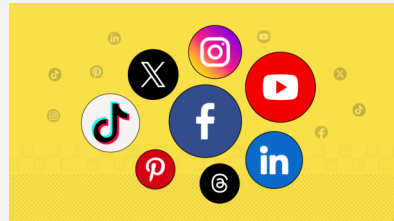




1. Social Media	2. Cyberbullying	3. Email Ettiquette								
<p>Social media is any online platform accessed through an app or website that allows people to communicate with each other and to upload and share content such as posts, comments, videos or images to friends and a wider audience.</p> <p>Most social media platforms have a minimum age, requiring users to be 13 to use them. For some platforms the minimum age might be older.</p> <p>There are billions of people worldwide using social media and so we need to consider carefully what information we share on social media platforms ensuring we also set our privacy settings to allow only the people that we want to see our information, photos and other posts</p> <div></div>	<p>Cyberbullying is the use of the internet on any type of device to intentionally cause someone to feel hurt or distressed. This can include:</p> <ul style="list-style-type: none">• Comments intended to cause upset or embarrassment.• “Hate” speech• Racist or Homophobic messages• Sexual messages• Repeated unwanted communication <p>Cyberbullying is a form of bullying using of digital technologies. It can take place on social media, messaging apps or platforms, live streams, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. It is important that people who feel that they are being harassed or bullied seek support. This could be reporting the activity to the app or platform on which the bullying is taking place such as Instagram, Snapchat or Facebook. Telling a parent or guardian. Telling a trusted adult, this could be any member of staff in school you feel comfortable talking to. You can also tell a friend who then may be able to support you, but it is likely that it will take intervention from an adult in order to make the bullying stop.</p>	<p>It is important to use email etiquette to ensure your email is treated seriously by the recipient and also to ensure that the message or information in your email can be easier to understand.</p> <div><ul style="list-style-type: none">• Include a clear subject line• Always use an appropriate greeting and ending.• Do not use emojis or slang.• Don't hit reply all or CC (Carbon Copy) everyone.• Use BCC (Blind Carbon Copy) not CC when appropriate.• Reply in a timely fashion.• Never use inappropriate language.• Spelling and grammar check.• Add an email signature.</div>								
4. Email Signature	5. Hacking Laws	6. Data Protection Act								
<p>When sending an email it is important that the recipient knows who the sender is. In some cases they may want to check if the email is legitimate before replying. To make it easy to do this it is common for senders to give some information</p> <div><p>In all emails</p><ul style="list-style-type: none">• Include First Name• Include Surname [Last Name]• No Nicknames<p>In a Job:</p><ul style="list-style-type: none">• Include Job title and department• Include employer• Include employer address• Include contact details—email/telephone<p>As a student:</p><ul style="list-style-type: none">• Include your School name.• Include your Class code/Form code.</div>	<p>The Computer Misuse Act (1990) and its amendments were created so that hacking and crimes committed using a computer could be prosecuted. The act is based on three principles and makes the following actions illegal:</p> <table><tr><th>PRINCIPLES</th><th>LEGAL ACTIONS</th></tr><tr><td>Unauthorised access to digital/computer material. This means a person using a computer with the intent of accessing anything for which they do not have permission.</td><td>Punishable by up to 2 years in prison and a £5,000 fine.</td></tr><tr><td>Unauthorised access to digital/computer material with intent to commit or facilitate the commission of further offences. This means a person gaining access to a computer without permission in order to com- mit another crime.</td><td>Punishable by up to 5 years in prison and an unlimited fine determined by the damage caused and the severity of the crime.</td></tr><tr><td>Unauthorised acts with intent to impair the opera- tion of a computer. This means a person intentional- ly impairing the operation of or access to any com- puter, data or program on any computer. This includes creating or supplying materials that could be used to carry out this offence.</td><td>Punishable by a prison sen- tence of up to 10 years and an unlimited fine, but this puts life at risk or endangers national security, the sentence can be life imprisonment.</td></tr></table>	PRINCIPLES	LEGAL ACTIONS	Unauthorised access to digital/computer material. This means a person using a computer with the intent of accessing anything for which they do not have permission.	Punishable by up to 2 years in prison and a £5,000 fine .	Unauthorised access to digital/computer material with intent to commit or facilitate the commission of further offences. This means a person gaining access to a computer without permission in order to com- mit another crime.	Punishable by up to 5 years in prison and an unlimited fine determined by the damage caused and the severity of the crime.	Unauthorised acts with intent to impair the opera- tion of a computer. This means a person intentional- ly impairing the operation of or access to any com- puter, data or program on any computer. This includes creating or supplying materials that could be used to carry out this offence.	Punishable by a prison sen- tence of up to 10 years and an unlimited fine , but this puts life at risk or endangers national security, the sentence can be life imprisonment .	<p>Any organisation which collects and stores your data whether it is a school, a business such as an online store or restaurant, the NHS or even the government, must abide by the a set of principles.</p> <p>We are data subjects (data about us is collected and stored) and the Data Protection Act means we have a right to find out, correct and in some cases delete any information organisations keep on file about us.</p> <div><div><p>Data Protection Principles</p><div><div>Used fairly, openly, and in accordance with the law</div><div>Used for a specific and stated reason</div><div>Used only in a way that is necessary and sufficient for the purpose for which it was collected</div><div>Accurate and up-to-date</div><div>Only kept for as long as it is needed</div><div>Protected against loss, damage, and unauthorised access</div></div></div><div><p>Data Subject Rights</p><div><div>Find out how your data is being used (by an organisation)</div><div>Access the data that an organisation has about you</div><div>Update your data</div><div>Have your data deleted</div><div>Stop an organisation from processing your data</div><div>Transfer your data to a different organisation</div></div></div></div>
PRINCIPLES	LEGAL ACTIONS									
Unauthorised access to digital/computer material. This means a person using a computer with the intent of accessing anything for which they do not have permission.	Punishable by up to 2 years in prison and a £5,000 fine .									
Unauthorised access to digital/computer material with intent to commit or facilitate the commission of further offences. This means a person gaining access to a computer without permission in order to com- mit another crime.	Punishable by up to 5 years in prison and an unlimited fine determined by the damage caused and the severity of the crime.									
Unauthorised acts with intent to impair the opera- tion of a computer. This means a person intentional- ly impairing the operation of or access to any com- puter, data or program on any computer. This includes creating or supplying materials that could be used to carry out this offence.	Punishable by a prison sen- tence of up to 10 years and an unlimited fine , but this puts life at risk or endangers national security, the sentence can be life imprisonment .									

1. Social Engineering	2. Phishing	3. Hacking
<p>Social engineering is a set of methods used by cybercriminals to deceive individuals into handing over information that they can use for fraudulent purposes.</p>  <p>Shouldering (also known as shoulder surfing) is an attack designed to steal a victim's password or other sensitive data. It involves the attacker watching the victim while they provide sensitive information, for example, over their shoulder. This type of attack might be familiar; it is often used to find out someone's PIN at a cash machine.</p> <p>Blagging (also known as pretexting) is an attack in which the perpetrator invents a scenario in order to convince the victim to give them data or money.</p>	<p>A phishing attack is a more complex social engineering attack in which the victim receives an email disguised to look as if it has come from a reputable source, in order to trick them into giving up valuable data. The email usually provides a link to another website where the information can be inputted.</p> <p>Phishing: Key indicators of a phishing email</p> <ul style="list-style-type: none"> • Unexpected email often out of office hours with a request for information • Message may contain spelling & grammar errors • Suspicious hyperlinks in email usually linking to a web address that contains spelling errors and/or lots of random numbers and letters • Text that is hyperlinked to a domain name that you don't recognise and/or isn't connected to the email sender • Generic emails that don't address you by name or contain any personal information that you would expect the sender to know 	<p>Hacking <i>in the context of cyber security</i> is: Gaining unauthorised access to or control of a computer system.</p> <p>More often this will not involve complex software or computing skills and will be as simple as finding someone's password written down and then using it to access their account without permission.</p> <p>Why might people want to hack? To steal data / To disrupt services / For financial gain / For political reasons (espionage and activism)/ For fun (planting the flag) / For ethical reasons</p> <p>Ethical hackers called Pen Testers (Penetration Testers) are often hired by companies to test for vulnerabilities in their computing systems. They will attempt to gain access through methods like looking for computers or accounts which are not secured or do not have up to date security. They may also attempt Brute force attacks and Denial of Service attacks to check how the client's computer system will handle this happening for real</p>
4. Cyber Attacks	5. Malware	6. Protecting your device
<p>Denial of service attack (DoS) This is a cyberattack in which the criminal makes a network resource unavailable to its intended users. This is done by flooding the targeted machine or website with lots of requests in an attempt to overload the system.</p> <p>Distributed denial of service attack (DDoS) This uses the same concept as a DoS attack, but this time it is multiple computers making the attacks at the same time.</p> <p>It is a lot harder to:</p> <ul style="list-style-type: none"> • Stop the attack by simply blocking a single source • Identify who is responsible, as lots of machines are making requests, many of them because they are infected by malware <p>Brute force attack This is a form of attack that makes multiple attempts to discover something (such as a password).</p> <p>Internet bots - Bots are automated programs that perform tasks repeatedly. Not all Bots are harmful, many bots are a crucial part of the internet's infrastructure and perform useful tasks.</p>	<p>Typical actions of malware include affecting the performance of a computer or network by slowing it down, deleting or modifying files. Most malware is distributed via email or as a hyperlink on a website that the user will be tricked to click.</p> <p>Spyware- secretly monitors user actions, and sends information to the hacker. Some spyware can even use your webcam without your knowledge.</p> <p>Keylogger - spyware which records the keys a user presses on a keyboard. This could be a username and password or even messages sent to others.</p> <p>Viruses- spreads through normal programs and might slow down your device or change your applications and documents.</p> <p>Worms- spread from device to device and copy themselves hundreds of times. A worm might copy itself onto your email account and then send a copy to all of your email contacts!</p> <p>Trojan horse- pretends it will be a useful and safe program, when actually it will try to attack your device.</p> <p>Adware- displays adverts while it is running; some can serve as spyware, gathering information about you from your hard drive, the web sites you visit, or your keystrokes.</p> <p>Ransomware- files are deleted or access to systems and accounts denied until the criminal is paid a ransom to secure access.</p>	<p>Firewalls - A firewall checks incoming and outgoing network traffic. It scans the data to make sure it doesn't contain anything malicious and that it follows the rules set by the network.</p> <p>Anti-malware - Often called Anti-virus, this is software that scans any file that is able to execute code. The anti-malware will have a list of definitions of sequences of code that they are aware are malicious. If the code in your files matches the definitions, the files are quarantined.</p> <p>Auto-updates - This refers to software that automatically checks for available updates for the software you have on your computer. Once it finds an update, the software can be set either to alert the user or to install it automatically. This software is often included with an operating system.</p> <p>User permissions - Users on a network can be put into groups, with each group having a unique set of privileges, such as: Which network drives they have access to, Their read/write permissions, Which printers they are able to use, What software they can use, Which websites they are allowed to access</p>