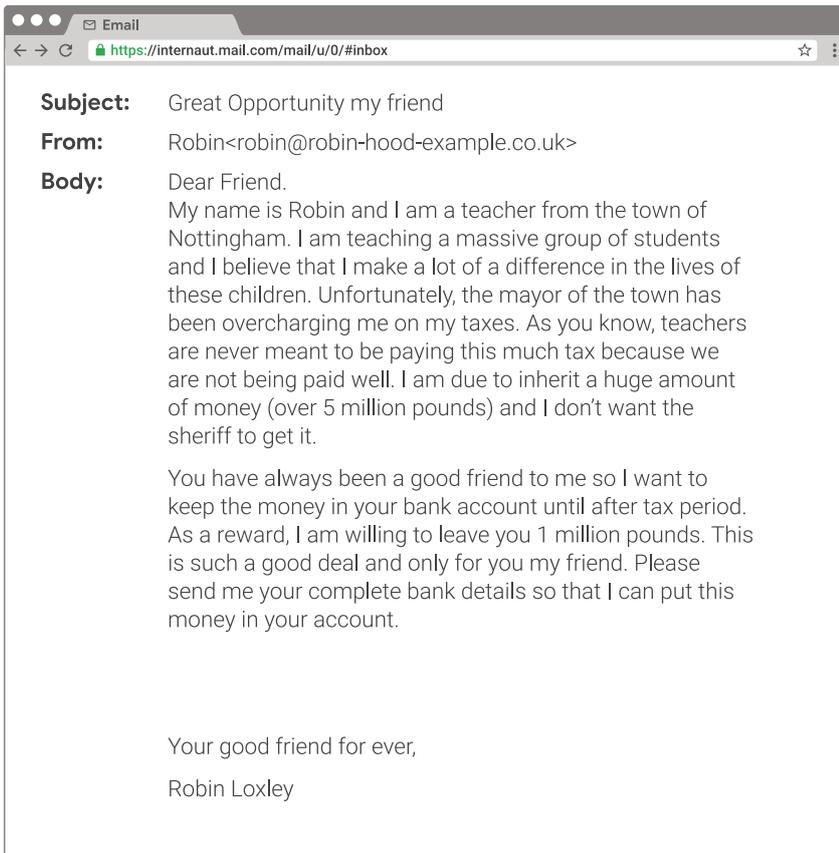


3. Is this real or fake?

Real Fake

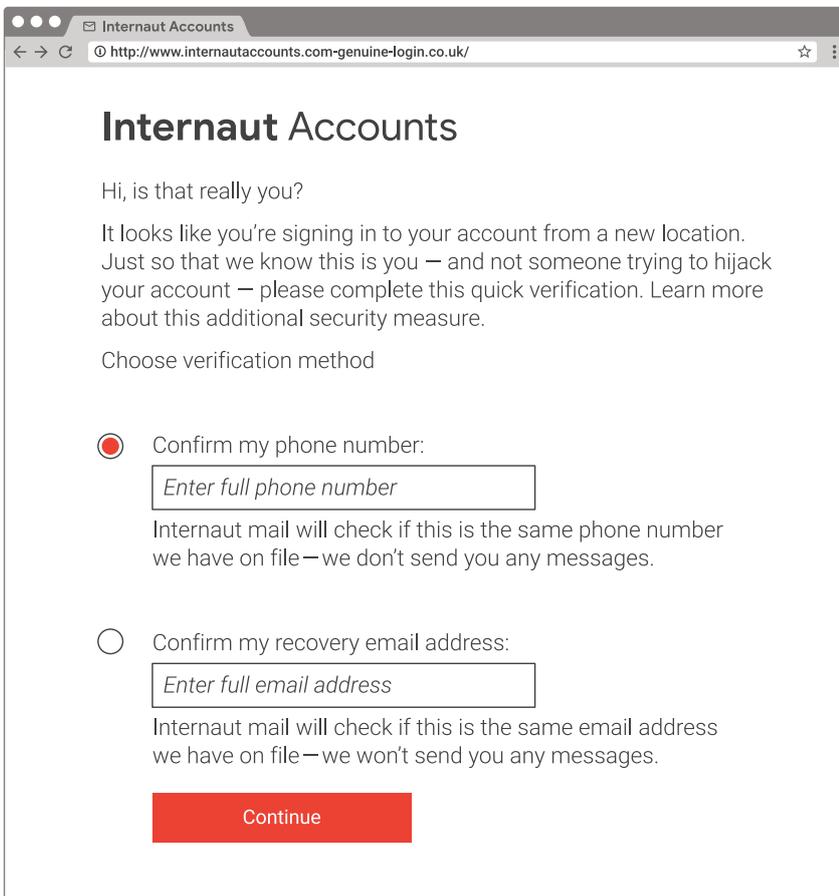
Continued on the next page →

Phishing examples



4. Is this real or fake?

Real Fake



5. Is this real or fake?

Real Fake

Be Internet Alert: Activity 2

Who are you, really?

Pupils practise their anti-phishing skills by discussing possible responses to suspicious online texts, posts, pictures, and emails.

Activity



You'll need:

- A copy of the 'Who are you, really?' worksheet cut into strips, with one scenario on each strip.
- A bowl or container to hold the strips when pupils pick one.

1. Pick a scenario from the container.
2. In your group, discuss possible responses to the message (and decide on three to six different options.)
3. Decide on which would be the best option and why.
4. See the cheat sheet on pages 25-26.
5. Discuss whether you agree with it.
6. Class feedback – display each scenario on the whiteboard. Each group can explain what they decided was the best response and why.

Please see lesson plan on page 54 for differentiation activity.

Continued on the next page →

Who are you, really?

Let's talk



How do you know it's really them?

When you're on the phone with a friend, how can you tell it's them, even though you can't see them?

Sometimes people pretend to be other people online as a prank. Other times, they impersonate someone in order to steal personal information. When you're on the internet, strangers could ask to connect with you. It's up to you to decide whether you want to connect with that person, and what or how to reply.

Fortunately, you can verify people's identity and spot scammers. Here are a few ideas to start thinking about:

- **Is their profile picture suspicious?**

Is their profile picture blurry or hard to see? If so, be cautious; a blurry photo is easier to hide behind. It's also common for scammers to steal photos from a real person in order to set up a fake profile.

- **Does their displayed name match their username?**

On social media, for instance, does their profile URL match their given name? (For example, Jane Doe, with an address that's something like SocialMedia.com/jane.doe.)

- **Do they have a personal biography?**

If so, does it sound like it was written by a real person? Fake accounts might not have much 'About Me' information or might have grouped together some information to create a fake profile.

- **How long has the account been active?**

Is the profile new or does it show a lot of activity? Fake accounts often lack a history of posts or social interactions.

Summary

You control who you talk to online. Make sure the people you connect with are who they say they are!

Who are you, really?

Scenario 1

Sandeep gets an online message request from a stranger. 'Hi! Do you want to hang out? Can you add me to your friends list?' – Jason'

Scenario 2

Layla gets a text message on her mobile phone from someone she doesn't recognise. 'Hi, this is Jen! Remember me from the summer?'

Scenario 3

After maths lesson with Mrs. Beckstrom, Alex gets this message on his mobile phone. 'I'm Mark from your maths lesson with Mrs. Beckstrom. Did you understand the homework?'

Scenario 4

Dami gets a message from someone he doesn't follow. 'Hi! Love your posts, you're SO funny! Give me your phone number and we can talk more!'

Scenario 5

Charlotte gets a message from someone with whom she isn't familiar. 'I saw you in the playground today. YOU'RE CUTE! What is your address? I can come over to hang out.'

Scenario 6

Maryam receives a message online: 'Hi, I just met your friend Sam! She told me about you, would love to meet you. What's your address?'

Continued on the next page →

Who are you, really?

Scenario 1

Sandeep gets this message from someone she doesn't recognise: 'Hi! Do you want to hang out? Can you add me to your friends list? – Jason'

- **Ignore Jason.** If you don't know him, you can just decide not to talk to him.
- **'Hi, Jason. Do I know you?'** If you aren't sure, ask first.
- **Block Jason.** If you've checked who he is and decide to block him, you won't get any more messages from him.
- **Add Jason to your friends list.** Not recommended, unless you've verified who he is.
- **Give him personal info.** Should you respond with something like, 'Great to know new people nearby! I'm new in town. We can meet after school sometime. (I go to Emerson Middle school.)'? No! It's never good to give away personal information to people you don't know, especially online.

Scenario 2

Layla gets a text message on her mobile phone from someone she doesn't recognise. 'Hi, this is Jen! Remember me from the summer?'

- **Block Jen.** This could be a rude thing to do if you actually know her. Use this option only if you know her but you don't want to get her messages any more or you're sure you didn't meet anyone named Jen last summer.
- **Ignore Jen.** Like we said above, if you don't know this person, you can just not talk to her.
- **'Hi, Jen. Do I know you?'** This is a safe option if you aren't sure what to do.
- **'Hey! What's up? Nice to hear from you.'** This is fine, as long as you do actually remember her from the summer!
- **'Are you the girl with the red hair?'** If you aren't sure whether you know her, you can try to get more information to help you remember.
- **'I don't remember you, but we can still meet sometime.'** Really not a good idea; you should never offer to meet with anyone you don't know.

Scenario 3

After maths lesson with Mrs. Beckstrom, Alex gets this message on his mobile phone. 'I'm Mark from your maths lesson with Mrs. Beckstrom. Did you understand the homework?'

- **Ignore Mark.** As always, if you don't know this person, you don't have to respond at all.
- **Block Mark.** A good choice if you're sure there's no Mark in Mrs. Beckstrom's maths class.
- **'Hi, Mark. Are you the one sitting behind me?'** If you aren't sure, you can ask.
- **'Sure. Can explain after school.'** This is a good choice only if you're sure who this person is.
- **'I don't take maths with Mrs. Beckstrom – I have Mr. Snyder.'** If you don't trust this person, you shouldn't be giving them personal information, like the name of your maths teacher.
- **'Call me on 07123 456 789.'** Probably not; unless you're certain that you know this person, it's not a good idea to send your personal information.

Who are you, really?

Scenario 4

Dami gets a message from someone he doesn't follow. 'Hi! Love your posts, you're SO funny! Give me your phone number and we can talk more!'

- **Ignore @footballgirl12.** You don't have to respond if you don't want to.
- **Block @footballgirl12.** If you find this person suspicious, you can block them and never hear from them again.
- **'Hi, do I know you?'** If you aren't sure, ask questions before giving out personal information like your phone number.
- **'OK, my number is...'** Nope! Even if you've verified who this person is, it isn't a good idea to give out personal information over social media. Find another way to get in touch, through parents, teachers, or some other trusted person.

Scenario 5

Charlotte gets a message from someone with whom she isn't familiar. 'I saw you in the playground today. YOU'RE CUTE! What is your address? I can come over to hang out.'

- **Ignore.** Probably a good choice.
- **Block this person.** Don't hesitate if you get a bad feeling about someone.
- **'Who are you?'** Probably not. If the message sounds suspicious, it might be better not to answer or block them.
- **'Is that you Lizi? YOU'RE CUTE too! I live at 24 Circle Court.'** This isn't a good idea, even if you think you know who Lizi is. Before you give someone new your address or other personal information, check them out, even if you assume you know them.

Scenario 6

Maryam receives a message online: 'Hi, I just met your friend Sam! She told me about you, would love to meet you. What's your address?'

- **Ignore.** If you don't know this person but you do have a friend named Sam, your safest choice is to check with Sam before responding to this message.
- **Block.** If you don't know this person and you don't have a friend named Sam, it's probably a good idea to use your settings to block this person from contacting you any further.
- **'Who are you?'** Probably not a great idea; if you don't know the person, it's better not to answer, at least until you've heard back from Sam.

Interland: Reality River

The river that runs through Interland flows with fact and fiction. But things are not always what they seem. To cross the rapids, use your best judgement and don't fall for the antics of the phisher lurking in these waters.

Open a web browser on your desktop or mobile device (e.g., tablet), visit [g.co/interland](https://www.google.com/interland), and navigate to the land called Reality River.



Please read: The detailed lesson plans on pages 52-55 (ages 7-9), and pages 65-67 (ages 9-11).

Let's talk



Reality River should get pupils thinking. After they play, these questions should encourage a discussion of the game's themes.

- How did you know if something in the game was real or fake? What were the signs?
- What is a phisher? What does it do and how does it affect the game?
- Which clues in the game hinted that something was strange about certain situations?
- Do you think that playing this game will help you be safer online in the future?
- Now that you've played this game, what's one thing you might do differently when you're online in future?
- What should you do if you're unsure or worried about something you come across online?

Discussion questions for younger years

- How did you know if something in the game was real or fake? What were the signs?
- Do you think that playing this game will help you to be safer online in the future?
- Now that you've played this game, what will you always try to remember when you're online in future?
- What should you do if you're unsure or worried about something you come across online?



Protect Your Stuff

Be realistic about privacy and security

Please read the detailed lesson plans:

- Pages 56-61 for years 3 & 4: Ages 7-9
- Pages 68-71 for years 5 & 6: Ages 9-11

Activities:

- Suitable for both ages 7-9 and 9-11
- Please read the safety guide at the front of the booklet before running any activities with pupils

Lesson summary

Overall aims

Pupils will learn to understand the importance of protecting their personal information online and be aware that information they put online is not necessarily safe and/or private. They will look at ways of securing their information online, and asking for help if they are concerned about their own or others' online safety.

Objectives

Pupils will learn

- ✓ Ways to develop safe habits online, including the importance of protecting personal information.
- ✓ How to respect online privacy boundaries for themselves and others.
- ✓ Ways to seek or ask for help if they or others feel unsafe online.

Outcomes

Pupils can

- ✓ Explain why it's important to keep personal information private online.
- ✓ Describe ways to keep personal information private online by using safety tools and privacy settings.
- ✓ Describe how to find and ask for help if someone feels unsafe online.

Activity guide

Activity 1: **How to build a strong password (10 mins)**

Activity 2: **Shh... Keep it to yourself! (15 mins)**

Activity 3: **Taking care of yourself and others (10 mins)**

Activity 4: **Interland: Tower of Treasure (20 mins)**

Assessment opportunities

- Assessing pupils' pre-existing knowledge in the introductory activity.
- Think, pair, and share with peers.
- Class discussion and teacher circulation during activities.
- Pupils responding to scenarios.

Plenary

Pupils share advice based on what they've learnt.

Protect Your Stuff

Vocabulary



Privacy

Protecting your personal information and that of others.

Security

Using good habits for securing hardware and software.

Two-step verification

A security process where logging in to a service requires two steps. For example, you may have to enter your password and enter a code that was sent to your mobile phone.

Security token

A key fob or other small hardware device that you carry in order to authorise access.

Password

A secret combination used to access something.

Hacker

A person who uses a computer to gain access to private information without permission.

Scammer

Someone who cheats or tricks someone else into giving away their private information or even money.

How to build a strong password



One thing that can help ensure our personal information is safe online is to use a strong password. What do you think a strong password could be?

Please read: **The detailed lesson plans on pages 56-61 (ages 7-9), and pages 68-71 (ages 9-11).**

Pupils learn how to create a strong password – and make sure that it stays private after they create it.

Activity



You'll need:

- Internet-connected devices for pupils or groups or pupils.
- A chalk/whiteboard.
- Student handout: Guidelines for creating strong passwords on page 33.

Let's play the password game.

1. Create passwords

We'll all split into teams of two. Each team will have 60 seconds to create a password.

2. Compare passwords

Two teams at a time will write their password on the board.

3. Vote!

For each pair of passwords, we'll all vote and discuss whose is stronger.

Let's talk



Better safe than sorry

Digital technology makes it easy to communicate with friends, classmates, teachers and others. We can connect with the world in so many ways: via email, text and instant messages; in words, pictures and videos; using phones, tablets and laptops. How do you connect with your friends?

But the same tools that make it easy for us to share information also make it easier for hackers and scammers to steal it and use it to damage our devices, our relationships and our reputations. Protecting all the things that go into creating our online reputations means doing simple, smart things like using screen locks on our devices, being careful about putting personal information on devices that can be lost or stolen, and above all, choosing good passwords.

- Who can guess what the two most commonly used passwords are?
(Answer: '1 2 3 4 5 6' and 'password'.)
- Let's brainstorm some other bad passwords.
(Examples: your full name, your phone number, the word 'chocolate')
- Who thinks these passwords are good?

Continued on the next page →

How to build a strong password

Summary

Here's an idea for creating an extra-secure password. Think of a fun phrase that you can remember. It could be your favourite song lyric, book title, film, catchphrase, etc.

- Choose the first letter or first two letters of each word in the phrase.
- Change some letters to symbols.
- Make some letters uppercase and lowercase.

How to build a strong password

Guidelines for creating strong passwords

Here are some tips to help you build a great password:

Strong passwords are based on a descriptive sentence that's easy for you to remember and difficult for someone else to guess.

Moderate passwords are strong and not easy to guess by bad software, but could be guessed by someone who knows you.

Weak passwords commonly use personal information, are easy to crack and can be guessed by someone who knows you.

DO

- Use a unique password for each of your important accounts.
- Use at least eight characters.
- Use combinations of letters (uppercase and lowercase), numbers, and symbols.

DON'T

- Don't use personal information (name, address, email, phone number, National Insurance number, mother's maiden name, birth dates, etc.), or common words in your password.
- Don't use a password that's easy to guess, like your nickname, name of your school, favourite football team, etc.

Tips

- Don't share your password with anyone other than your parents/guardians.
- Try to change your passwords regularly — ideally every six months.

Shh... Keep it to yourself!

Use a school device to demonstrate where to look, and what to look for, when customising privacy settings.



Please read: The detailed lesson plans on pages 56-61 (ages 7-9), and pages 68-71 (ages 9-11).

Activity



You'll need:

- One school device connected to a projector to display the temporary social media account from the Think Before You Share lesson.
- One device with apps for each student or group of students.

1. Review options

I have my laptop hooked up to the projection screen. Let's navigate to the settings page of this app. We can see that our options include:

- Changing your password.
- Getting alerts if someone tries to log in to your account from an unknown device.
- Making your online profile, including photos and videos, only visible to your chosen circles of family and friends.
- Enabling two-factor authentication or two-step verification.

2. Additional verification options

Let's talk about two-step and two-factor verification.

- Two-step verification: When you log into your account, it will require two steps. For example, it may ask you to enter your password AND text you a code that has to be entered within 10 minutes before it expires.
- Two-factor verification: The system will require two types of information to log you in. For example, it may ask for your normal password and your fingerprint.

Which privacy and security settings are right for you? That's something to discuss with your parent or guardian. But remember, the most important security setting is in your brain – you make the key decisions about when, how much and with whom you share your personal information.

Let's talk



Privacy means security

Online privacy and online security go hand in hand. Most apps and software offer ways to control what information we're sharing and how.

When you're using an app or website, look for an option like 'My Account' or 'Settings'. That's where you'll find the privacy and security settings that let you decide:

- What information is visible in your profile.
- Who can view your posts, photos, videos, or other content that you share.

Learning to use these settings to protect your privacy – and remembering to keep them updated – will help keep you as safe as possible.

Shh... Keep it to yourself!

Summary

Choosing a strong, unique password for each of your important accounts is a good first step. Now you need to remember them and also keep them safe.

Writing down your passwords isn't necessarily a bad idea. But if you do this, don't leave a page with your passwords in plain sight, such as on your computer or desk. Safeguard your list, and protect yourself, by hiding it somewhere.

Taking care of yourself and others

Activity



You'll need:

- Copies of the three scenarios from Activity 4 on page 13.

1. Let's look at the three scenarios from Lesson 1, from Activity 4 on page 13 in our groups.
2. Discuss the following in your groups
 - What can someone do if they feel unsafe online?
 - Who can they tell or go to?
 - What might happen when they tell?
 - What might happen after that?
3. Time to feed back to the rest of the class!

Interland: Tower of Treasure

Mayday! The Tower is unlocked, leaving the Internaut's valuables such as personal information and passwords at high risk. Outrun the hacker and build an untouchable password every step of the way to secure your private information once and for all.

Open a web browser on your desktop or mobile device (e.g., tablet), visit [g.co/interland](https://www.google.com/interland), and navigate to the land called Tower of Treasure.



Please read: [The detailed lesson plans on pages 56-61 \(ages 7-9\)](#), and [pages 68-71 \(ages 9-11\)](#).

Let's talk

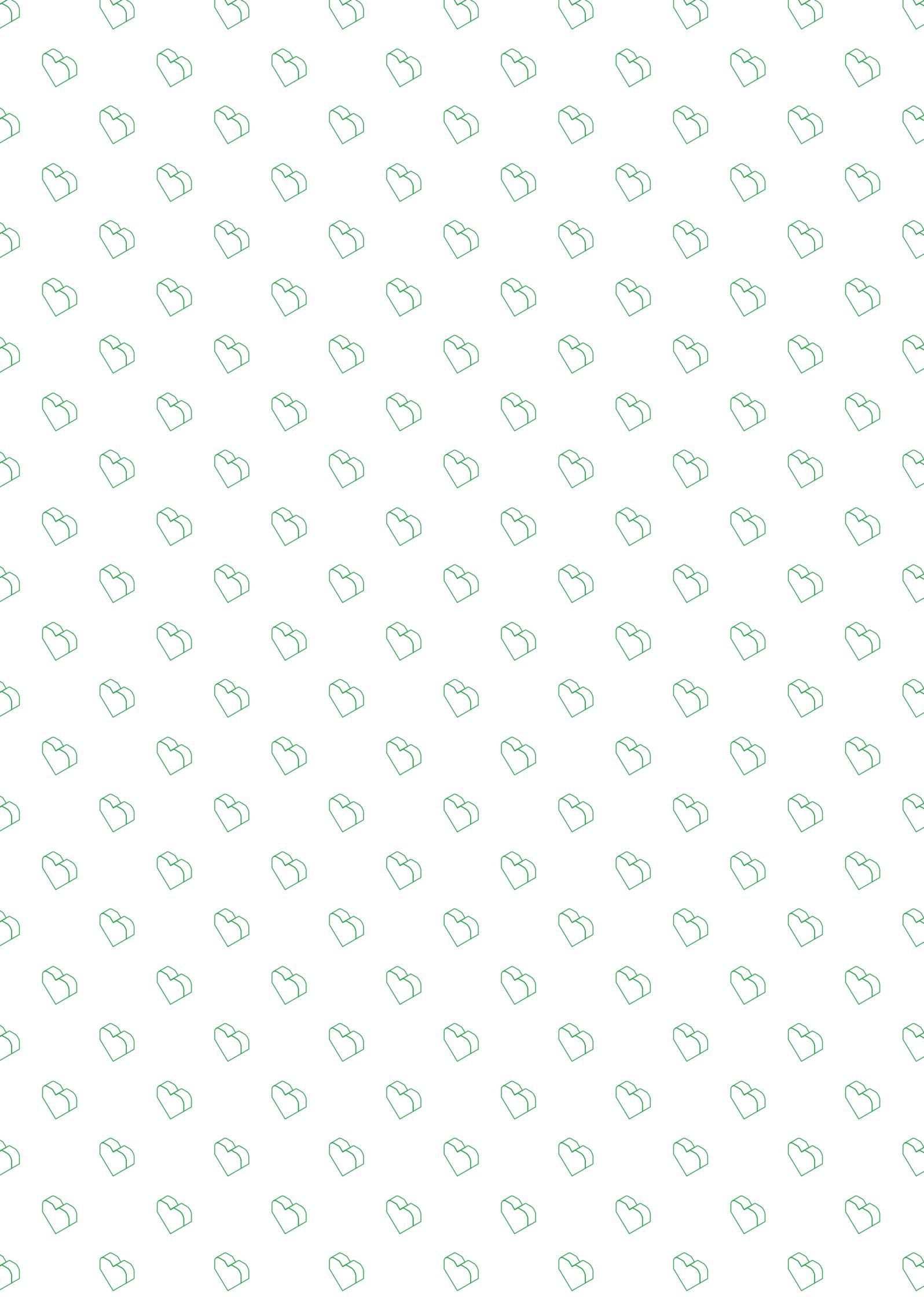


Tower of Treasure will get pupils thinking. After they play, use these questions to start a discussion of the game's themes.

- What are the elements of a super-strong password?
- When is it important to create strong passwords in real life? What tips have you learned about how to do so?
- What's a hacker? Describe this character's behaviour and how they affect the game.
- Did Tower of Treasure change the way you plan to protect your information in the future?
- Name one thing you'll do differently after learning these lessons and playing the game.
- Craft three practice passwords that pass the 'super strong' test.
- What are some examples of sensitive information that should be protected?

Discussion questions for younger years

- What makes a super-strong password?
- When is it important to create strong passwords in real life? What tips have you learned about how to do so?
- Name one thing that you'll remember to do now after playing the game.



Respect Each Other

The power of online positivity

Please read the detailed lesson plans:

- Pages 56-61 for years 3 & 4: Ages 7-9
- Pages 72-74 for years 5 & 6: Ages 9-11

Activities

- Suitable for both ages 7-9 and 9-11
- Please read the safety guide at the front of the booklet before running any activities with pupils

Lesson summary

Overall aims

This is the final lesson in a series of four looking at online safety. Learning to convey kindness and empathy online – and knowing how to respond to negativity and hurtful behaviour – is essential for building and maintaining healthy relationships. These skills can help to reduce feelings of isolation which can sometimes lead to bullying, depression, academic struggles and other problems. The activities in this lesson teach pupils how to interact positively online as well as enabling them to recognise and manage negative online behaviours.

Objectives

Pupils will learn

- ✓ How to develop respectful, empathetic and healthy online relationships.
- ✓ Ways to manage and respond in a healthy and safe way to hurtful online behaviour.

Outcomes

Pupils can

- ✓ Demonstrate ways to build positive and healthy online relationships and friendships.
- ✓ Describe strategies they can use to respond to hurtful online behaviour, in ways that keep them safe and healthy.
- ✓ Identify sources of support that can help friends and peers if they are experiencing hurtful behaviour online.

Activity guide

Activity 1: **How can I stand up to others online? (15 mins)**

Activity 2: **Turning negative into positive (20 mins)**

Activity 3: **Mixed messages (5 mins)**

Activity 4: **Reacting to role models (10 mins)**

Activity 5: **Interland: Kind Kingdom (20 mins)**

Assessment opportunities

- Assessing pupils' pre-existing knowledge in the introductory activity.
- Think, pair, and share with peers.
- Class discussion and teacher circulation during activities.

Plenary

Pupils share advice based on what they've learnt.

Respect Each Other

Vocabulary



Bullying

Unwanted, aggressive behaviour that is repeated (or has the potential to be repeated) over time.

Bystander

Someone who has the power to intervene or report bad behaviour, but doesn't do anything to stop it.

Upstander

Someone who intervenes to stop and/or report inappropriate behaviour.

Harassment

To create an unpleasant or hostile situation with uninvited and unwelcome verbal or physical conduct.

Amplify

To make something louder or stronger.

Block

To help prevent an individual from accessing your profile, sending you messages, etc.

How can I stand up to others online?

Pupils identify what a bystander should do if they witness bullying or nastiness towards someone they know.



Please read: The detailed lesson plans on pages 56-61 (ages 7-9), and pages 72-74 (ages 9-11).

Activity



1. Make a circle of words describing feelings that explains how someone who has read something nasty online about someone they know may feel (a bystander).
2. In your groups write down a tip for what this bystander could do to stand up for others and deal with the situation.
3. Make a graffiti wall of the suggestions.
4. Which ones do you think are the most helpful?

Continued on the next page →

How can I stand up to others online?

Let's talk



Why does kindness matter?

Sometimes it's important to remind ourselves that behind every username and profile picture there's a real person with real feelings, and we should treat them that way. When bullying or other inappropriate behaviour happens, most of the time there are three types of people involved.

- A **bully** — or bullies.
- Someone being bullied — the **target**, or **victim**.
- One or more people we call **bystanders**.

A bystander has the power to intervene and report inappropriate behaviour, but doesn't do anything to stop it. Your goal is to call out bad behaviour and stand up for kindness and positivity. A little positivity can go a long way online. But the opposite is also true: A little negativity can spread into something serious, with upsetting and possibly harmful consequences online.

Here are some ways that upstanders can help stop bullying and stop negative messages online:

- **Set a good example**

Being a positive voice among your friends helps spread positive feelings all around.

- **Be a friend**

Being consistently friendly — both online and offline — shows your classmates that they're not alone, which can be especially helpful if they're being bullied or just feeling sad.

- **Don't encourage bad behaviour by giving it an audience**

Don't 'like' or respond to hurtful comments or posts. Sometimes bullies act aggressively in order to get attention, and if you and your friends don't encourage them, they're more likely to stop.

- **Don't pass on hurtful messages**

Instead, tell the person who sent the message that you don't think it was funny or acceptable, and consider contacting the person who was targeted to provide help and support if needed.

- **Report mean, bullying behaviour**

Use online reporting tools or tell your parent, teacher, friend or sibling.

Turning negative into positive

A 3-step activity to learn how to reframe negative comments into more positive ones.

Activity



Materials needed:

- Your whiteboard or interactive whiteboard.
- Handouts of fictitious negative comments.
- Writing materials for pupils.

1. We're all looking at the negative comments.
2. Look at the first negative comment together.
3. In pairs, reframe the rest of the negative comments into more positive ones.

Let's talk



Turning negative to positive

Children your age are exposed to — and produce — a wide range of content, which can include lots of negative messages that promote bad behaviour.

- Have you (or anyone you know) ever experienced a random act of kindness online? How did it make you feel?
- Have you (or anyone you know) seen someone be negative on the internet? How did that make you feel?
- What simple actions can we take to turn negative interactions into positive ones?

We can respond to negative emotions in constructive ways by rephrasing or reframing unfriendly comments and becoming more aware of tone in our online communication.

Summary

Whether standing up for others, reporting something hurtful or ignoring something to stop it from being amplified even more, you have a variety of strategies to choose from, depending on the situation. Everyone is responsible for creating a positive online experience.

Continued on the next page →

Worksheet: Activity 2

Turning negative into positive

'Lol Connor is the only one in class not going on the camping trip this weekend.'

'Everybody wear purple tomorrow but don't tell Yasmin.'

'Sorry I don't think you can come to my party. It'll cost too much money.'

'No offence but your handwriting is embarrassing so you should probably switch groups for this project.'

'This makes me cringe – who told Aisha she can sing??'

'You can only join our group if you give me the login to your account.'

'Am I the only one who thinks Clare looks kinda like a Smurf?'



Mixed messages



Pupils interpret the emotions behind text messages to practise thinking critically and avoiding misinterpretation and conflict in online exchanges.

Please read: The detailed lesson plans on pages 56-61 (ages 7-9), and pages 72-74 (ages 9-11).

Activity



Materials needed:

- Sample text messages or posts written on the board.

1. Review messages

Let's take a look at these sample text messages or posts on the board:

- 'K 😎'
- 'Whatever 😒'
- 'I'm so angry with you 😡'

2. Read messages out loud

Now, for each message, we're going to ask one person to read it aloud in a specific tone of voice (e.g. angry, sarcastic, friendly). What do you notice? How might these come across to other people? How might each 'message sender' better communicate what they really mean?

Let's talk



It's easy to misunderstand

Young people use different types of communication interchangeably, but messages sent via chat and text can be interpreted differently than they would in person or over the phone.

- Have you ever been misunderstood in a text? For example, have you ever posted a joke and your friend thought you were being serious?
- Have you ever misunderstood someone in a text or chat? What did you do to help clarify the communication? What could you do differently?

Summary

It can be hard to understand how someone is really feeling when you're reading what they wrote or texted. Make sure that you choose the right methods of communication – and that you don't read too much into things that people say to you online.

Reacting to role models

Simple class discussion of how children sometimes model celebrity behaviour.
N.B. See differentiation support sheet on page 82 for kindness 'emoji' images.



Please read: The detailed lesson plans on pages 56-61 (ages 7-9), and pages 72-74 (ages 9-11).

Let's talk



What celebrities can teach children

There are plenty of examples of how bullying and harassment aren't just issues for children – look at how celebrities can treat each other online and offline too.

We've been talking about how important it is to be kind to classmates and friends online, as well as offline. Can you think of any examples when celebrities acted negatively towards each other?

Do you think some children start bullying or making unkind comments because they see celebrities behaving this way?

Summary

The way you and your friends treat each other online will have a big impact on the digital world that your generation builds. Do you think your generation can build an internet that's kinder and more positive than the environments some adults have created for themselves?

A lot of adults think you'll probably be better at this too...

Interland: Kind Kingdom

Vibes of all kinds are contagious – for better or for worse. In the sunniest corner of town, cyberbullies are running amok, spreading negativity everywhere. Block and report bullies to stop their takeover and be kind to other Internauts to restore the peaceful nature of this land.

Open a web browser on your desktop or mobile device (e.g., tablet), visit g.co/interland, and navigate to the land called Kind Kingdom.



Please read: The detailed lesson plans on pages 56–61 (ages 7–9), and pages 72–74 (ages 9–11).

Let's talk

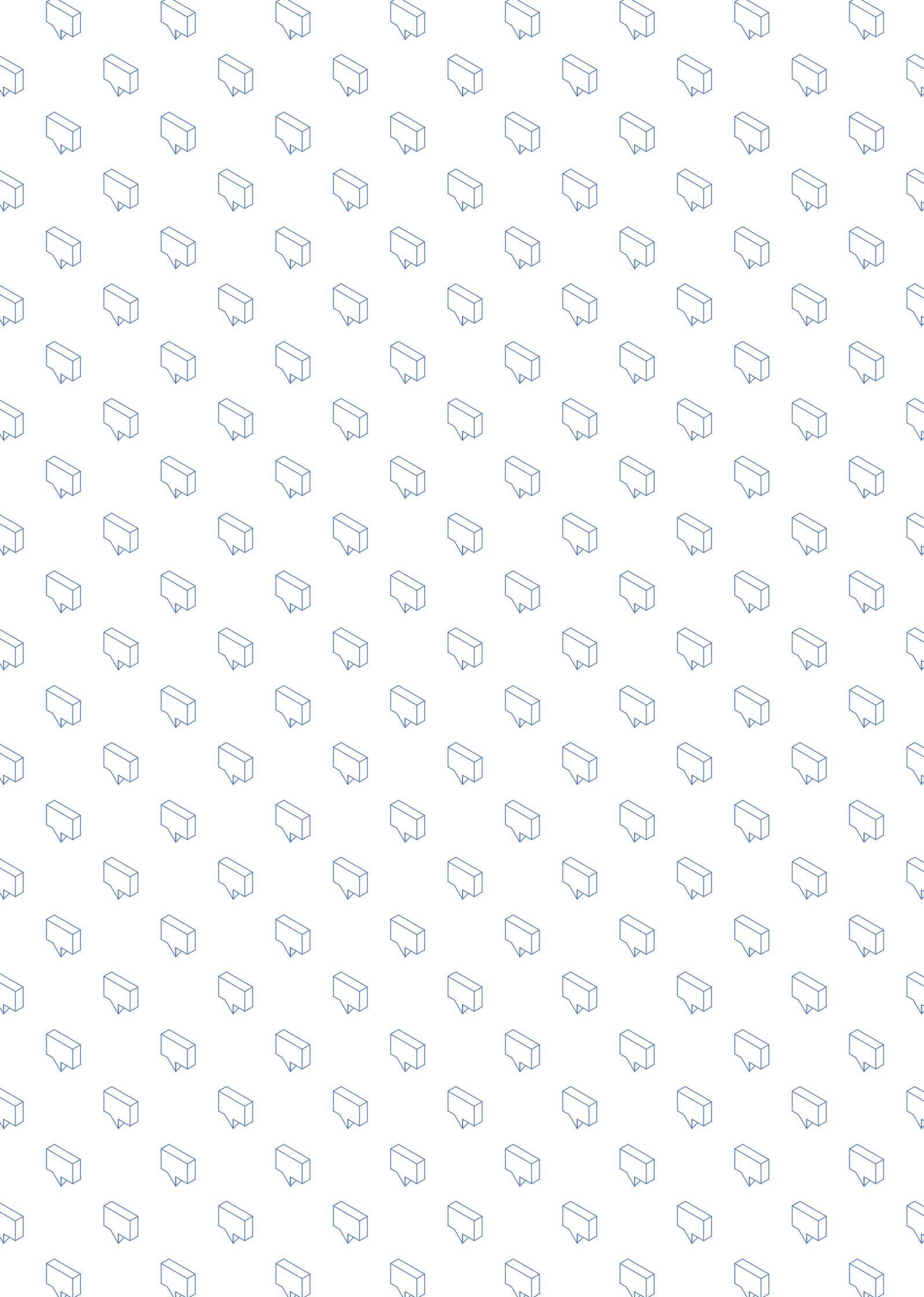


Playing Kind Kingdom will get pupils thinking. Afterwards, use these questions to start a discussion of the game's themes.

- What scenario in Kind Kingdom do you relate to most and why?
- Describe a time when you've taken action to spread kindness to others online.
- In what situation would it be appropriate to block someone online?
- In what situation would it be appropriate to report someone's behaviour?
- Why do you think the character in Kind Kingdom is called a cyberbully?
Describe this character's qualities and how their actions affect the game.
- Does this game change the way you plan to behave towards others?

Discussion questions for younger years

- When would it be right to block someone online?
- When would it be right to tell someone about someone else's behaviour?
- Why do you think that the character in Kind Kingdom is called a 'cyberbully'?
- What's this character like? How does the cyberbully's behaviour affect the game?



When in Doubt, Discuss

A brief guide to encouraging Internet Brave behaviour

Discussion

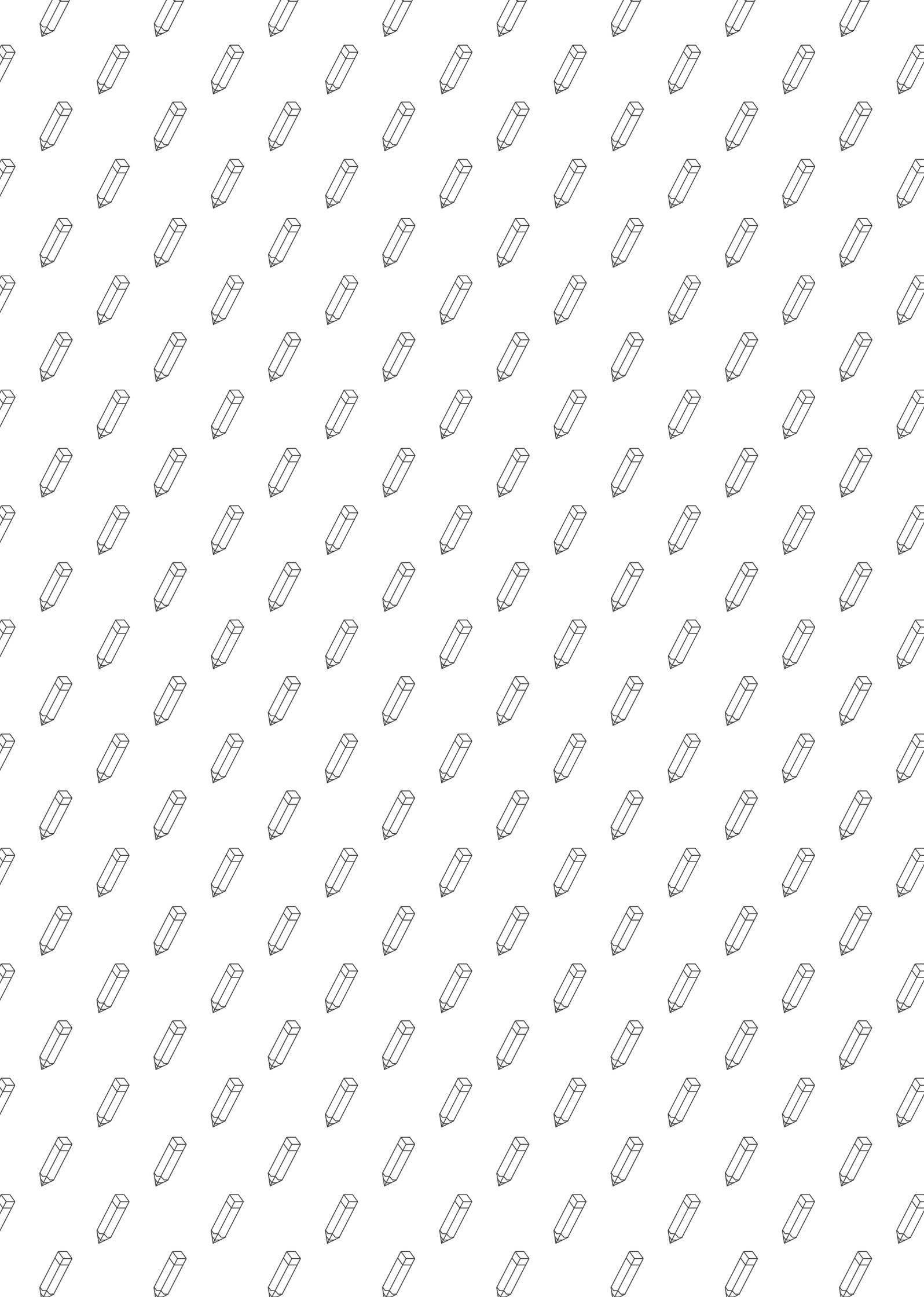
One piece of advice that appears consistently throughout these lessons applies to any online activity: If you come across something confusing or tricky, talk to a trusted adult about it. Pupils should learn this from any one of the lessons, but for quick reference, below is a list of situations in which the 'When in Doubt, Discuss' principle might be most useful to your pupils.

Pupils should talk with a trusted adult whenever they feel the need.

Some common situations include, but are not limited to, the following:

- They suspect that their account may have been compromised.
(Discussion opportunity: What can you do to make your account security even stronger? See page 32.)
- They need help from a trusted adult remembering a password.
- They are unsure whether something is a scam, or suspect they might have fallen for one. (Discussion opportunity: What are the warning signs? See page 19.)
- Someone tries to discuss something online with them that makes them uncomfortable.
- They receive suspicious messages from a stranger.
- They want to discuss online acts of kindness and *unkindness*.
- They are concerned that they may have shared something online that they should not have.

Encourage open communication in your classroom and remind pupils that you're always there for support. Peer-to-peer schemes or student support groups, especially with slightly older students, is one effective way to build student empowerment around this topic.



Be Internet Legends

Lesson plans

Assurance

These detailed lesson plans have been quality assured by the PSHE Association.

Overview

Lesson 1, Be Internet Sharp & Be Internet Alert (for ages 7-9)

Lesson 2, Be Internet Secure & Be Internet Kind (for ages 7-9)

Lesson 3, Be Internet Sharp – Think Before You Share (for ages 9-11)

Lesson 4, Be Internet Alert – Check it's For Real (for ages 9-11)

Lesson 5, Be Internet Secure – Protect Your Stuff (for ages 9-11)

Lesson 6, Be Internet Kind – Respect Each Other (for ages 9-11)

Be Internet Sharp & Be Internet Alert

Overall aims

This lesson plan highlights the age-appropriate activities within the two pillars: 'Be Internet Sharp' and 'Be Internet Alert'. You will find all the activities within the booklet. Please note some of these activities have been adapted for this age group. Please see the lesson overviews within the main booklet for a full description of the overall aims of each pillar. Please make sure the chosen activities are not repeated in years 5-6.

Objectives

Pupils will learn

- How they can protect their online reputation.
- How to work out whether information online is true and reliable.

Outcomes

Pupils can

- Demonstrate ways of protecting their online reputation.
- Identify ways of working out whether information online is reliable.

Reminder

Please make sure you read the teacher guide to pupil safety before you start any of the activities in this booklet.

Assessment opportunities

- Assessing pupils' pre-existing knowledge.
- Class discussion and teacher circulation during activities.

Timing

This plan could be used for a one-hour lesson, with approximate timings given to allow you to select activities as you feel appropriate to meet the needs of your pupils.

Plenary

Pupils reflecting on activities and progress made since introductory activity.

Be Internet Sharp & Be Internet Alert

Baseline activity



(10 mins)

Class discussion around the two pillars 'Be Internet Sharp' and 'Be Internet Alert' to gauge the pupils' starting point.

Explain to the class that someone's online reputation is anything that appears about them on the internet.

Then ask, 'How can someone make sure what they do or say online does not damage their online reputation?'

Examples may include: don't post embarrassing photos or videos online, don't write unkind or hurtful comments and posts online, be kind to others, check privacy settings to make sure people can't see all your personal information.

'Being Internet Sharp' means knowing what kind of information to put online to protect your online reputation.

Explain that today we will also look at 'Being Internet Alert' which means being able to work out whether things we see online are true.

Activity guide



Activity 1: Is it OK to share? (10 mins)

In pairs, ask pupils to invent a character of around their age. Ask them to draw this character or write the character's name in the middle of a piece of paper. Write up a list on the board of a character's 'personal' information (e.g. name, address, photo of a friend, date of birth, password). Ask them to choose those which would help the person to build a positive online reputation. Feed back as a class and ask them to discuss what the consequences of posting or sharing the other examples would be.

Differentiation activities: If pupils need more support, provide them with a list of a character's 'personal' information (e.g. name, address, photo of a friend, date of birth, password). See the support worksheet on page 77. Ask them to say, or to put a smiley or sad face next to each aspect to indicate if it is OK to share this information online or not. If pupils need more of a challenge, ask them to design a poster for the classroom with 'Dos and Don'ts' for a positive online reputation.

Be Internet Sharp & Be Internet Alert

Activity guide



Be Internet Sharp – Activity 4: Keeping it private (10 mins)

Invite pupils to work in groups to review the three written privacy scenarios. Ask each group to discuss and agree upon the best privacy solution for each character.

Privacy scenarios: what should you do?

Example 1: A child at your school has a bad haircut and isn't happy with it. Someone takes a picture and shares it online.

- Is it kind to share another person's bad hair day?
- How do you think that person would feel?

Example 2: Someone writes in their diary. Another person copies what they wrote and posts it online.

- Was the other person wrong to post the diary entries?
- How would you feel if someone did this with your diary?

Example 3: A group of friends decide to meet at a friend's house after school to play video games. One person in the group posts the house address and mobile number of the friend they are going to.

- Can you think of any reason why sharing a home address or a phone number on a public place online could be a problem?
- Are there more private ways to communicate this message – e.g. sending a private message or text?

For each scenario ask: 'Is this OK to share?' For pupils who need more of a challenge, provide them the definition for 'digital footprint' from the vocabulary section and ask how each scenario could leave a negative digital footprint.

Be Internet Sharp – Activity 5: Interland: Mindful Mountain

An online game navigating the world of online privacy. This is followed by a discussion. Please see activity booklet for the questions.

Be Internet Alert – Activity 1: Don't bite that phishing hook! (15 mins)

Divide the class into groups and give each group the examples of messages and websites from the activity booklet. Pupils decide which are real and reliable and which are fake and untrustworthy, giving reasons why.

Differentiation activities: For pupils who need more support, use the real/fake clue cards (you will need to print duplicate copies of these) and ask them to match each card against the scenario they think it belongs to. Discuss the clues to ensure that they understand why the messages could be examples of scams or phishing. For pupils who need more of a challenge, ask them to write their own 'Look out for Phishing!' top five clues checklist.

Be Internet Sharp & Be Internet Alert

Activity guide



Be Internet Alert – Activity 3: Interland: Reality River (20 mins)

An online game navigating the world of online privacy. This is followed by a discussion. Please see booklet on page 27 for the questions.

Plenary

2 for 2 (5 mins)

Ask pupils to spend a few minutes reflecting on the activities in the lesson and ask them to write the following:

- Two things they probably shouldn't share and make public online.
- Two examples of online scams they should watch out for.

(Stretch: ask them to give reasons for their answers)

Extension

Ask pupils to design an advice leaflet or poster based on what they have learned in the activities. They could take this home to their parents to teach them what it means to be 'Internet Sharp' and 'Internet Alert' and tips on how they can achieve this.

Lesson materials

A list of resources needed can be found next to each activity within the booklet.

Be Internet Secure & Be Internet Kind

Overall aims

This lesson plan highlights the age-appropriate activities within the two pillars 'Be Internet Secure' and 'Be Internet Kind' of the Be Internet Legends programme.

You will find all the activities within the booklet. Some of these activities have been adapted for this age group. Please see the lesson overviews within the activity booklet for a full description of the overall aims of each pillar. Please make sure the chosen activities are not repeated in years 5-6.

Objectives

Pupils will learn

- How to make strong passwords to secure their information online.
- Ways in which they can be 'kind' to others online.

Outcomes

Pupils can

- Identify ways in which they can secure their information online by creating strong passwords.
- Identify what they can do to be kind online.

Reminder

Please make sure you read the teacher guide to pupil safety before you start any of the activities in this booklet.

Assessment opportunities

- Assessing pupils' pre-existing knowledge in introductory activity.
- Class discussion and teacher circulation during activities.

Timing

This plan could be used for a one-hour lesson, with approximate timings given to allow you to select activities as you feel appropriate to meet the needs of your pupils.

Plenary

Pupils reflecting on activities and progress made since introductory activity.

Be Internet Secure & Be Internet Kind

Baseline activity



(10 mins)

Protecting my personal information online: how confident am I?

Ask pupils to draw a scale from 0-10. 0/1 representing not at all confident, to 10 representing very confident.

Invite them to mark on their scale how confident they feel in terms of their knowledge and understanding of protecting their own personal information online.

Ask pupils to close their eyes and to put up their hand when you call out where they have rated themselves, 0-3, 4-7, 8-10. This will be re-visited at the end of the lesson.

Ask pupils to discuss in groups why it is important to protect personal information and to write as many reasons as they can on separate sticky notes.

Invite one or two pupils from each group to bring up their sticky note ideas and place on a flipchart/display board.

Summarise and share what pupils have written on their sticky notes.

Possible answers: people may access your home address, phone number, see photos, messages and emails that you don't want made public etc.

Ask the pupils: What is a password and why is it important?

Then say that you're also going to be discussing being kind online. Ask: How can people be kind online? What sort of things might they do?

Be Internet Secure & Be Internet Kind

Activity guide



Be Internet Secure – Activity 1: How to build a strong password (10 mins)

Explain to pupils that one of the ways that can help to ensure personal information is safe online is to use a 'strong' password. Ask them what they think is meant by a 'strong' password. (mix of upper and lowercase letters, symbols, numbers for letters, etc) Divide the class into teams of two pupils.

Each team has 60 seconds to come up with what they think is a 'strong' password.

Ask two teams at a time to write their 'strong' passwords on the board.

Invite the class to vote on which passwords they think are 'strong'. Pupils could also come up with examples of weak passwords and what makes them weak.

Differentiation: Pupils needing support could be given some examples of weak passwords and asked how they could improve them. (e.g 'password' 'school' 'their name') Pupils needing to be challenged could create a 'Dos and Don'ts' checklist on how to write a strong password and give clues to what a weak password would be.

Be Internet Secure – Activity 2: Shh... Keep it to yourself! (15 mins)

- Choose a school device to demonstrate where pupils can locate privacy settings. This can be undertaken on the teacher's class computer and demonstrated via the class whiteboard, via pupils' own school tablets or where laptops are located for lessons in computing.
- Ask pupils if they have heard of the 2-step verification process and explain how it works. (When you log into an account, it will be a 2-step process, i.e. entering a password and another piece of memorable data about you.)
- Demonstrate going into My Account or Settings to explore privacy and security settings and show how privacy can be protected in this way.
- Ask pupils to compose a short slogan which helps them to remember the key advice.

Differentiation: Pupils needing support should be given a one-to-one explanation of the demonstration and could then create a 'Shh.. Keep it to yourself!' cartoon giving key advice, to reinforce their learning. This could be shared on the school website. Pupils needing to be challenged could create a 'Shh... Keep it to yourself!' rule to be shared in assembly. This could take the form of a mnemonic poem or rap.

Be Internet Secure & Be Internet Kind

Activity guide



Be Internet Kind – Activity 3: Taking care of yourself and others (10 mins)

This activity revisits the scenarios in Lesson 1, Activity 4 (Keeping it private), this time focusing on help-seeking.

Give out the three scenarios/dilemmas from Pillar 1, Activity 4 to pupils to be discussed in their table groups.

Key questions to answer are:

- What can the person do if they feel unsafe online?
- Who they can tell or go to?
- What might happen when they tell?
- What might happen after that?

Ask each group to share their responses with the rest of the class.

Differentiation: Ask pupils who need support to discuss the scenarios with you, the teacher, or another adult, focusing on what the person could do if they feel unsafe online and whom they tell in school and outside of school in each case. Ask those that need more challenge to design a 'Who to go to' flyer or poster for display in the classroom.

You could label the corner of each room teacher, parent, no one, CEOP (the Child Exploitation and Online Protection command of the National Crime Agency). Read the scenario and ask pupils to move to the corner for the one they would tell and explain why they chose this option. Key point – you don't tell 'no one' if you see something upsetting!

Be Internet Secure – Activity 4: Interland: Tower of Treasure (20 mins)

An online game where pupils are asked to build an 'untouchable' password and secure made-up 'private' information on the game.

Discuss with pupils: 'How would you find and ask for help if you felt unsafe online?'

Possible answers:

- Reporting
- Blocking
- Speaking to a teacher, parent, friends, sibling or another trusted adult.

Be a 'Kindness Superhero' (10 mins)

Ask pupils to draw someone who treats others kindly when they are online.

Around the outside, ask pupils to draw or write what this person is thinking, saying and doing to demonstrate kindness online. Remind pupils about extending real life behaviour into online behaviour – e.g. don't say things online that you wouldn't say to someone face-to-face.

Be Internet Secure & Be Internet Kind

Activity guide



Be Internet Kind – Activity 1: How can I stand up to others online? (15 mins)

1. Ask pupils to make a circle of words describing feelings for a bystander who has witnessed or read unkind behaviour online.
2. In groups, invite pupils to write down on a sticky note one practical suggestion for what the bystander could do to deal with the situation.
3. Make a class graffiti wall of the suggestions and read them out to the pupils. Which ones do they think would be particularly helpful?
4. Ask pupils to devise their own 'Be cool when someone is cruel' online advice checklist for classroom display.

Differentiation: Pupils needing to be challenged could create a rap/poem to share at a school assembly giving advice on how to combat unkind online behaviour. For pupils requiring support ask them to use the graffiti wall suggestions to compose their own 'Be cool when someone is cruel' advice message or tweet.

Be Internet Kind – Activity 4: Reacting to role models (10 mins)

Class discussion: Ask pupils to consider how some celebrities sometimes behave unkindly towards others when they are using social media. Remind them that this kind of behaviour does not present a good role model for others and only perpetuates that it is OK to be unkind online. As a class they now know how to stand up for others and how to respond to unkind or unhealthy behaviour online.

Be Internet Kind – Activity 5: Interland: Kind Kingdom

Open a web browser on desktop or mobile device (e.g. tablet), visit g.co/interland and navigate to the land called Kind Kingdom. This is followed by the discussion questions in the activity section of the booklet.

Be Internet Secure & Be Internet Kind

Plenary

(5 mins)

Invite pupils to revisit the scale they filled in at the beginning of the lesson. Where would they rate their confidence levels now?

Ask them to list two ways they can be kind online.

Ask pupils to make a poster that can be shared with their parents and siblings. Give them a choice between the two pillars: 'Be Internet Secure' and 'Be Internet Kind'.

1. Poster for 'Be Internet Secure'

Top tips on how to stay secure online. This may include tips on how to create a strong password, what to do if they receive messages from people they don't know and how to manage their privacy settings on an app of their choosing.

2. Poster for 'Be Internet Kind'

Top tips on how to stand up for others and what it means to be kind online.

Extension

These posters could form part of a display in the classroom or elsewhere at school.

Lesson materials

A list of resources needed can be found next to each activity within the booklet.

Be Internet Sharp — Think Before You Share

Reminder

Please make sure you read the teacher guide to pupil safety on the inside cover before you start any of the activities in this booklet.

Timing

This plan could be used for a one-hour lesson, with approximate timings given to allow you to select activities as you feel appropriate to meet the needs of your pupils.

Objectives Pupils will learn

- What having a positive digital footprint means.
- Ways in which they can start to build a positive digital footprint.

Outcomes Pupils can

- Explain what it means to have a positive digital footprint, and why this is important.
- Explain things someone can do to build a positive digital footprint.

Baseline activity



You'll need:

- Pens and sticky notes

(10 mins)

Write the following on the board: Your online reputation is anything that appears about you on the internet.

Then ask, 'How could someone create a positive digital footprint for themselves in order to help protect their online reputation?'

Ask pupils to work in pairs and come up with three suggestions which they write on sticky notes.

Invite pairs to share their responses with their table group. Ask each group to then share with the rest of the class one or two of what they consider to be the most important points about creating a positive digital footprint to maintain their online reputation.

Examples of responses may include: don't post embarrassing photos or videos online, don't write unkind or hurtful comments and posts online, be kind to others, check privacy settings to make sure people can't see all your personal information.

After discussion, reiterate the theme of the lesson: 'Being Internet Sharp means knowing what kind of information to put online to create a positive digital footprint and protect your online reputation.'

Continued on the next page →

Be Internet Sharp — Think Before You Share

Activity guide



Activity 1: Is it OK to share? (10 mins)

In pairs, ask pupils to invent a character of around their age. Ask them to draw this character or write the character's name in the middle of a piece of paper, and around the outside, write or draw 'personal' information about this person. Remind pupils that this shouldn't be real information, or about themselves or anyone they know. Examples of information could include things like favourite foods or colours, names of teddies or toys, silly nicknames, number of siblings, school they go to etc.

When they have finished, ask pupils to look at each piece of 'personal' information and identify whether it is OK to share that information online or not. What effect might sharing have on the character's online reputation?

Differentiation: If pupils need more support, provide them with a list of a character's 'personal' information (e.g. name, address, photo of a friend, date of birth, password) — we have provided a support worksheet on page 77. Ask them to say, or to put a smiley or sad face next to each aspect to indicate if it is OK to share this information online or not. If pupils need more of a challenge, ask them to create two social media profiles of their character: one with personal information that would create a negative digital footprint, and one which would create a positive digital footprint.

Activity 2: Whose profile is this, anyway? (10 mins)

Pupils study a collection of online personal information about three fictitious characters to see what it tells them about each one. Ask pupils to list at least two pieces of personal information they have obtained by reading each character's profile.

On a scale of 1-10, how would they rate their character's digital footprint in terms of risk, both now and in the future?

Discussion: How much can we find out about someone just from what they post online, even if we don't know them?

Differentiation: Pupils who need more support could use highlighter pens to underline the personal information on their sheet instead of writing it out. Pupils who need a challenge could write or prepare to present to the group a short 'future forecast' outlining the possible impact of the information that has been shared on their character's future life.

Activity 3: How do others see us? (20 mins)

N.B this requires the completion of Activity 2 first.

Recap with pupils the possible consequences of their characters sharing more information than they intended to online.

Pupils consider the viewpoints of how other people might view the characters' profiles.

Be Internet Sharp — Think Before You Share

Activity guide



Activity 4: Keeping it private (10 mins)

Invite pupils to work in groups in order to review the three written privacy scenarios.

Ask each group to discuss and agree upon the best privacy solution for each character.

Differentiation activities: Pictures have been provided of each scenario for pupils who need more support. For each scenario ask: 'Is this OK to share?' For pupils who need a challenge, ask how each scenario could damage someone's online reputation, both now and in the future, and how it might leave a negative digital footprint.

Additional activity:

Activity 5: Interland: Mindful Mountain (20 mins)

An online game navigating the world of online privacy. This is followed by the discussion questions in the activity section of the booklet.

Plenary

3-2-1 (5 mins)

Ask pupils to spend a few minutes reflecting on the activities in the lesson and ask them to write down or draw the following:

3. Three ways in which they can create a positive digital footprint.
2. Two ways in which someone can ask for help if they regret posting something online.
1. One question they have – they should be given the opportunity to provide this anonymously.

Extension

Ask pupils to design an 'Internet Sharp' advice leaflet or poster based on what they have learned in the activities. They could take this home to their parents to teach them what it means to be internet sharp with tips on how they can achieve this.

Lesson materials

A list of resources needed can be found next to each activity within the booklet.

Be Internet Alert — Check it's For Real

Reminder

Please make sure you read the teacher guide to pupil safety on the inside cover before you start any of the activities in this booklet.

Timing

This plan could be used for a one-hour lesson, with approximate timings given to allow you to select activities as you feel appropriate to meet the needs of your pupils.

Objectives Pupils will learn

- How to be a critical consumer while online.
- About different online scams, including what 'phishing' means.

Outcomes Pupils can

- Describe ways to critically evaluate what we see on social media.
- Explain how social media can mislead or misrepresent reality.
- Identify different types of online scams people our age may experience, including 'phishing'.
- Identify sources of support for someone who is worried about anything online.

Baseline activity



You'll need:

- Traffic light cards

(10 mins)

Ask pupils to hold up traffic light cards to show how confident they feel about understanding what is true or fake online. (Red – not at all confident / amber – quite confident / green – very confident.)

Write up the following question on the board: 'How can you tell if something you see or read on the internet is fake or unreliable?'

Think, pair, and share. Ask pupils to take one minute to think for themselves and then a few minutes to discuss in pairs. Then spend five minutes discussing as a class and write down what the pupils come up with. Examples may include:

- Pop-ups you didn't click on appear asking for passwords and personal information.
- Weird photos on social media.
- Emails with strange addresses telling you that you've won a prize.

Be Internet Alert — Check it's For Real

Activity guide



Activity 1: Don't bite that phishing hook! (15 mins)

Divide the class into groups and give each group the examples of messages and websites from the activity booklet. Pupils decide which are real and reliable and which are fake and untrustworthy, giving reasons why.

Differentiation activities: For pupils who need more support, use the (real/fake) clue cards (you will need to print duplicate copies of these) and ask them to match each card against the scenario they think it belongs to. Discuss the clues with them to ensure that they understand why the messages could be examples of scams or phishing. For pupils who need a challenge, ask them to write their own 'Look out for Phishing!' top five clues checklist.

Activity 2: Who are you, really? (20 mins)

1. Each group picks a scenario from a container – one person in each group reads it aloud.
2. The group discusses possible responses to the message (and decides on three to six different options.)
3. The group decides on which would be the best option and discusses why they think this.
4. Each group is given the corresponding 'cheat sheet' to match their scenario. They discuss whether they agree with it, and compare it to their group responses.
5. Class feedback – display each scenario on the whiteboard. Each group explains what they decided was the best response and why – the class decide if they agree.

Differentiation: You could give pupils requiring support the differentiated list of scenarios and ask them to give reasons why they think the statements are unreliable (fake). For pupils who need more challenge invite them to create their own advice tips for younger pupils.

Additional activity:

Activity 3: Interland: Reality River (20 mins)

Pupils play the online computer game followed by a discussion using the questions in the activity booklet.

Continued on the next page →

Be Internet Alert — Check it's For Real

Plenary

You'll need:

- Traffic light cards

(5 mins)

Ask pupils to write down one thing they could teach someone else about how to be 'Internet Alert'.

Examples might include:

- I'm going to tell my teenage brother to watch out for emails from an unknown sender telling him he has won an iPad as it's probably too good to be true.
- If you come across a phishing email you should always report it.

Ask pupils to hold up traffic light cards to show how confident they now feel about how to be internet alert and critical of what they come across online. (Red – not at all confident / amber – quite confident / green – very confident). Compare results with the start of the lesson to measure progress.

Extension

Ask pupils to compose a message or tweet for the school website informing their parents of the meaning of 'Internet Alert'. Examples of what to include could be:

- What the key words mean.
- Clues to look out for that something online may not be all it appears.
- How and where to get support if someone is worried about anything they see online.

Lesson materials

A list of resources needed can be found next to each activity within the booklet.

Be Internet Secure — Protect Your Stuff

Reminder

Please make sure you read the teacher guide to pupil safety on the inside cover before you start any of the activities in this booklet.

Timing

This plan could be used for a one-hour lesson, with approximate timings given to allow you to select activities as you feel appropriate to meet the needs of your pupils.

Objectives
Pupils will learn

- Ways to develop safe habits online, including the importance of protecting personal information.
- How to respect online privacy boundaries for themselves and others.
- Ways to seek or ask for help if they or others feel unsafe online.

Outcomes
Pupils can

- Explain why it is important to keep personal information private online.
- Describe ways to keep personal information private online by using safety tools and privacy settings.
- Describe how to find and ask for help if someone feels unsafe online.

Continued on the next page →

Be Internet Secure — Protect Your Stuff

Baseline activity



You'll need:

- Traffic light cards

(10 mins)

Protecting my personal information online: how confident am I?

Ask pupils to draw a scale from 0-10. 0 representing 'not at all confident', all the way to 10 – representing 'very confident'.

Invite them to mark on their scale how confident they feel in terms of their knowledge and understanding of protecting their own personal information online.

Ask pupils to close their eyes and to put up their hand when you call out where they have rated themselves, 0-3, 4-7, 8-10. This will be re-visited at the end of the lesson.

Ask pupils to discuss in table groups why it is important to protect personal information and to write as many reasons as they can on separate sticky notes. Invite one or two pupils from each table to bring up their sticky note ideas and place on a flipchart/display board. Summarise and share what pupils have written on their sticky notes.

Possible answers: people may access your home address, phone number, see photos, messages and emails that you don't want made public etc.

Extension:

Ask pupils, which privacy settings are available to use to keep safe online? Examples could include: secure passwords, privacy settings on social media, 2-step login process.

Activity guide



Activity 1: How to build a strong password (10 mins)

Remind pupils that one of the ways that can help to ensure personal information is safe online is to use a 'strong' password.

Ask them to define what they think are the features of a 'strong' password (mix of upper and lowercase letters, symbols, numbers for letters, etc.)

Divide the class into teams of two pupils.

Each team has 60 seconds to come up with what they think is a 'strong' password.

Ask two teams at a time to write their 'strong' passwords on the board.

Invite the class to vote on which passwords they think are 'strong'. Pupils could also come up with examples of weak passwords and what makes them weak.

Differentiation activities: Pupils needing support could be given some examples of weak passwords and asked how they could improve them. (e.g 'password' 'school' 'their name') Pupils needing to be challenged could create a 'Dos and Don'ts' checklist on how to write a strong password and give clues to what a weak password would be.

Be Internet Secure — Protect Your Stuff

Activity guide



Activity 2: Shh... Keep it to yourself! (15 mins)

- Choose a school device to demonstrate where pupils can locate privacy settings. This can be undertaken on the teacher's class computer and demonstrated via the class whiteboard, via pupils' own school tablets or in the place in school where laptops are located for lessons in computing.
- Ask pupils if they have heard of the 2-step verification process and explain how it works. (When you log into an account, it will be a 2-step process, i.e. entering a password and another piece of memorable data about you).
- Demonstrate going into 'My Account' or 'Settings' to explore privacy and security settings and show how privacy can be protected in this way.
- Ask pupils to compose a short slogan which helps them to remember the key advice.

Differentiation activities: Pupils needing support should be given a one-to-one explanation of the demonstration and could create a 'Shh... Keep it to yourself!' cartoon giving key advice. This could be shared on the school website.

Pupils needing to be challenged could create a 'Shh... Keep it to yourself!' rule to be shared in assembly. This could take the form of a mnemonic poem or rap.

Activity 3: Taking care of yourself and others (10 mins)

This activity revisits the scenarios in Lesson 1, Activity 4 (Keeping it private), this time focusing on help-seeking.

Give out the three scenarios/dilemmas from Lesson 1, Activity 4 to pupils to be discussed in their table groups.

Key questions to answer are:

1. What can the person do if they feel unsafe online?
2. Who they can tell or go to?
3. What might happen when they tell?
4. What might happen after that?

Ask each group to share their responses with the rest of the class.

Differentiation activities: Ask pupils who need support to discuss the scenarios with you, the teacher, or another adult, focusing on what the person could do if they feel unsafe online and whom they tell in school and outside of school in each case. Ask those that need a challenge to design a 'who to go to' flyer or poster for display in the classroom.

Continued on the next page →

Be Internet Secure — Protect Your Stuff

Activity guide



Additional activity:

Activity 3: Taking care of yourself and others (10 mins)

Online game where pupils are asked to build an 'untouchable' password and secure made-up 'private' information on the game.

Discuss with pupils: 'How would you find and ask for help if you felt unsafe online?'
Possible answers: reporting, blocking, speaking to teacher, parent, friends, sibling...

Plenary

(5 mins)

Invite pupils to re-visit the scales they filled in at the beginning of the lesson.

Where would they rate their confidence levels now?

Extension

Ask pupils to make a poster with top tips on how to stay secure online that can be shared with their parents and siblings. This may include tips on how to create a strong password, what to do if they receive messages from people they don't know and how to manage their privacy settings on an app of their choosing. These could also form part of a display in the classroom or elsewhere at school.

Lesson materials

A list of materials needed can be found next to each activity within the booklet.

Be Internet Kind — Respect Each Other

Reminder

Please make sure you read the teacher guide to pupil safety on the inside cover before you start any of the activities in this booklet.

Timing

This plan could be used for a one-hour lesson, with approximate timings given to allow you to select activities as you feel appropriate to meet the needs of your pupils.

Objectives Pupils will learn

- How to develop respectful, empathetic and healthy online relationships.
- Ways to manage and respond in a healthy and safe way to hurtful online behaviour.

Outcomes Pupils can

- Demonstrate ways to build positive and healthy online relationships and friendships.
- Describe strategies they can use to respond to hurtful online behaviour, in ways that keep them safe and healthy.
- Identify sources of support that can help friends and peers if they are experiencing hurtful behaviour online.

Baseline activity



(10 mins)

Be someone who stands up for others.

Ask pupils to draw someone who treats others kindly when they are online. Around the outside, ask pupils to draw or write what this person is thinking, saying and doing to demonstrate kindness. Remind pupils about extending real life behaviour into online behaviour – e.g. ‘don’t say things online that you wouldn’t say to someone face-to-face’.

Ask table groups to share what they have thought and written about. Invite each table group to feedback on one key factor that they felt was most important. Ask pupils to consider:

- Why does kindness matter online?
- What can we do if someone isn’t being kind and is instead being hurtful and unkind?
- Emphasise how it is important to stand up for others, in order to reduce negative and unkind messages online.

Possible answers might include: kindness online matters because being unkind could hurt someone in the same way as it does face-to-face; if someone is being unkind you can report/block/tell a trusted adult.

Continued on the next page →

Be Internet Kind — Respect Each Other

Activity guide



Activity 1: How can I stand up to others online? (15 mins)

1. Ask pupils to make a circle of words describing feelings for a bystander who has witnessed or read unkind behaviour online.
2. In table groups, invite pupils to write down on a sticky note one practical suggestion for what the bystander could do to deal with the situation.
3. Make a class graffiti wall of the suggestions and read them out to the pupils. Which ones do they think would be particularly helpful?
4. Ask pupils to devise their own 'Be cool when someone is cruel' online advice checklist for classroom display.

Extension: Pupils needing to be challenged could create a rap/poem to share at a school assembly giving advice on how to combat unkind online behaviour.

Pupils requiring support: Using the graffiti wall suggestions, ask pupils to compose their own 'Be cool when someone is cruel' advice message or 'tweet'.

Activity 2: Turning negative into positive (20 mins)

A 3-step activity to learn how to reframe negative comments into more positive ones.

1. Ask pupils to read the negative online comments listed on their worksheet.
2. Show the pupils how the first negative comment could be reframed so that it might be more positive/less hurtful to the recipient.
3. Invite pupils to work in pairs in order to reframe the rest of the negative comments into more positive ones.

Differentiation activities: Pupils requiring support: Ask pupils to say or list against each online comment how the person receiving it could respond, i.e. tell an adult in school, report it to CEOP, etc. Pupils needing to be challenged could read through the negative comments on the worksheet and consider how the recipient might be feeling, i.e. sad, angry, upset. Ask them to list the actions they would undertake in response to each situation.

Activity 3: Mixed messages (5 mins)

Invite pupils to consider examples of text messages on the board and ask for volunteers to read out the texts in different tones (angry, sarcastic, friendly) to show that they are difficult to interpret and meanings can be confusing. Ask pupils to consider:

- What do they mean?
- How might the recipient interpret them?
- How could they be better communicated/phrased?

Be Internet Kind — Respect Each Other

Activity guide



Activity 4: Reacting to role models (10 mins)

Class discussion: Ask pupils to consider how some celebrities sometimes behave unkindly towards others when they are using social media. Remind them that this kind of behaviour does not present a good role model for others and only perpetuates that it is OK to be unkind online.

As a class, they now know how to stand up for others and how to respond to unkind or unhealthy behaviour online.

Remind pupils that how they treat each other online will have a big impact on each other and on the digital world. It is in their power to build an internet that is a kind and positive place to communicate and be heard.

Differentiation activities: Pupils requiring support could be given a large selection of emojis that they will need to use to help them be kind online. Pupils needing to be challenged could prepare a short blog on how to be kind online for a publication on the school website.

Additional activity:

Activity 5: Interland: Kind Kingdom

Open a web browser on a desktop or mobile device (e.g. tablet), visit g.co/interland and navigate to the land called Kind Kingdom. This is followed by the discussion questions in the activity section of the booklet.

Plenary

(5 mins)

Revisit the template they filled out at the start of the lesson. Ask the pupils to write around the template with any additional ideas and thoughts they have about how to be kind online. Invite table groups to feedback three key skills that they think they would now use to respond to negative online behaviour.

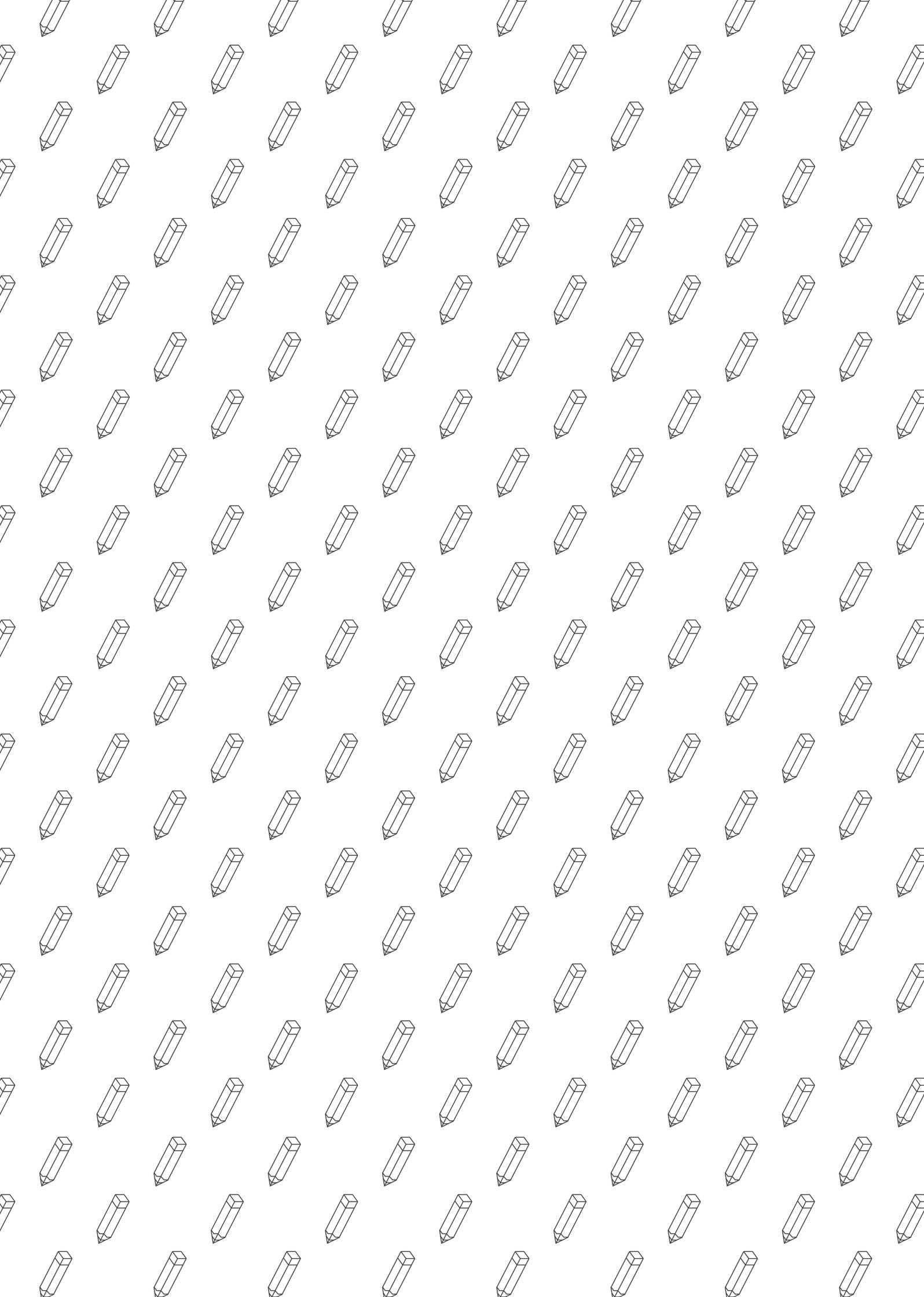
Extension

Ask pupils to design a social media post with top tips for 'How can I stand up to others online?'. One post could be chosen to share on the school social media or in the school newsletter for parents and other pupils. This could include:

- Reporting mean, bullying behaviour.
- Not passing on hurtful messages.
- Setting a good example by being friendly and kind to others.
- Not encouraging nasty behaviour by 'liking' mean posts online.

Lesson materials

A list of resources needed can be found next to each activity within the booklet.



Support worksheets

Assurance

These support worksheets have been quality assured by the PSHE Association.

Overview

Support worksheets, Lesson 1, Activity 1 (Page 77)

Support worksheets, Lesson 1, Activity 4 (Two versions of this for ages 7-9 and 9-11) (Pages 78-79)

Support worksheets, Lesson 2, Activity 1 (Page 80)

Support worksheets, Lesson 3, Activity 1 (Page 81)

Support worksheets, Lesson 4, Activity 4 (Page 82)

Can you avoid oversharing?

Activity



Here is a list of information about Fatima.

1. Put a smiley face next to the things you think it is OK to make public and to share on social media. :-)

2. Put a sad face next to each one you think is private and shouldn't be made public on social media. :-(

- My name is Fatima Turan
- I live at 1234 Brookfield Avenue, Nottingham, UK
- Here is a photo of my friend pulling a silly face (insert photo)
- My date of birth is 23rd August 2003
- The password to my computer is Fatima123
- My locker password is 321
- My cat's name is Fluffy
- I love pop music
- My dad's name is Tariq
- I have three brothers
- My mobile phone number is 123456789123
- I love swimming!
- My favourite football team is Manchester United.

Keeping it private

Look at each image and decide: Is this OK to share? Why or why not? Give reasons.

Activity



Example 1: A child that you know at school has a bad haircut and is quite upset about the way that they look.



**LOL look what Jenny P wrote in her diary!!!
Hahaha HOW SAD!**

"Can't wait until Saturday. No idea what to wear. I really, really hope Ed is coming. I can't stop thinking about him. He is so amazing. I wish he noticed me and wasn't going out with Rihanna! I hate her! I mean why is life so unfair..."

Example 2: Someone writes in their diary. Another person copies what they wrote and posts it online.



**Here's the plan guys.
Meet at Amit's house
after school. 1234
Borrowdale Lane
- call him if you get
lost 01234 543 298
- C U there!!**

Example 3: Someone posts a friend's address and telephone number so a group can meet up to play video games.

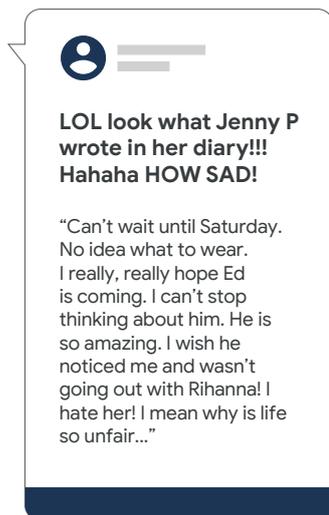
Keeping it private

Look at each image and decide: Is this OK to share? Why or why not? Give reasons.

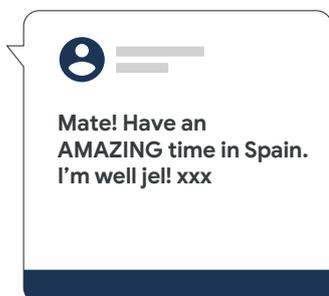
Activity



Example 1: A child that you know at school has a bad haircut and is quite upset about the way that they look.



Example 2: Someone writes in their diary. Another person copies what they wrote and posts it online.



Example 3: Someone posts ‘Have a good holiday’ on a friend’s social media page.

Don't bite that phishing hook!

Activity



Read the following statements and say why you think they may be unreliable if you saw them online.

- Free iPad! Just enter your name and address.
- Pass this email on to everyone you know or you will get bad luck for a month.
- Dear friend. Please can I keep some money in your bank account for a little while? Send me the details and I will pay it in. From Sam.
- Which dog are you most like? Take our test to find out!
- Click here for a free mobile phone.
- Pass this message on to ten friends to win a big prize. Don't break the chain!

How to build a strong password

Activity



Why are these passwords 'weak' and easy to guess?

- Password123
- secret
- keep out
- Rex (pet dog's name)
- SaraAhmed (their own name)

Challenge: Can you make them strong passwords? What could you change or add?

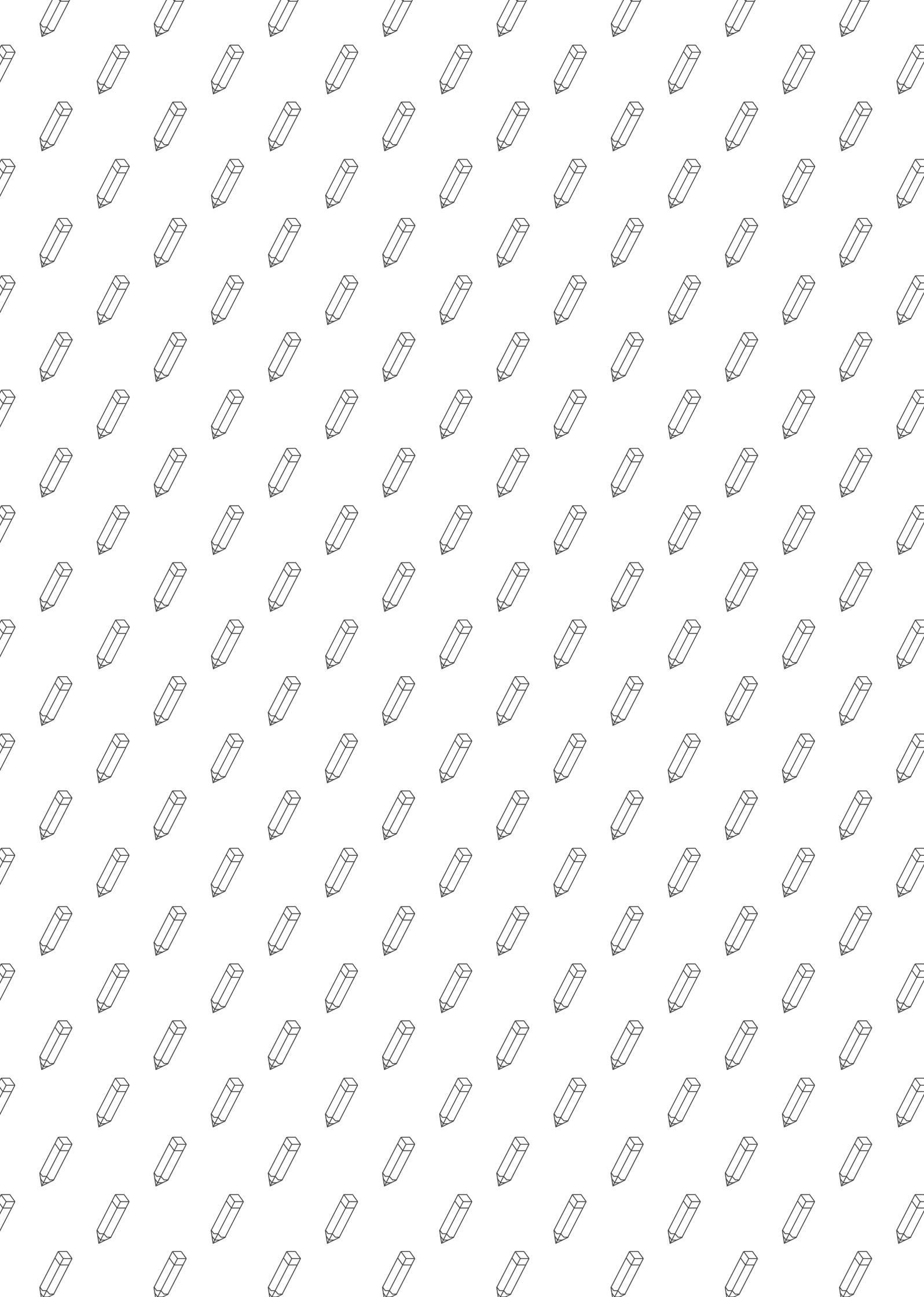
Do as I do, not as I say

Activity



Here is a selection of emojis that pupils could use to help them be kind online.





Be Internet Legends

Pledge & certificate



You're an Internet
Legend



IS AWARDED INTERNET LEGENDARY STATUS

You have proven to be:

- Sharp:** You understand how to share with those you know and those you don't.
 - Alert:** You know how to tell the difference between the real and the fake.
 - Secure:** You create powerful passwords to safeguard important information.
 - Kind:** You positively impact others with kindness and disempower bullying behaviour.
 - Brave:** You know the importance of openly communicating with trusted adults about online activity.
- You are now a safe, fearless explorer of the online world.**

DATE

SIGNATURE



g.co/BeInternetLegends



Be Internet Legends.

Being an Internet Legend means being sharp, alert, secure, kind, and brave. To demonstrate these qualities, I plan to stick to the following guidelines:



Think Before You Share

I will thoughtfully consider what I share and with whom, and keep extra-sensitive information to myself (i.e., home address, current location, other people's business).



Check it's For Real

I will watch out for phishing and scams, and report questionable activity every time.



Protect Your Stuff

I will take responsibility for protecting important information by crafting strong and unique passwords with characters, numbers, and symbols.



Respect Each Other

I will spread positivity and use the skills I have learned to block and report negative behaviours.



When in Doubt, Discuss

I will use my voice when I notice inappropriate behavior and seek out a trusted adult to discuss situations that make me uncomfortable. Because that's what it takes to be a safe and fearless explorer of the online world.

Signed,

_____ ◆ _____ ◆

_____ ◆ _____ ◆



[g.co/BeInternetLegends](https://www.google.com/BeInternetLegends)



This work is licensed under the Creative Commons Attribution 4.0 International License.
To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/> or send
a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

© 2018 Google Inc.