

'CyberSense' – Preventing unwanted or inappropriate behaviour associated with technology
Module 1: Strategies to de-escalate conflict using questions and apologies

Lesson Plan 5:	Spot the Symbol
Resources	'CyberSense' website, smart board, projector & additional activity.
Aim	Pupils should be able to, "Understand the importance of applying security settings on social networking sites and know how to set them". These are requirements set out by OFSTED in the 2013 PSHE report.
Objectives – Pupils will:	<p>Be able to identify safe and unsafe symbols on websites, helping to keep themselves safe online.</p> <p>Discuss the different actions to take when they might find themselves in risky situations online.</p> <p>Understand how to create safe passwords to keep personal information secure when using the internet.</p>
Starter	<p>Click on the 'Phishing' exercise and ask pupils to discuss which of the emails in the inbox are likely to be from trusted sources.</p> <p>Click on the inbox and you will be taken to the 'Prize giveaway' email. Ask a volunteer to read out the message and discuss what to do if you receive an e-mail like this.</p> <p>Ask pupils to discuss whether they would fill in the form and give out their personal details to someone they don't know. Then identify three possible consequences of giving out personal information online.</p>
Introduction	<p>Ask pupils to work in small groups to discuss what actions Kadeem should take in response to abusive posts that other people are placing on his 'wall'.</p> <p>To reveal the abusive posts, click on the 'Is this abuse?' icon.</p> <p>Then click on the actions button to reveal a number of potential actions. In small groups, ask pupils to consider which action might be most appropriate and discuss why they would chose this option.</p> <p>Each group should feedback their answers and discuss why they feel <i>their</i> action is the best one to take in this situation. To develop the discussion further, the teachers notes contain some questions and discussion ideas.</p>
Development	<p>There are 3 activities in this section:</p> <ol style="list-style-type: none"> 1. Click on the 'Unwanted messages' exercise and ask volunteers to read out the text on Kadeem's wall. Ask a pupil to click on the actions button and decide what action Kadeem should take. Would <i>they</i> know how to block someone if they had a profile page? 2. Click on 'safe passwords' and discuss Kadeem's passwords. Decide which one is the safest and why? In groups, create a group password and have a volunteer from each group enter their password into the tool provided. The aim is to see who creates the safest password - which is shown on the monitor on the screen. 3. Next click on 'personal safety', ask a volunteer to read aloud the text in Carl's inbox and then get the class to decide what action Kadeem should take to help keep his personal information safe.
Plenary	<p>In small groups, get the pupils to write down three things they have learnt from the 'Spot the Symbol' exercise. Ask for a volunteer from each group to feedback to the class.</p> <p>To summarise the session, click on 'Kadeem's Tips' to help keep pupils safe online.</p>

Assessment	Observe the discussion and small group work; assessment should focus on pupils' knowledge of safety measures that can be taken in order to stay safe on line. The spot the symbol handout can be used to test pupil's knowledge about which symbols are safe and unsafe online.
Differentiation/ Additional Activity	The 'test an adult' handout is provided as a homework assignment to get pupils testing their parent/carer as well as reiterating what they have learnt from the session.

Teachers Notes –Spot the Symbol

Starter activity – 'Phishing' exercise

Here are points for further discussion concerning the risks of giving personal information to an unknown email/website.

- Why do you think they are asking for your personal details to win access to the game?
- Do you trust the website? If so, why?
- What do you think might happen if you give your personal details to someone you don't know?
- If a stranger asked you, face to face, for personal information such as your address, would you give them it?

Introduction – 'Is this abuse?' exercise:

To develop the discussion further, here are some questions to get the pupils thinking more about the consequences of posting those messages online.

- How do you think the girl in the video felt knowing everyone was making fun of her?
- Why do you think Michael posted the video in the first place? Was it a joke/just a bit of fun? Or do you think he wanted to hurt the girl?
- Could the other people who posted messages be classed as bullies?
- What is the right action for Kadeem to take?
- Would you know where to go to access these actions on this type of website?

'Unwanted messages' exercise:

Points for discussion about knowing how to block someone who is sending abusive messages online.

- Would you know how to block someone?
- What would make you block someone?
- What type of person should you block and why?

Development

'Safe Passwords' exercise:

Questions for discussion to state importance of having a secure password for all accounts.

- Why is it so important to have a secure password?
- Should you use the same password for all your accounts? (email, profile, gaming account)
- What risks could you face if your password is weak?
- How can you make your password more secure?
- What should you never include in your password?

'Personal Safety' exercise:

Would you put the personal statements listed below on your profile page?

Favourite colour	School	Phone number
Full name	Best friend	Photos of yourself/others
Date of birth	Email address	
Favourite song	Favourite food	

After each statement ask the question why you would or would not give this information out for everyone to see online?

Plenary: 'Kadeem's Tips' exercise:

This section is to re-cap the importance of the 'Spot the Symbol' exercise, encouraging pupils to think about each statement and write down what they have learnt from the sessions. Pupils should be able to, "Understand the importance of applying security settings on social networking sites and know how to set them." These are requirements set out by OFSTED in the 2013 PSHE report.