

8.2.2 eSafety

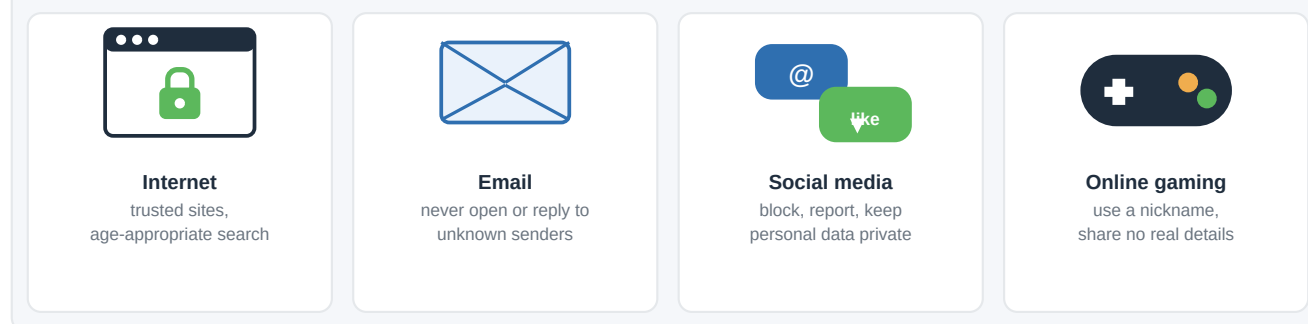
Syllabus 2026 - 2028

WHAT YOU NEED TO KNOW

- The need for eSafety when using the internet, email, social media and online gaming
- How to minimise the dangers of using each of them

eSafety means staying safe when using the internet and online services. People face dangers such as contact with strangers, cyberbullying, inappropriate content, scams, identity theft and malware, so they need to know how to protect themselves.

Figure 31: Staying safe online



Area	Dangers	How to minimise them
The internet	Unsuitable or false content; harmful or fake websites; malware from downloads; giving away personal data.	Only use trusted websites recommended by teachers; use a search engine that only allows access to age-appropriate websites; check the web address and look for https; do not download from unknown sites; do not give out personal data; report anything that upsets you.
Email	Phishing and scams; malware in attachments and links; unknown people making contact; personal data and images being forwarded or intercepted.	Do not open, or reply to, an email from an unknown person; do not click links or open attachments you did not expect; do not send personal identifiable data or images by email, as they can be shared, copied or intercepted; use strong passwords; report and delete spam.
Social media	Contact with strangers who are not who they claim to be; cyberbullying; sharing images that cannot be deleted; loss of privacy.	Know how to block and report unwanted users; keep privacy settings tight; do not meet an online contact face to face (if it ever happens, tell an adult and meet in a public place); do not distribute inappropriate images; do not use inappropriate language; respect the confidentiality of other people's personal data and do not post it.
Online gaming	Strangers and bullying in chat; scams; theft of accounts; spending money by mistake.	Do not use real names; use a nickname and an avatar; do not give out personal or financial data; use strong passwords; do not share your location; block and report abusive players.

General good practice

- Think before you post: anything shared online can be copied and may never be removed
- Keep passwords private and do not share them, even with friends
- Tell a trusted adult if something online worries you
- Keep devices and anti-malware software up to date

EXAM TIP

For each area, give a **danger** and the matching **action**. For example, 'a person may not be who they say they are, so do not meet an online contact face to face'. For email, the key action is not to open or reply to messages from **unknown** people.

Key terms

Term	Meaning
eSafety	Staying safe when using the internet and online services.
Cyberbullying	Using online services to hurt or threaten someone.
Block	Stopping a user from contacting you.
Report	Telling the site or an adult about unwanted behaviour.
Privacy settings	Controls over who can see your information.
Age-appropriate	Suitable for the user's age.
Personal identifiable data	Data that can identify a person.
Inappropriate	Unsuitable or offensive.

Practice questions

Answer each question in full sentences. Command words used: State (give a short answer), Describe (say what it is like), Explain (give reasons), Analyse (break it down and examine it), Suggest (apply your knowledge to a situation), Compare and contrast (similarities and differences), Evaluate (weigh up and reach a judgement).

No.	Question	Marks
1	State two dangers of using social media.	[2]
2	Describe what a user should do if they receive an email from an unknown person.	[3]
3	Explain why real names should not be used in online games.	[2]
4	Analyse the risks of meeting an online contact face to face.	[3]
5	Suggest three ways a learner can stay safe on social media.	[3]
6	Compare and contrast the eSafety risks of email with those of online gaming.	[4]
7	Evaluate the use of a search engine that only allows age-appropriate websites for young learners.	[5]

Total: 22 marks