Kit's Digital Detective Mission

1. (A) 'KitFox123' is the safest choice. (3 marks)

Working: Option B uses a name, which is easy to guess. Option C is a common word that hackers can guess quickly. Option A is a mix of letters and numbers, making it harder to guess.

1 mark for choosing A; 2 marks for explaining that it is harder for others to guess than a name or the word 'password'.

2. You should not reply, close the message, and tell a trusted adult immediately. (2 marks)

Look for: The child must identify that they should not share information and should involve an adult.

Good: I would not tell them my name or school.

Better: I would not reply to the stranger and I would tell my teacher or my mum.

Best: I would not reply to the message because it is unsafe. I would tell a trusted adult, like a teacher or parent, so they can help me report the stranger.

What moves an answer up: Moving from 'good' to 'best' requires identifying the action (not replying) and the support system (telling an adult).

3. 1. It keeps you safe from people who might want to find you in real life. 2. It prevents people from using your information to pretend to be you. (4 marks)

Look for: Two distinct reasons relating to physical safety or identity protection.

Good: Because it is dangerous and strangers might come to your house.

Better: It is important because you don't want strangers to know where you live, and your phone number is private information.

Best: You should never share these because strangers could use them to find where you live in real life, and it is important to keep your personal details private to stay safe.

What moves an answer up: Moving up requires explaining the 'why' behind the safety rule rather than just stating it is dangerous.

4. A teacher, a parent, a grandparent, or a guardian. (2 marks)

Working: Any two responsible adults who look after the child.

1 mark for each valid adult mentioned.

5. It is not acceptable because it is unkind and can hurt someone's feelings (cyber-bullying). You should tell the friend to stop, not share the message, and tell an adult. (4 marks)

Look for: Recognition that mean messages are harmful and the need to report or stop the behaviour.

Good: It is mean and you should not do it.

Better: It is not acceptable because it hurts the other person's feelings. I would tell my friend to stop and tell a teacher.

Best: Sending mean messages is a form of cyber-bullying and is very unkind. I would not join in, I would tell my friend it is wrong, and I would report it to a teacher so they can help.

What moves an answer up: Moving up requires identifying the behaviour as bullying and suggesting a proactive, responsible response.

6. Example: 1. Keep passwords secret. 2. Never talk to strangers. 3. Be kind to everyone. 4. Tell an adult if you are worried. 5. Think before you click. (10 marks)

Look for: Five clear, safe, and kind rules for online behaviour.

Good: 1. Don't share passwords. 2. Be nice. 3. Don't talk to strangers. 4. Tell an adult. 5. Stay safe.

Better: 1. Keep your password secret. 2. Never talk to strangers online. 3. Always be kind to friends. 4. Tell an adult if you feel sad. 5. Only use safe websites.

Best: 1. Keep your password a secret from everyone. 2. Never share personal information with strangers. 3. Always be kind and polite to others. 4. Tell a trusted adult if something worries you. 5. Think carefully before you click or share anything.

What moves an answer up: Moving up requires more specific, actionable advice that covers the 'safe and kind' objective.

What a secure answer looks like

A secure answer shows the child understands that the internet is a public space and that their personal

information must be protected. They should be able to identify a trusted adult to report concerns to.

If your child is stuck

Ask the child: 'If you were in a park and a stranger asked where you lived, what would you do?' Then explain that the internet is just like a big, public park.

Common mistakes to watch for

Children often think that if a person is 'nice' in a message, they are safe to talk to. Remind them that anyone can pretend to be anyone online.