Computing - Online safety

What I should already know: Recognise how social media platforms are used to interact .Understand the purpose of emails Identify reliable information when searching online.Know how to stay safe on social media.Consider the impact technology can have on mood. Know about cyberbullying. Know that not all emails are genuine, recognising when an email might be fake and what to do about it. Understand some of the methods used to encourage people to buy things online.Understand that technology can be designed to act like or impersonate living things.Understand that technology can be a distraction and identify when someone might need to limit the amount of time spent using technology. Understand what behaviours are appropriate in order to stay safe and be respectful online and know different ways we can communicate online.TUnderstand some ways to deal with online bullying. Understand how online information can be used to form judgements. Know that apps require permission to access private information and that you can alter the permissions. Know where to go for support if you are being bullied online or feel that your health is being affected by time online.

Enquiry Questions

What issues online can give us negative feelings and how do I get help?

What is the impact and consequence of sharing online?

How do I create a positive online reputation?

Can I describe how to capture bullying content as evidence?

How do you manage personal passwords effectively?

What strategies can I use to keep me safe online?

Key Vocabulary

Anonymity – someone is anonymous if his/her identity is not known.

Antivirus – software designed to detect and destroy computer viruses.

Biometrics – used to recognize the identity, or verify the claimed identity, of someone. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Block and report – You can stop receiving messages, calls, and status updates from certain contacts by blocking them. You can also report them if you think they are sending problematic content or spam.

Consent – agree

Copy – duplicate

Digital footprint – the information about a particular person that exists on the internet as a result of their online activity.

Digital personality – a term used to describe the idea of an online personal electronic identity. It is the 'you' that others see when they come across the digital footprints you leave behind.

Financial information – information about you financial circumstances (money).

Hacking – the gaining of unauthorized access to data on a computer.

Inappropriate – not suitable

Malware – software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Online bullying - bullying over social media

Online reputation – The things online that you have liked, shared and commented on, as well as what others have shared about you, may shape what other people think about you; this is your online reputation.

Password – a key or a secret codeword or a string of characters, which is used to protect your assets or information from others in the cyber world.

Paste – insert

Personal information –any information that can be used to identify you

Phishing – an attack where cyber criminals act as trusted senders to 'fish' for information.

Privacy settings – controls available on many websites and apps to limit who can access your profile and what information visitors can see.

Private – personal

Reliable source – Capable of being trusted or depended on.

Report – to give a description of something or information about something to someone

Reputation – the general belief or opinion that other people have about you.

Scammers – a person who commits or participates in a fraudulent scheme or operation.

Screengrab – an image that you create by capturing and copying part or all of a television or computer display at a particular moment.

Secure - safe

Settings – A software control panel that enables the user to configure the appearance or actions in an application, operating system or the hardware.

Software updates – A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software.

Two factor authentication - a security system that requires two separate, distinct forms of identification in order to access something.

URL – the address of a given unique resource on the Web.

Username – a special name given to a person to uniquely identify them on a computer network.

Computing Skills:

To know that a digital footprint means the information that exists on the internet as a result of a person's online activity

To know what steps are required to capture bullying content as evidence.

To understand that it is important to manage personal passwords effectively.

To understand what it means to have a positive online reputation.

To know some common online scams.

NC Skill: use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

Before you share online think:
Who do I want to see this?
Do I need to ask someones permission?
Is this something I should be sharing?
Am I sharing something I know is true?

Using avatars, usernames and not sharing personal information are good ways to reduce both your digital footprint and digital personality.

Mr Fox   Alien man   Scrappy   Lollipop

Sometimes things online can make us feel sad, worried, uncomfortable or frightened.

Telling a trusted adult, using privacy settings and blocking/reporting/screengrabbing are some of the ways to get help and make sure any problems online are dealt with in a proper and safe manner.

Sometimes things online can make us feel sad, worried, uncomfortable or frightened.

Telling a trusted adult, using privacy settings and blocking/reporting/screengrabbing are some of the ways to get help and make sure any problems online are dealt with in a proper and safe manner.

SMART

S — Stay Safe
Don't give out your personal information to people / places you don't know.

M — Don't Meet Up
Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.

A — Accepting Files
Accepting emails, files, pictures or texts from people you don't know can cause problems.

R — Reliable?
Check information before you believe it. Is the person or website telling the truth?

T — Tell Someone
Tell an adult if someone or something makes you feel worried or uncomfortable.

Follow these SMART tips to keep yourself safe online!

© Teaching Ideas
www.teachingideas.co.uk

SAFETY
Do not give out your personal details online – such as your name, school, address or phone number.

Not everyone is who they say they are!

Links to other curriculum areas: British values: Mutual respect, Individual liberty