KS3 Computing: revision notes

Staying safe online

Contents

1. Protecting yourself
2. Online threats
3. Cyberbullying and wellbeing
4. The law
5. Key terms
6. Quick questions
7. What to do next

Protecting yourself

- Keep **personal information** private: your full name, address, school, phone number and passwords.
- Use strong passwords: long, with a mix of letters, numbers and symbols, and a different one for each account. **Two-factor authentication** adds a second check, such as a code sent to your phone.
- Think before you post: your **digital footprint** (the trail of information you leave online) can last for ever. Check your **privacy settings** and turn off location sharing.
- Most social media apps have a minimum age of 13.

Online threats

- **Phishing** is a fake message that tries to trick you into giving personal details. Warning signs: urgent requests, links to log in, odd sender addresses, spelling mistakes and greetings like "Dear customer".
- **Malware** is software designed to cause harm: viruses, spyware, and **ransomware** (which locks your files and demands payment). Don't open unexpected attachments, and keep software updated.
- People online may not be who they say they are. Never agree to meet someone you only know online, and tell a trusted adult if anyone makes you uncomfortable.

Cyberbullying and wellbeing

- If you are cyberbullied: don't reply, save the evidence, block and report the person, and tell a trusted adult.
- Check news with other reliable sources before sharing it; photos and videos can be faked.
- Take breaks from screens.

Your notes

The law

- The **Computer Misuse Act** 1990 makes it illegal to access a computer without permission (hacking), or to change data or spread **malware**.
- **Data protection** laws control how organisations store and use personal data. Guernsey has its own law: the **Data Protection** (Bailiwick of Guernsey) Law 2017.
- Copyright protects people's work: don't copy it without permission.

Key terms

Personal information	Details that identify you, such as your address or phone number.
Digital footprint	The trail of information you leave online.
Phishing	Fake messages that try to trick you into giving personal details.
Malware	Software designed to damage a computer or steal data.
Ransomware	Malware that locks your files and demands payment.
Two-factor authentication	A second check, as well as a password, to prove who you are.
Cyberbullying	Bullying that happens online.
Privacy settings	Controls over who can see your information and posts.
Computer Misuse Act	A law that makes hacking and spreading malware illegal.
Data protection	Laws that control how personal data is stored and used.

Quick questions

Cover the answers and test yourself: remembering is what makes it stick.

1. Which of these is the strongest password?
2. What is phishing?
3. Which of these is a warning sign that a message might be phishing?
4. What is a digital footprint?
5. What should you do if you are cyberbullied?
6. What is malware?
7. What is two-factor authentication?
8. What does the Computer Misuse Act make illegal?

Answers

1. T7#rover!Blue9
2. Fake messages that try to trick you into giving personal details
3. It urgently asks you to click a link and log in
4. The trail of information you leave online
5. Save the evidence, block the person, report it and tell a trusted adult

Your notes

6. Software designed to damage a computer or steal data
7. A second check, such as a code sent to your phone, as well as a password
8. Accessing a computer system without permission

What to do next

Practise 13 questions on this topic

Try 4 exam questions, with mark schemes

Read the lesson, one step at a time

Free revision for GCSE and KS3 at lycolearn.co.uk. Some notes are for one exam board only, and say so in brackets.

Your notes