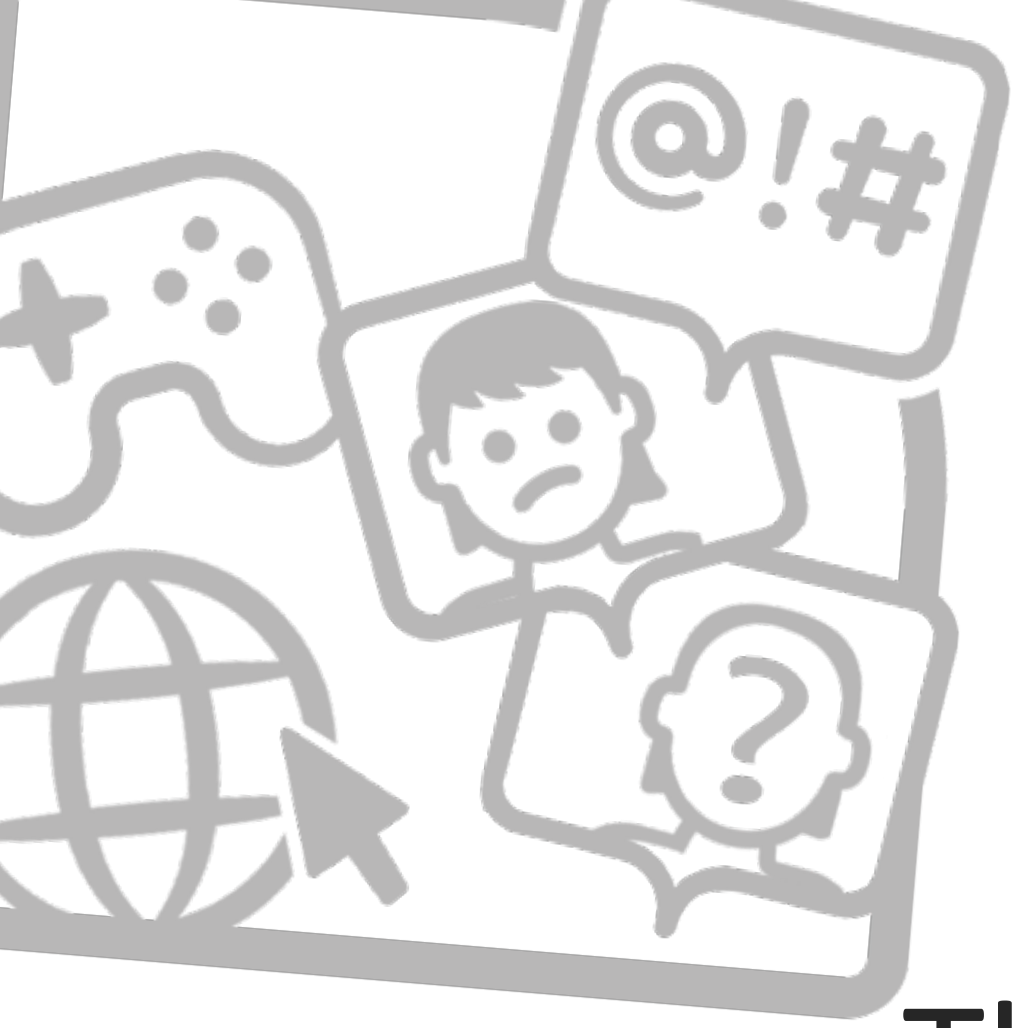

The little **BIG** book of Online Safety Terms

A summary A-Z collection of common Online Safety terminology explained

Children's Safeguarding Assurance Partnership
Blackburn with Darwen - Blackpool - Lancashire

lancashire safeguarding adults board

working together to stay safe online

Edition FOUR - November 2021

Quick Reference:

Jump to...

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	#			

E: graham.lowe2@lancashire.gov.uk

A

Action Fraud: The UK's national reporting centre run by the City of London Police and the National Fraud Intelligence Bureau. Action Fraud provides a central point of contact to report fraud and cybercrime, giving help and advice through specialist advisors.

Address: Usually short for 'web address' – the location for a particular web page on the internet (see also: *URL*).

Advance-Fee Scam: See *'419 Scam'* below.

Adware: Programs which display adverts on a user's screen to influence or encourage purchases.

AMA: (*Ask Me Anything*) A typically informal online Q&A where an individual offers to answer any questions posed on a given topic. Sometimes associated as a factor in Online Bullying.

Among Us: A popular online game where one of the participants is selected to be an imposter whom the other players must defeat in order to win.

Anti-Virus: A program that is used to prevent, detect and remove malware or viruses on a user's computer or mobile device (see also: *malware* and *virus*).

App (Application): A program developed for a specific purpose. Typically installed (downloaded) by a user on a mobile device.

Artificial Intelligence (AI): The use of technology to perform tasks normally requiring human intelligence such as speech recognition systems. Users are sometimes unaware they are interacting with a computer system rather than a human being (e.g. a pop-up 'assistant' on a website).

Attachment: Files such as photos, documents or programs that are typically sent with an e-mail message or social network post. Attachments can be any sort of file and can contain viruses or malware.

Augmented Reality (AR): The use of technology to superimpose a computer-generated image onto a real-world background. An example of AR use is in the popular games Pokémon Go and Wizards Unite.

AUPs: (*Acceptable Use Policy*) A set of rules commonly associated with establishments such as schools that identify the Do's and Don'ts when using the equipment and services provided.

Avatar: An image or icon often associated with online gaming used to represent the user (see also: '*gamertag*').

B

Bitcoin: A popular cryptocurrency which can be traded or used to purchase items without using traditional banking services (see also: *crypto*).

Blacklist: A term used to describe a list of undesirable or blocked websites, apps or keywords.

Bloatware: Typically used to describe software seldom used when compared with the excessive storage demands on a system. Usually associated with software pre-installed by manufacturers to ship with new devices which slows down the new system's performance.

Block: Usually associated with Social Media to prevent someone from contacting an individual or viewing their profile.

Blog: A personal webpage or website where an individual (blogger) regularly gives their opinions or provides information on a given topic (see also: *vlog*).

Bluetooth: A wireless method used to exchange data over short distances, typically from mobile devices.

Bookmarks: Also referred to as '*favourites*', a list of commonly used web addresses stored in a browser, enabling the user quickly access specific websites or pages.

Bot: A (web robot) program that performs functions without requiring a user to give it instructions. Bots can be malware, installing on a system or device without the user's permission and may be remotely controlled over the internet and used to steal information or send spam (see also: *malware*).

Broadband: A relatively high-speed connection to the internet. Broadband connections are typically 'always on' so a device is connected to the internet whenever it is used.

Browser: A program that allows a user to use (browse) the world wide web to view web pages and sites. Common browsers include Internet Explorer, Microsoft Edge, Google Chrome, Safari and Firefox.

C

CAIC: A term used to refer to Child Abuse Images and Content. Such content should never be referred to as 'child porn'.

Catfishing: A deceptive activity using a fake online presence to pretend to be someone else. Typically used on social networks or dating websites to defraud a victim or commit identity theft.

CEOP: (Child Exploitation and Online Protection centre). An organisation within the National Crime Agency which helps to protect children and young people from sexual abuse and grooming online.

Chatroom: A place on the internet where users can chat or interact with one or more people by typing messages. Chatrooms can be both moderated (i.e. content is supervised) and unmoderated.

Challenges (Online): Viral online challenges ranging from fun 'dares' to more dangerous activities or sinister 'scare stories' which can be extremely upsetting for children. Typically circulating via Social Media, scare stories in particular often gain notoriety and attention by individuals sharing and raising awareness as a concern, inadvertently exacerbating the issue (i.e. Think Before You ~~Share~~ Scare).

Clickbait: Online content purposely designed to attract users to click a link for further details. Often in the form of a misleading or surprising headline, by clicking on the link, the user generates income for the site.

Computer network: A number of computers linked together to allow an exchange of data. It may be in a single location or building (Local Area Network (LAN)) or over a large geographic area (Wide Area Network (WAN)).

Console: A dedicated system usually connected to a screen (e.g. TV or monitor) typically used for playing games. Consoles can also be smaller, handheld mobile devices with a built-in screen.

Content filter: A way of restricting access to content on the internet. Content filters use algorithms to examine a site's content before assigning it to a category which is then allowed or blocked depending on the policy applied. Often used in establishments such as schools to help reduce potential access to inappropriate sites.

Cookie: A small file that is sent by a server and stored on the user's computer when browsing a website. Cookies can be read by the server each time the user revisits the website and are used to keep track of personal preferences and other data such as login information.

COPPA (Children's Online Privacy Protection Act): US legislation regulating the collection of data by US-based companies on children under the age of 13.

Creeping: A term used to describe the act of following a person's social media activity to an excessive degree (see also: *stalking*).

Crypto: A broad term typically used to describe cryptocurrencies – digital currency which can be traded or used to buy goods or services (see also: *bitcoin*).

CSAP (Children's Safeguarding Assurance Partnership): Replacing the former LSCBs, CSAP works with partner organisations such as the Police, Health and Local Authorities to support and improve

safeguarding outcomes for children and young people across the Blackpool, Lancashire and Blackburn with Darwen region.

Cyberbullying: Bullying behaviour which takes place online, typically through the use of social media platforms or text messages. The most commonly raised concern by children and young people in relation to online safety.

D

Dad-dancing: A typically disparaging or humorous term used to describe someone (typically an adult) who is attempting to appear knowledgeable or in-touch with current trends but not succeeding.

Dark Patterns: A phrase used to describe a range of online marketing techniques sometimes used to encourage website visitors to make purchases (e.g. '*only 4 items left*') (see also: *Persuasive Design*).

Dark Web: An area of the wider internet often associated with illegal content or criminal activity.

Data Bleed: Information which is shared (often unknown to the user) between one platform and another, typically through installing third-party apps or games on a social network or by signing in to one app using the login from another app (e.g. '*Sign in using Facebook*').

DDoS (Distributed Denial of Service): A malicious attempt to make an online service or website unavailable to users by overwhelming it with traffic from multiple sources.

Deepfake: An image or video that has been digitally altered using Artificial Intelligence to provide a realistic, convincing representation of an individual not in the original media.

Digital Footprint: The information about an individual that exists online. Often referred to as the trail we leave behind when we use online services.

Decoy app: Sometimes referred to as '*secret*' or '*ghost*' apps, Decoy apps are used to store private information such as photos, videos or

messages. They appear like a normal everyday app (e.g. calculator) but offer a way to hide information users may not want to be seen by others.

Download: The transferring of a file from one computer system or server 'down' to a user's device.

Doxxing: Used to describe the practice of researching the internet to collect personal or private information on an individual or organisation and subsequently publishing with malicious intent.

E

E-commerce: Buying or selling items or services over the internet (e.g. online shopping).

Earworm: A term used to describe a song or piece of music that continuously occupies a person's mind long after it was originally heard.

Echo Chamber: See '*Filter Bubble*' below.

EFACW (Education for a Connected World): A framework from UKCIS identifying expected levels of knowledge at differing ages around the online environment. The framework provides a series of progressive statements across 8 strands which can be used to benchmark or plan online safety education for pupils and students (see also: *'EVOLVE' & 'UKCIS'*).

E-mail: A method of communicating over the internet. E-mail messages are written by one person and then sent to another (one or more people) using a dedicated program (e.g. outlook, gmail).

E-mail address: The address used by an e-mail system to send and receive e-mail messages (e.g. mailboxname@providername.com).

Encryption: The process of encoding data (e.g. messages, website traffic) to prevent unauthorised interception.

E-Safety: See *'Online Safety'* below.

Emoji: A set of icons (e.g. smileys) used to express moods or feelings when included in messages, often used in place of older 'text-speak' acronyms (e.g. lol).

Ephemeral (content): A collective term used to describe content that is temporary in nature such as '*self-deleting*' or '*time-limited*' messages or images sent on social media platforms.

EVOLVE (Project): Based around the EFACW framework, Project EVOLVE is a suite of freely-available education resources developed by the South West Grid for Learning used to teach a variety of online safety themes and topics in an age-appropriate and progressive way (see also: *EFACW*).

Extremism (online): The use of the online environment to post hateful or extreme content which typically supports or encourages terrorism and/or violent extremism (see also: *Radicalisation*).

F

Facebook: A highly-popular social networking platform where users can create an online profile and share updates, pictures, videos and messages. Users can also 'friend' other users and chat with those using the same platform through the *Facebook Messenger* service.

Fake News: Typically disparaging colloquial term often used to describe or denounce a range of untrue, unreliable or misleading statements or information.

Family agreement: An agreement between family members setting out expectations about the use of the online environment including devices, time online and expected behaviour.

Favourites: Website addresses stored in a browser for quick access, allowing a user to go directly to common or regularly visited web pages – also referred to as 'bookmarks'.

File/s: Data stored on a computer or device. Files can take a variety of forms such as a document, videos, pictures or music.

Filter Bubble: A term used to describe the effect of online bias provided by newsfeeds or opinions. Social network algorithms provide content personalised to the user which can give a one-sided, unbalanced or biased view of a topic (sometimes referred to as an online *'echo chamber'*).

Firewall: A software program or piece of equipment that provides a virtual barrier to help prevent malware or hackers from accessing an individual's system via the internet.

Flag: To highlight or report online content to site owners, moderators or the Police.

Flaming: Sending an inflammatory or aggressive message over the internet likely to cause offence or create argument.

Follow: A method used to remain updated or keep in contact with someone on Social Media platforms such as Twitter. Similar to subscribing to a Vlogger's YouTube channel.

FOMO (Fear Of Missing Out): The pressure or anxiety typically associated with Social Media that events or discussions may be happening that an individual is not involved with or aware of. Often associated with the perceived need for individuals to always be connected online (see also: *peer pressure*).

Fortnite (Battle Royale): A hugely popular, free-to-play online survival game released in July 2017, involving 100 players competing to be the last-person-standing in player-versus-player combat.

Forums: An online discussion group (chat room) typically surrounding a particular topic, event or viewpoint.

Friending: Adding someone to a list of friends or contacts on a social networking site, often associated with Facebook. By '*friending*' someone online, it often gives them certain privileges such as accessing an individual's online profile not available to others (see also: *Profile*).

Full Fact: An independent charitable organisation providing a useful web reference facility. Full Fact is often referred to when checking the

veracity or reliability of claims or news stories (e.g. viral scare stories, political claims) (see also: *Fake News*). https://fullfact.org/

G

Gamertag: An alias or identifier used in online games to represent the player.

Gaming: The activity of playing video games using a computer, dedicated console or hand-held device. Most modern games include an online element allowing play and communication with other players (see also: *console*).

Ghosting: Relating to dating, the practice of ending a relationship abruptly by withdrawing from all communication with the former partner (e.g. not replying to messages or phone calls).

Google: The world's most popular search engine used to find content on the web (see also: '*search engine*').

GPS: (Global Positioning System) Used by Smartphones and Satellite Navigation Systems to identify a user's location. The facility is often used by apps to determine where a user is located and co-ordinates can be included with an image when taking a photograph with a GPS-enabled device.

Griefer: A gaming term used to describe a player who purposely harasses or upsets other players (i.e. to cause 'grief') within a game (see also: *troll*).

Grooming: When a perpetrator attempts to develop a relationship with a child or young person for unlawful purposes such as sexual exploitation or radicalisation. Perpetrators may focus on vulnerabilities or insecurities and it can happen online, offline or be a combination of both (see also: *online grooming*).

H

Hackathon: A term referring to a limited-time activity (e.g. 24/48 hours) where individuals come together to collaborate and focus on solving a particular problem.

Hacker: Individuals or groups who attempt to gain unauthorised access to computer systems/data. Typically done remotely online via the internet using a computer or mobile device.

Hardware: The physical components of a device, computer system or network.

Hashtag: Used to describe an unspaced phrase or word prefixed with the hash symbol # (e.g. #worldcup). Commonly used on social media platforms such as Twitter or Instagram to tag or group messages around a common theme (see also: *trending*).

History: The record within an internet browser that shows which websites have been visited and when.

Hits: Used to describe the number of times a website, webpage or content (e.g. online video) is visited/viewed by users.

Homepage: The main or front page that first appears when accessing a website, often described as a website's 'shop window'. Also used to describe the default website displayed when first opening the internet browser on a system.

HTTP / HTTPS: Used as a prefix to a url (web address), HTTP (HyperText Transfer Protocol) is the set of rules determining how website information is formatted and transmitted across the world wide web. The addition of an 'S' to HTTP indicates a Secure connection.

I

Icon: Usually a small picture used to identify an app or a file on a device or computer's screen.

Identity Theft: The practice of impersonating someone else, often to pursue financial gain, by utilising personal details collected about an individual.

IMEI number: A unique 15-digit identifier on mobile devices. Used by mobile providers to block and prevent network access when a mobile phone is reported lost - important to make a record of.

In-app purchases (IAP): A method of allowing users to purchase virtual items, typically within a game. In order to generate revenue, 'free' games will usually include in-app purchasing for additional 'in-game' items or to enable further progress.

Influencer: A term used to describe an online personality or celebrity who can influence perceptions, views or decisions (e.g. purchases) through social media due to their large number of online followers.

Information Privacy: A term used to describe a variety of principles and practices to keep personal information private (e.g. *be careful what you share, never give out your password*).

Instagram / Insta: A popular social media app typically used to share information, pictures and video content with an online community.

Internet: A global inter-network of computers providing a platform for various information and communication facilities, the world wide web being one of the services that runs across it.

Internet Service Provider (ISP): A company that provides connectivity to the internet.

Intimate Image Abuse: A term often used in place of 'revenge porn' to describe the sharing or uploading of sexually explicit images or videos without the originator's consent (see also: *revenge porn*).

IP address: An IP (Internet Protocol) address is a unique series of numbers (separated by full stops) used to identify individual computers connecting across a network.

IRL: A shortened term for In Real Life (see also: *offline*).

iTunes: Apple's online e-commerce site which provides games, movies, music and apps that can be purchased, typically for use on an Apple device (e.g. iPhone, iPad).

J

Jumpscare: Commonly associated with horror movies (and more recently online games), *Jumpscares* are a means of frightening an individual by an abrupt, unexpected change in image on screen often accompanied by a startling sound to make the observer 'jump'.

Junk Mail: Unwanted or unsolicited e-mail messages typically in the form of advertising or marketing. It is estimated that Junk or Spam e-mail messages account for almost half of all e-mail traffic worldwide (see also: *spam*).

K

Kbps: The speed of a connection measured in the number of kilobits sent per second (kilobits – a thousand bits). As speeds increase, Kbps is increasingly replaced by Mbps (megabits – a thousand kilobits) or Gbps (gigabits – a thousand megabits).

L

Lag / Lagging: A term typically used in online gaming to describe a slow connection that has a negative effect on play.

Link: Shortened term for 'hyperlink' – a formatted word or phrase on a website or in a document that by clicking or tapping on, will open a specific webpage or file. Links are often displayed as underlined or coloured text.

Likes: An expression of approval used on social media. Often used as an acknowledgement rather than an explicit show of approval.

Livestream: A method of sharing video content in real-time. Video is broadcast live from a device as it is recorded (see also: *streaming*).

Log off/out: A term used to describe disconnecting from a computer, network, service or app.

Log on: A term used to describe connecting to a computer, network, service or app, typically through the use of a username and/or password in order to identify the user.

Login: A login is a name used to identify to a computer, website, service or app who you are, usually combined with a password.

Loot boxes: A virtual reward system in online games. Typically containing random items, Loot Boxes can be purchased and offer a *chance* of obtaining additional in-game items. Concerns are often linked to suggestions of being a form of online gambling.

M

Malware: Shortened term for 'malicious software' used to collectively describe a variety of undesirable programs that can display unwanted advertisements (adware), steal private information (spyware), expose a system to hackers (trojans) or damage a computer (viruses).

Meme: A typically humorous or amusing image, text or video clip shared rapidly across internet users. The medium can be an existing or well-known image, video or text which is altered for humorous effect.

Metadata: A term used to describe 'data about data'. Metadata can be used to provide information about a website or image which is used by search engines to provide relevant results to search queries (e.g. context, author, image size, subject).

Millennial: A term used to describe someone typically born during the 1980s or 1990s - Millennials are generally identified as someone who has grown up with technology with the Internet and Social Media forming part of their lives from an early age (sometimes used in the context of being a '*Digital Native*').

MMS: Multimedia messages sent and received by a mobile device, typically pictures and videos (See also *SMS*).

Moderator: A moderator (often shortened to 'mod') ensures that activity or comments on a platform (e.g. forum) abide by the terms and conditions of use. Moderators can be a person or a program (Artificial Intelligence) that will take action where the rules are broken (e.g. swearing/offensive language). Not all platforms are pro-actively monitored and may rely on users flagging or reporting issues which a moderator subsequently (re-actively) investigates (see also: *flag*).

MyAdvice: A wide-scale, schools-based engagement activity by Lancashire Safeguarding Boards to secure the views and opinions of Children and Young People about the online world. The collated views inform future development to support keeping children safe online.

N

Navigation: The way of moving around a website. The quality of a website is often determined by how easy it is to navigate and find the information required.

NCSC (National Cyber Security Centre): The UK's technical authority for cyber threats, providing cyber security guidance and support for the public and private sector.

Net: A colloquial term or abbreviation of 'internet' (see also: *internet*).

Netiquette: A term used to describe the accepted conventions for online interaction, esp. those surrounding e-mail or messaging (e.g. typing in CAPITALS is interpreted as being LOUD or SHOUTING).

Network: Computers or devices linked together to exchange data (see also: *computer network*).

Noob / Newbie: A (typically derogatory) term associated with online gaming to describe a new or inexperienced player.

Nudes: A term sometimes used by young people when referring to *'sexting'* images (see also: *Sexting*).

O

OCSE: An abbreviation used to denote Online Child Sexual Exploitation.

Offline: A term used to describe when a person is not connected to the internet, often used in the context of 'in real life' (irl) – e.g. to meet a person offline is to meet them in person.

Online: Used to describe when a person is connected to the internet or currently interacting on a social media platform or game. Research suggests young people increasingly view less of a distinction between the online and offline worlds in comparison to adults.

Online Grooming: A core risk area of online safety used to describe the process by which perpetrators use the internet to befriend and subsequently exploit children or young people for sexual purposes (see also: *grooming*).

Online Safety: The general description given to refer to staying safe in the online environment. Replacing the outdated term 'e-safety', it is often used to encompass the variety of potential risks associated with being online. In the context of safeguarding, it is a key aspect typically defined as '*a safeguarding issue where technology is involved*'.

Operating System: The main software that controls the operation of a computer or device and manages other programs or apps. The most common operating systems are Microsoft Windows, Apple's Mac OS/iOS and Android.

Overlay: A term sometimes used to describe an app whose main purpose may not be immediately obvious to the user. Used in a marketing context, an *overlay* may provide a specific function whilst

its underlying purpose is to generate business or collect data from the user.

P

Parental Controls: A variety of options typically used to monitor or restrict access by children and young people to undesirable apps, games or websites. Parental controls can also be used to manage time spent online when using mobile devices and gaming consoles or to control the availability of internet access in the home environment.

Patch: A term used to describe an update to an app, piece of software or operating system to improve its functionality or security.

Password: A secure word, phrase or series of letters/numbers/characters known only to an individual. Passwords are used to restrict access to a computer, device or network and in conjunction with a username, are used to access an online account or platform such as social media or a secure website.

Peer Pressure: The perceived need to conform or behave in-line with others within a particular social group in order to be popular or gain respect (see also: *fomo*).

PEGI: (Pan European Game Information) – similar to the system commonly associated with film classification, PEGI ratings are the system used in the UK for games, using age ratings of 3, 7, 12, 16 & 18. PEGI also uses 'content descriptors' which provide information about the content of the game such as whether it contains violence or bad language (e.g. Minecraft has a PEGI rating of 7).

Permissions: The settings used to allow or block an app or service access to (often personal) data on a device - e.g. Apps on smartphones may request access to a user's location data or phone contacts in order to provide personalised content.

Persuasive Design: A practice often used by designers of social media, games or apps to influence user behaviour to use the

platform on a regular basis. Examples of *Persuasive Design* may include rewards for consistent use or penalties should the user not use the platform daily. Often cited as a contributor in online 'addiction' (See also: '*Streaks*' & '*Dark Patterns*').

Pharming: A fraudulent scam (pronounced 'farming') used to get personal/private information. The scam involves unknowingly re-directing users from a genuine website to a 'spoof' duplicate site which is used to extract confidential (typically financial) information (See also: *phishing*).

Phishing: A scam (pronounced 'fishing') intended to mislead individuals into revealing confidential information such as bank details or passwords. Typically done via e-mail, the intended target may be offered a financial incentive (e.g. tax refund) and encouraged to claim with a link to a fraudulent (and often convincing) site set up to impersonate a genuine website (See also: v*ishing*).

Photoshop: Originally industry-standard graphics editing software, the term is also often used colloquially as a verb to describe the practice of editing images or *selfies* to change the subject's appearance.

PIES (framework): A widely-recognised framework model to support addressing interrelated aspects of online safety with a cohesive approach (Policies; Infrastructure; Education; Standards).

Policy (Online Safety): A collective set of principles, rules and expectations about how online safety will be addressed in an organisation. Policies will often contain additional appendices addressing specific aspects such as escalation procedures, incident logs and acceptable use/behaviour agreements. Effective online safety policies should be aligned with the organisation's broader Safeguarding Policy (see also: *AUPs*).

Post: To contribute to a conversation on social media or in an online forum.

POSH: (Professionals Online Safety Helpline) – a dedicated helpline from the South West Grid for Learning providing online safety guidance and support to professionals working with children and young people.

Private browsing: Private (or incognito) browsing is a function within web browsers which allows users to privately browse the web without creating a record of which sites have been visited (see also: *history*).

Prevent (Duty): UK Government strategy placing a responsibility on a range of public-facing bodies to have due regard to the need to prevent people from being drawn into terrorism. A growing aspect of the broader radicalisation/extremism agenda involves the use of technology for unlawful purposes (see also: *radicalisation*)

Profile: A set of information about an individual typically used on social networking platforms. A profile will typically include general information intended for others to see about the individual such as a username and general interests but should avoid providing too much personal information that could be used to identify them such as the person's location or date of birth.

PvP (Player versus Player): A term used to describe games in which players compete against other (human) players in a multi-player environment (as opposed to a player versus computer-controlled opponent).

Q

QR Code: Functioning similar to a bar code, a QR Code is a series of black and white squares which can be quickly read by suitable apps on a smartphone. QR Codes are often used to represent a web link and can typically be found in magazines or on advertising boards.

QuickTips: A series of useful CSAP animations covering a variety of topics including Privacy & Security, Frauds & Scams and Online Shopping.

R

Radicalisation: A term used to describe the grooming or influencing of an individual to support extremist views or ideologies. Indicators of online radicalisation have some similarities with those aspects of online grooming more typically associated with online child sexual exploitation (see also: *extremism*).

Raging: A term associated with online gaming to describe inappropriate behaviour or a loss of temper, usually after losing in a game.

Ransomware: A type of malicious software used to infect a computer or device to render it unusable until the user pays a fee (see also: *malware*).

Ratting: (Remote Access Trojan) Malware typically used by criminals to record or take control of a user's computer or mobile device.

Remote Learning: The use of a range of online platforms to provide an alternative to (or complement) traditional face-to-face learning activity, typically using video conferencing features (see also: *Teams & Zoom*).

Report Remove: A highly-recommended tool from the IWF and Childline that enables young people to discretely self-refer nude images or videos of themselves for removal from the internet.

Revenge Porn: The illegal posting or sharing of sexual or intimate (adult's) content without the subject's consent with the intent to cause distress or embarrassment (see also: *Intimate Image Abuse*). The term should not be used in relation to content involving children or young people.

RHC (Report Harmful Content): A national reporting helpline supporting users over the age of 13 in reporting harmful content online.

Router: A device that connects other devices (e.g. tablets, smartphones, computers) to an internet-enabled connection, often providing WiFi connectivity in the home.

S

ScamSmart: A national campaign from the Financial Conduct Authority (FCA) to provide information and guidance on how to avoid pension and investment scams.

Search engine: A website, such as Google, which enables users to search for websites or information about a particular topic. Restrictions can be applied to search engines such as Google that will help to reduce (though not remove entirely) potentially inappropriate websites.

Security updates: New or updated versions of software or operating systems to improve or fix issues and vulnerabilities that have been found. It is important to install recommended security updates as soon as they are released to prevent hackers or malware from taking advantage of the vulnerabilities identified (see also: *patch*).

Selfie: A term used to describe a 'self-portrait' photograph often taken at arm's length distance.

Server: A system that manages a network or website to provide users with webpages or files requested.

Sexting: A term used to describe the sending or receiving of sexually explicit photos, messages or videos, typically on a mobile device such as a smartphone using a social media platform such as Snapchat, WhatsApp or Instagram. Also referred to as '*nudes*' or '*nude selfies*'.

SGII: (*Self-Generated Indecent Images*) Acronym used to refer to indecent sexualised images taken by an individual of themselves, either voluntarily or through coercion.

Sharenting: The practice of Parents proudly sharing pictures or videos of their children via their Social Media accounts, thereby

putting them in the online world at increasingly younger ages without choice. The term is also associated with the over-sharing of such pictures, messages or clips to a point of annoyance to other users.

Skin: A design used to customise the appearance of something such as a website, social media profile or gaming character/equipment.

Skin Gambling: A term used to describe exchanging virtual items acquired in games (e.g. skins) in return for virtual coins/credits used to place bets on games of chance.

Skype: A popular online program used to have conversations across the internet using VOIP technology, either through a voice/chat function or by videos (see also: *voip*).

Social Media: A collective term used to describe websites and applications which enable users to interact, network and share content (see also: *Social Networking*).

Smart devices: A term used to describe an increasing variety of devices in the home that connect over the internet to share or interact with its user and/or other devices. Common examples include laptops, computers, smartphones, tablets, smart TVs and gaming consoles.

Smartphone: A mobile phone that as well as making calls and texts can also perform many of the functions more commonly associated with a traditional computer such as browsing the web, playing games or downloading/using apps and programs.

SMART Rules: A set of useful online safety principles or themes used to support staying safe online (Safe; Meeting; Accepting; Reliable; Tell).

SMS: Acronym used in place of 'Short Message Service', more commonly referred to as texts (see also: *text*).

Snapchat: A popular social networking app that allows users to send photos, videos or messages to contacts. Photos can be set to 'self-delete' which can often engender a false sense of security when

sharing images. The 'Snap Maps' feature allows others to see the user's current location on a map.

Social Networking: The practice of connecting, communicating or interacting online with other individuals or groups, typically through a Social Media platform (see also: *Social Media*).

Software: Programs or code that run on a computer or device to perform a function.

Spam: Originally used to describe unsolicited or junk e-mail messages sent en-masse to a large number of recipients without their consent. Spam has evolved to also describe comments or adverts on social media promoting products or services (see also: *junk mail*).

Spear-fishing: A malicious targeted form of *phishing* attack. *Spear-fishing* is targeted at specific individuals or organisations to gain unauthorised access to sensitive information and is typically in the form of an e-mail or message from an apparently genuine or trusted source (see also: *phishing*).

Spyware: A term used to describe a malicious program that actively monitors activity without the user's knowledge to collect personal information and/or record actions or online activity (see also: *malware*).

Stalking (cyber): The practice of following or harassing someone using technology causing distress or mental trauma. Stalking may occur in a variety of ways including through social media or location services on smartphones.

Stranger danger: A message or phrase typically associated with online grooming warning about the dangers of chatting with unknown people online who may intend causing some form of harm to a child (see also: *online grooming*).

Streaks: A feature on Snapchat whereby users are rewarded for exchanging snaps (i.e. messages, photos, videos) with friends on consecutive days - as *streaks* get longer, users are rewarded with special emojis. A long *streak* is often perceived as a sign of good

friendship but should a consecutive snap not be sent, the entire streak is lost (see also: *Persuasive Design*).

Streaming: A method of listening to music or viewing films, videos or television programmes online from a streaming service.

Surf: A term used to describe browsing content or sites on the world wide web (i.e. '*surf the web*').

Swiggle: A popular child-friendly search engine from SWGfL often used with younger children as a recommended alternative to Google or Bing.

T

Tablet: A portable device larger than a smartphone used to go online. An iPad is an example of a tablet.

Tag: A method used to identify or include people in posts or photos on social media platforms such as Facebook.

Teams: A popular collaboration tool from Microsoft allowing users to host virtual meetings or remote learning events online using video conferencing technology (see also: *Remote Learning*).

Text: A short name for text messages sent from a mobile phone (see also: *SMS*).

Text-speak: An older term used to describe shortened words or acronyms used in messaging, esp. teenagers (e.g. lol (laugh out loud), pos (parent over shoulder), brb (be right back) – see also: *emoji*).

Third-party applications: Apps or programs not included with a host program (e.g. operating system), which are developed by another organisation or individual. They can be downloaded and installed from a vendor such as iTunes or Google Play to add additional functionality.

TikTok: Formerly called *Musical.ly*, TikTok is a highly popular social media platform allowing users aged 13+ to interact, create, share and view video clips of up to 3 minutes duration.

Trend / Trending: A description used when a topic becomes highly popular online (see also: *hashtag* and *viral*).

Trojan: An example of malware, a trojan is a program disguised as something else which subsequently performs a malicious function such as installing spyware or accessing files (see also: *malware*).

Troll: A term used to describe someone online who deliberately posts offensive or inflammatory comments in order to upset or obtain a reaction (see also: *griefer*).

Ts & Cs: (Terms and Conditions of use) – the rules of use for an app, website or service which users are required to agree to. Typically includes what personal information the app/site collects and how it may be used by the service provider.

TUK (ThinkUKnow): A useful educational website provided by CEOP providing advice, guidance and resources for children, parents and professionals to support keeping children safe online (see also: *CEOP*).

Twitch: A popular live-streaming platform often used by gamers to share gameplay as it happens which others can view and comment on in real time.

Twitter: A popular social media platform where users can send and receive 'tweets' (short messages) which are limited to 280 characters or less.

Two-Factor Authentication (2FA): Sometimes referred to as two-step verification, 2FA is a security process whereby two different authentication methods are required to access an account or app. 2FA may take the form of requiring a Password plus a multi-digit Code sent to the user's mobile device.

U

UKCIS (UK Council for Internet Safety): Formerly UKCCIS (UK Council for Child Internet Safety), UKCIS is a collaboration between the

government, tech industry representatives and other organisations to work collectively towards improving online safety in the UK.

Upload: The opposite of download - to copy or send information or files from one device 'up' to another device or platform connected to the internet (see also: *download*).

URL (Uniform Resource Locator): More commonly referred to as a web address, a URL is the address which links to a specific webpage on the internet. e.g. the URL for Lancashire Safeguarding Boards is www.lancashiresafeguarding.org.uk

USB (Universal Serial Bus): A type of physical connection on many devices often associated with USB storage drives as a method to transfer files between devices. Often cited in organisations as a potential means to transfer computer viruses or malware.

V

Video hosting sites: Dedicated websites allowing users to upload or view (stream) media clips such as movies or music videos. Popular video hosting sites include YouTube and Vimeo.

Viral: A phrase used to describe the rapid and wide sharing or vast popularity of a topic, video clip, story or message across the online environment, esp. through social media. (see also: '*trending*')

Virtual: A term used to describe a simulation or online representation of something in the real world.

Virtual Reality / VR: A term often associated with the use of a dedicated headset to simulate an immersive, 3-dimensional experience. Often cited as the next step in online interactions, moving from existing (flat) 2-D screens towards immersive, 3-D technologies.

Virus: A piece of malicious software that causes harm to a system or device such as deleting files or taking over a computer. Anti-virus software can help to protect systems along with appropriate

behaviour such as using reputable or trusted websites (see also: *anti-virus*).

Vishing: Similar to 'Phishing', Vishing involves the use of phones (Voice) to call potential victims to fraudulently obtain private details such as account details or passwords to be used for financial gain (see also: *Phishing*)

Vlog: Video content published on social media (e.g. YouTube) on a regular basis by an individual (or vlogger) or brands. Popular individual vloggers are also referred to by children and young people as 'YouTubers' (see also: *blog*).

VoIP: A term (Voice over Internet Protocol) used to describe making a telephone (voice) call over a network such as the internet (see also: *Skype*).

VPN: Virtual Private Network – a means of creating a secure (encrypted) 'tunnel' through the internet.

W

Walled Garden: A means of allowing access to only pre-approved content or websites. Often used to help protect younger children when introducing them to the online world (see also: *whitelist*).

Web: An abbreviation for the World Wide Web (see also: *www*).

Web page: A single page on a website displayed using an internet browser (see also: *website*).

Webcam: A camera that is either plugged in or built into a device which allows images and videos to be shared across the internet. Smartphones typically have in-built cameras which enable them to be used to take pictures or videos, particularly for use on social media platforms (see also: *livestream*).

Website: A term used to describe a collection of web pages on a site. Websites can provide a variety of functions and can take a variety of

forms e.g. games, news, information, video, educational, reference etc (see also: *web page*).

WhatsApp: A highly-popular messenger app for smartphones owned by Facebook, using the internet to send/receive messages, images or video.

Whitelist: A term used to describe a list of approved websites users are allowed to access (see also: *blacklist*).

WiFi: A wireless network allowing users to wirelessly connect to the internet. Typically preferred on mobile devices as images and video can use substantial amounts of a user's data allowance.

Wiki: A website or page that allows users to contribute content (usually information) in collaboration with others (e.g. Wikipedia). Whilst the information is typically moderated by a user community, it is user-generated and therefore should not be assumed to be definitive or unbiased.

Worms: A piece of malicious code that reproduces itself on a system in order to spread around computers or a network (see also: *malware*).

WWW (World Wide Web): An online service which runs across the internet, allowing users to create webpages/sites which are stored on web servers (see also: *internet*).

X

XRW: (*Extreme Right Wing*) Online content associated with criminal activity motivated by political or cultural viewpoints including Racism, Extreme Nationalism, Fascism and Neo-Nazism.

Y

YouTube: Extremely popular video hosting site owned by Google containing a variety of commercial and user-generated content across

a vast variety of topics. Often used as a tool to research information (e.g. *How to fix…*). (see also: *vlog*).

Youtuber: See *'Influencer'* above.

Z

Zipit: A useful app created by Childline which aims to help young people deal with challenging sexting or flirting situations, providing humorous responses to help to stay in control.

Zoom: A popular video conferencing system allowing users to host virtual meetings or remote learning events online (see also: Remote Learning).

#

2FA: See '*Two-Factor Authentication*' above.

3C's: A thematic approach to identify online risks (Content; Contact; Conduct). Sometimes includes reference to a 4th 'C' - Commercialisation.

3G: Third generation – a fast mobile connection allowing phone users to access the internet where slower connections would prove difficult (e.g. making video calls).

4G: Fourth generation – an even faster mobile connection approaching similar speeds to that typically found on home broadband connections.

5G: Fifth generation – a superfast mobile connection offering much faster connections than previous versions.

419 Scam: A common online scam promising the victim a share of a large sum of money in return for a small up-front fee. Often referred to as an 'advance-fee scam'.

7MB (7-minute briefing): A series of extremely popular safeguarding summary briefings developed by the Children's Safeguarding

Assurance Partnership and Lancashire Safeguarding Adults Board to introduce a snapshot overview of a specific safeguarding topic.

---

www.safeguardingpartnership.org.uk/online/resources/

E: graham.lowe2@lancashire.gov.uk

Children's Safeguarding Assurance Partnership
Blackburn with Darwen - Blackpool - Lancashire

lancashire safeguarding adults board

working together to stay safe online