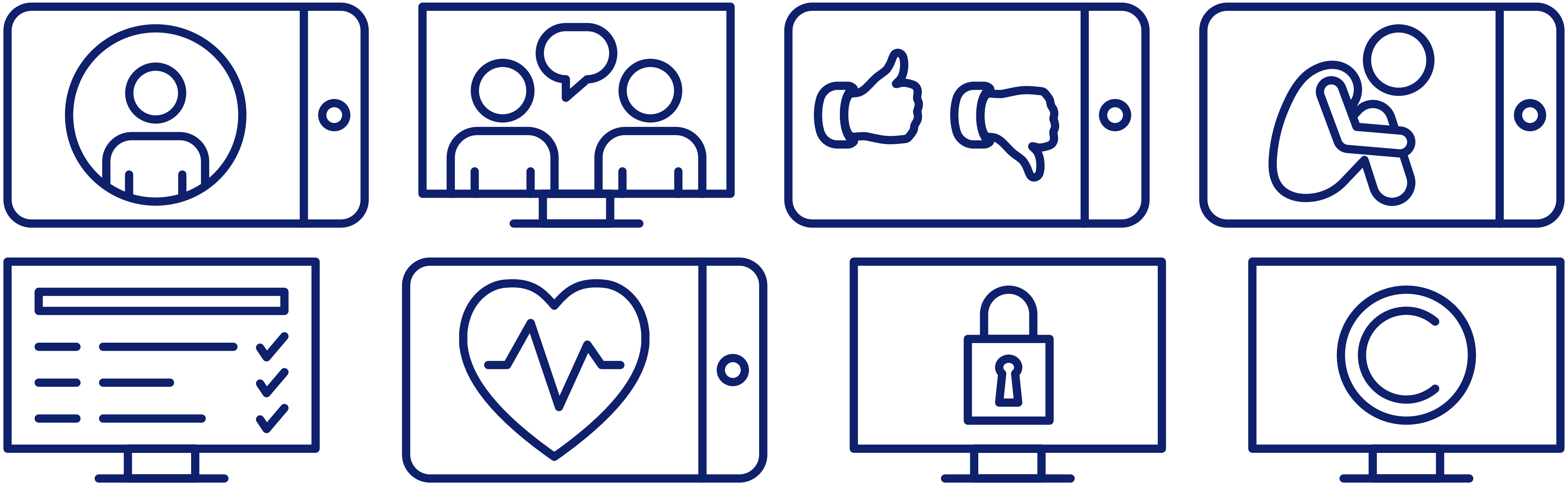
Education for a Connected World – 2020 edition

A framework to equip children
and young people for digital life



UK Council for
Internet Safety

Introduction to the 2020 edition

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage.

As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.

This framework describes the knowledge, understanding and skills that children and young people should have the opportunity to develop at different ages and stages. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, how to get support, and what skills they need to be able to navigate it safely.

Children and young people's online activity and behaviour can be different both within and across an age range. This framework is intended to be used flexibly in order to support learning that is relevant to children and young peoples' online behaviour and experiences and matched to their readiness for new learning.

Since the publication of the first edition of the framework in 2018 the introduction of new statutory subjects in all English schools has elevated the status of much of the knowledge young people will require from September 2020.

This edition expands learning outcomes related to understanding, respecting and protecting individual autonomy, the right to give or withhold consent and repositions some outcomes in response to new behaviours related to safeguarding.

Aims of the Framework

Education for a Connected World is a tool for anyone who works with children and young people. It enables the development of teaching and learning as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world.

It focuses specifically on eight different aspects of online education:

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

The framework aims to support and broaden the provision of online safety education, so that it is empowering, builds resilience and effects positive culture change. The objectives promote the development of safe and appropriate long term behaviours, and support educators in shaping the culture within their setting and beyond.

The status of this framework for English schools

From September 2020 Relationships Education and Relationships and Sex education will be compulsory for all secondary aged pupils in England and Relationships Education for all primary aged pupils in England. Health Education will be compulsory for all pupils in state-maintained schools. PSHE is already compulsory for Independent Schools[1].

Much of the specific knowledge young people will need to enable them to live safely and thrive online are identified throughout these new statutory subjects. It is important to ensure that factual knowledge is set within learning that provides a broader understanding of the digital world and the development of digital skills.

In 2019 the Department for Education produced non-statutory guidance 'Teaching online safety in schools – Guidance supporting schools to teach their pupils how to stay safe online, within new and existing subjects'[2]. This guidance makes extensive reference to this framework as a tool to support realising this outcome.

It is essential that education young people require to thrive in the digital environment is planned across the entire curriculum and as part of a whole school approach to digital learning and online safety.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805781/Relationships_Education__Relationships_and_Sex_Education__RSE__and_Health_Education.pdf
[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

Using Education for a Connected World

School leaders, teachers and other members of the children's workforce can use this framework for a wide range of purposes, including:

- Developing a rich, effective and developmental curriculum, which will support young people to be safe, healthy and thriving online
- Auditing and evaluating existing provision of online safety education
- Coordinating delivery of online safety education throughout the curriculum
- Improving engagement across the wider school community on issues related to online safety
- Developing effective training for staff and governors / board members

Online safety is a whole school issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education, Relationships and Sex Education, Health Education and Computing. It is designed, however, to be usable across the curriculum and to be central to a whole school approach to safeguarding and online safety.

About us

The framework has been developed by members of the UKCIS Education Working Group.

UKCIS is a group of more than 200 organisations drawn from across government, industry, law, academia and charity sectors working in partnership to help keep children safe online.

The UKCIS Education Working Group brings together leading organisations in online safety in education and the group focuses on how education settings in the UK are responding to the challenges of keeping their pupils safe online.

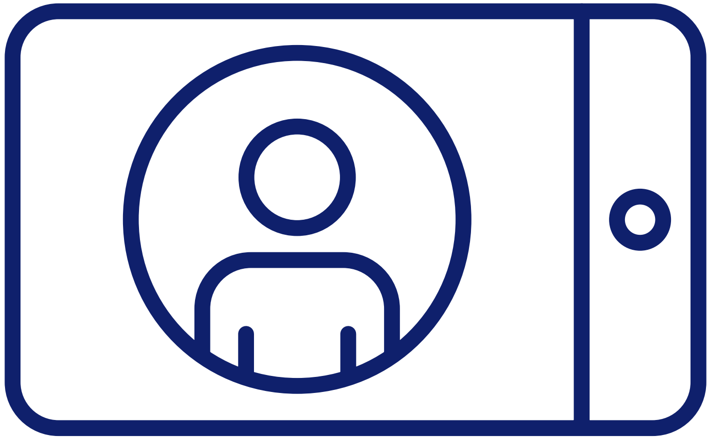
Feedback and development

Education for a Connected World is a working document and we would appreciate your feedback. You can report on your use of the framework and your online safety education needs by completing **this survey**.

Acknowledgements

UKCIS would like to thank members of the Education Working Group who have contributed significant time and expertise to the development of Education for a Connected World.

Many thanks to Common Sense Education for agreeing to the use of topic headings in their Digital Citizenship Curriculum as a source for the structure of the current Framework.



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes.

It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Self-image and identity

I can recognise, online or offline, that anyone can say ‘no’ / ‘please stop’ / ‘I’ll tell’ / ‘I’ll ask’ to somebody who makes them feel sad, uncomfortable, embarrassed or upset.

I can recognise that there may be people online who could make someone feel sad, embarrassed or upset.

If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust and how they can help.

I can explain how other people may look and act differently online and offline.

I can give examples of issues online that might make someone feel sad, worried, uncomfortable or frightened; I can give examples of how they might get help.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner’s experience and are achieved through learning that is matched to the readiness of the learner.

4 - 7

Self-image and identity

I can explain what is meant by the term ‘identity’.

I can explain how people can represent themselves in different ways online.

I can explain ways in which someone might change their identity depending on what they are doing online (e.g. gaming; using an **avatar**; social media) and why.

I can explain how my online identity can be different to my offline identity.

I can describe positive ways for someone to interact with others online and understand how this will positively impact on how others perceive them.

I can explain that others online can pretend to be someone else, including my friends, and can suggest reasons why they might do this.

I can explain how identity online can be copied, modified or altered.

I can demonstrate how to make responsible choices about having an online identity, depending on context.

I can identify and critically evaluate online content relating to gender, race, religion, disability, culture and other groups, and explain why it is important to challenge and reject inappropriate representations online.

I can describe issues online that could make anyone feel sad, worried, uncomfortable or frightened. I know and can give examples of how to get help, both on and offline.

I can explain the importance of asking until I get the help needed.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner’s experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11

Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online relationships

I can recognise some ways in which the internet can be used to communicate.

I can give examples of how I (might) use technology to communicate with people I know.

I can give examples of when I should ask permission to do something online and explain why this is important.

I can use the internet with adult support to communicate with people I know (e.g. video call apps or services).

I can explain why it is important to be considerate and kind to people online and to respect their choices.

I can explain why things one person finds funny or sad online may not always be seen in the same way by others.

I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. (e.g. email, online gaming, a pen-pal in another school / country).

I can explain who I should ask before sharing things about myself or others online.

I can describe different ways to ask for, give, or deny my permission online and can identify who can help me if I am not sure.

I can explain why I have a right to say 'no' or 'I will have to ask someone'. I can explain who can help me if I feel under pressure to agree to something I am unsure about or don't want to do.

I can identify who can help me if something happens online without my consent.

I can explain how it may make others feel if I do not ask their permission or ignore their answers before sharing something about them online.

I can explain why I should always ask a trusted adult before clicking 'yes', 'agree' or 'accept' online.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

4 - 7

Online relationships

I can describe ways people who have similar likes and interests can get together online.

I can explain what it means to 'know someone' online and why this might be different from knowing someone offline.

I can explain what is meant by 'trusting someone online', why this is different from 'liking someone online', and why it is important to be careful about who to trust online including what information and content they are trusted with.

I can explain why someone may change their mind about trusting anyone with something if they feel nervous, uncomfortable or worried.

I can explain how someone's feelings can be hurt by what is said or written online.

I can explain the importance of giving and gaining permission before sharing things online; how the principles of sharing online is the same as sharing offline e.g. sharing images and videos.

I can describe strategies for safe and fun experiences in a range of online social environments (e.g. **livestreaming**, gaming platforms).

I can give examples of how to be respectful to others online and describe how to recognise healthy and unhealthy online behaviours.

I can explain how content shared online may feel unimportant to one person but may be important to other people's thoughts feelings and beliefs.

I can give examples of technology-specific forms of communication (e.g. **emojis, memes and GIFs**).

I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my / our fault.

I can describe some of the ways people may be involved in online communities and describe how they might collaborate constructively with others and make positive contributions. (e.g. gaming communities or social media groups).

I can explain how someone can get help if they are having problems and identify when to tell a trusted adult.

I can demonstrate how to support others (including those who are having difficulties) online.

I can explain how sharing something online may have an impact either positively or negatively.

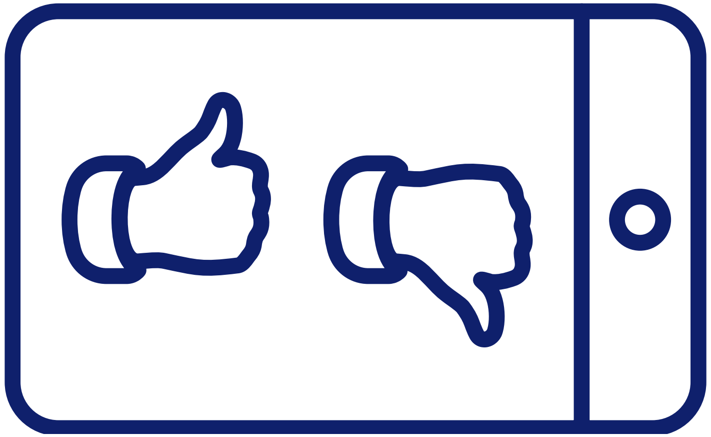
I can describe how to be kind and show respect for others online including the importance of respecting boundaries regarding what is shared about them online and how to support them if others do not.

I can describe how things shared privately online can have unintended consequences for others. e.g. **screen-grabs**.

I can explain that taking or sharing inappropriate images of someone (e.g. embarrassing images), even if they say it is okay, may have an impact for the sharer and others; and who can help if someone is worried about this.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11



Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

Online reputation

I can identify ways that I can put information on the internet.	I can recognise that information can stay online and could be copied.	I can explain how information put online about someone can last for a long time.
	I can describe what information I should not put online without asking a trusted adult first.	I can describe how anyone's online information could be seen by others.
		I know who to talk to if something has been put online without consent or if it is incorrect.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

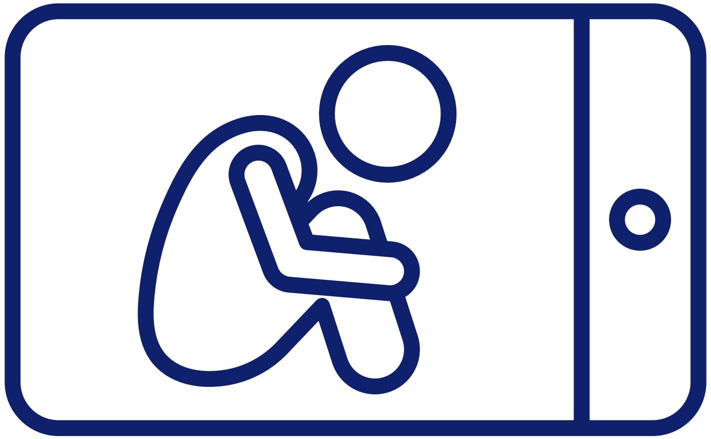
4 - 7

Online reputation

I can explain how to search for information about others online.	I can describe how to find out information about others by searching online.	I can search for information about an individual online and summarise the information found.	I can explain the ways in which anyone can develop a positive online reputation.
I can give examples of what anyone may or may not be willing to share about themselves online. I can explain the need to be careful before sharing anything personal.	I can explain ways that some of the information about anyone online could have been created, copied or shared by others.	I can describe ways that information about anyone online can be used by others to make judgments about an individual and why these may be incorrect.	I can explain strategies anyone can use to protect their '**digital personality**' and online reputation, including degrees of **anonymity**.
I can explain who someone can ask if they are unsure about putting something online.			

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11



Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

Online bullying

I can describe ways that some people can be unkind online.	I can describe how to behave online in ways that do not upset others and can give examples.	I can explain what bullying is, how people may bully others and how bullying can make someone feel.
I can offer examples of how this can make others feel.		I can explain why anyone who experiences bullying is not to blame.
		I can talk about how anyone experiencing bullying can get help.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

4 - 7

Online bullying

I can describe appropriate ways to behave towards other people online and why this is important.

I can give examples of how bullying behaviour could appear online and how someone can get support.

I can recognise when someone is upset, hurt or angry online.

I can describe ways people can be bullied through a range of media (e.g. image, video, text, **chat**).

I can explain why people need to think carefully about how content they post might affect others, their feelings and how it may affect how others feel about them (their reputation).

I can recognise online bullying can be different to bullying in the physical world and can describe some of those differences.

I can describe how what one person perceives as playful joking and teasing (including **'banter'**) might be experienced by others as bullying.

I can explain how anyone can get help if they are being bullied online and identify when to tell a trusted adult.

I can identify a range of ways to report concerns and access support both in school and at home about online bullying.

I can explain how to block abusive users.

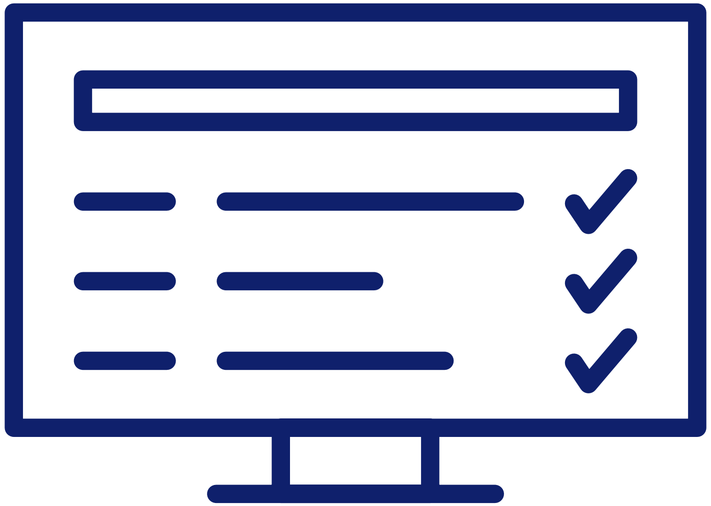
I can describe the **helpline services** which can help people experiencing bullying, and how to access them (e.g. Childline or The Mix).

I can describe how to capture bullying content as evidence (e.g **screen-grab**, **URL**, **profile**) to share with others who can help me.

I can explain how someone would report online bullying in different contexts.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11



Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.

Managing online information

I can talk about how to use the internet as a way of finding information online.

I can identify devices I could use to access information on the internet.

I can give simple examples of how to find information using digital technologies, e.g. **search engines**, **voice activated searching**).

I know / understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe / a joke.

I know how to get help from a **trusted adult** if we see content that makes us feel sad, uncomfortable worried or frightened.

I can use simple keywords in **search engines**.

I can demonstrate how to navigate a simple webpage to get to information I need (e.g. home, forward, back buttons; links, tabs and sections).

I can explain what **voice activated searching** is and how it might be used, and know it is not a real person (e.g. Alexa, Google Now, Siri).

I can explain the difference between things that are imaginary, 'made up' or 'make believe' and things that are 'true' or 'real'.

I can explain why some information I find online may not be real or true.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

4 - 7

Managing online information

I can demonstrate how to use key phrases in search engines to gather accurate information online.

I can explain what **autocomplete** is and how to choose the best suggestion.

I can explain how the internet can be used to sell and buy things.

I can explain the difference between a 'belief', an 'opinion' and a 'fact. and can give examples of how and where they might be shared online, e.g. in videos, memes, posts, news stories etc.

I can explain that not all opinions shared may be accepted as true or fair by others (e.g. monsters under the bed).

I can describe and demonstrate how we can get help from a trusted adult if we see content that makes us feel sad, uncomfortable worried or frightened.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

I can analyse information to make a judgement about probable accuracy and I understand why it is important to make my own decisions regarding content and that my decisions are respected by others.

I can describe how to search for information within a wide group of technologies and make a judgement about the probable accuracy (e.g. social media, image sites, video sites).

I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; **in-app purchases**, **pop-ups**) and can recognise some of these when they appear online.

I can explain why lots of people sharing the same opinions or beliefs online do not make those opinions or beliefs true.

I can explain that technology can be designed to act like or impersonate living things (e.g. **bots**) and describe what the benefits and the risks might be.

I can explain what is meant by **fake news** e.g. why some people will create stories or alter photographs and put them online to pretend something is true when it isn't.

7 - 11

I can explain the benefits and limitations of using different types of search technologies e.g. voice-activation search engine. I can explain how some technology can limit the information I aim presented with e.g. voice-activated searching giving one result.

I can explain what is meant by 'being **sceptical**'; I can give examples of when and why it is important to be 'sceptical'.

I can evaluate digital content and can explain how to make choices about what is trustworthy e.g. differentiating between adverts and search results.

I can explain key concepts including: information, reviews, fact, opinion, belief, validity, reliability and evidence.

I can identify ways the internet can draw us to information for different agendas, e.g. website notifications, **pop-ups**, targeted ads.

I can explain how search engines work and how results are selected and ranked.

I can explain how to use search technologies effectively.

I can describe how some online information can be opinion and can offer examples.

I can explain how and why some people may present 'opinions' as 'facts'; why the popularity of an opinion or the personalities of those promoting it does not necessarily make it true, fair or perhaps even legal.

I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how someone might encounter these online (e.g. advertising and '**ad targeting**' and targeting for **fake news**).

I understand the concept of **persuasive design** and how it can be used to influences peoples' choices.

Managing online information

I can describe ways of identifying when online content has been commercially sponsored or boosted, (e.g. by commercial companies or by **vloggers**, **content creators**, **influencers**).

I can explain what is meant by the term 'stereotype', how 'stereotypes' are amplified and reinforced online, and why accepting 'stereotypes' may influence how people think about others.

I can describe how **fake news** may affect someone's emotions and behaviour, and explain why this may be harmful.

I can explain what is meant by a '**hoax**'. I can explain why someone would need to think carefully before they share.

I can demonstrate how to analyse and evaluate the validity of 'facts' and information and I can explain why using these strategies are important.

I can explain how companies and news providers target people with online news stories they are more likely to engage with and how to recognise this.

I can describe the difference between on-line **misinformation** and **dis-information**.

I can explain why information that is on a large number of sites may still be inaccurate or untrue. I can assess how this might happen (e.g. the sharing of misinformation or disinformation).

I can identify, flag and report inappropriate content.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11

Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

Health, well-being and lifestyle

I can identify rules that help keep us safe and healthy in and beyond the home when using technology.

I can give some simple examples of these rules.

I can explain rules to keep myself safe when using technology both in and beyond the home.

I can explain simple guidance for using technology in different environments and settings e.g. accessing online technologies in public places and the home environment.

I can say how those rules / guides can help anyone accessing online technologies.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

4 - 7

Health, well-being and lifestyle

I can explain why spending too much time using technology can sometimes have a negative impact on anyone, e.g. mood, sleep, body, relationships; I can give some examples of both positive and negative activities where it is easy to spend a lot of time engaged (e.g. doing homework, games, films, videos).

I can explain why some online activities have age restrictions, why it is important to follow them and know who I can talk to if others pressure me to watch or do something online that makes me feel uncomfortable (e.g. age restricted gaming or web sites).

I can explain how using technology can be a distraction from other things, in both a positive and negative way.

I can identify times or situations when someone may need to limit the amount of time they use technology e.g. I can suggest strategies to help with limiting this time.

I can describe ways technology can affect health and well-being both positively (e.g. mindfulness apps) and negatively.

I can describe some strategies, tips or advice to promote health and well-being with regards to technology.

I recognise the benefits and risks of accessing information about health and well-being online and how we should balance this with talking to trusted adults and professionals.

I can explain how and why some apps and games may request or take payment for additional content (e.g. **in-app purchases**, **lootboxes**) and explain the importance of seeking permission from a trusted adult before purchasing.

I can describe common systems that regulate age-related content (e.g. **PEGI**, **BBFC**, parental warnings) and describe their purpose.

I recognise and can discuss the pressures that technology can place on someone and how / when they could manage this.

I can recognise features of **persuasive design** and how they are used to keep users engaged (current and future use).

I can assess and action different strategies to limit the impact of technology on health (e.g. **night-shift mode**, regular breaks, correct posture, sleep, diet and exercise).

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11

Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

Privacy and security

I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location).

I can describe who would be trustworthy to share this information with; I can explain why they are trusted.

I can explain that passwords are used to protect information, accounts and devices.

I can recognise more detailed examples of information that is personal to someone (e.g where someone lives and goes to school, family names).

I can explain why it is important to always ask a trusted adult before sharing any personal information online, belonging to myself or others.

I can explain how passwords can be used to protect information, accounts and devices.

I can explain and give examples of what is meant by 'private' and 'keeping things private'.

I can describe and explain some rules for keeping personal information private (e.g. creating and protecting passwords).

I can explain how some people may have devices in their homes connected to the internet and give examples (e.g. lights, fridges, toys, televisions).

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

4 - 7

Privacy and security

I can describe simple strategies for creating and keeping passwords private.

I can give reasons why someone should only share information with people they choose to and can trust. I can explain that if they are not sure or feel pressured then they should tell a trusted adult.

I can describe how connected devices can collect and share anyone's information with others.

I can describe strategies for keeping personal information private, depending on context.

I can explain that internet use is never fully private and is monitored, e.g. adult supervision.

I can describe how some online services may seek consent to store information about me; I know how to respond appropriately and who I can ask if I am not sure.

I know what the **digital age of consent** is and the impact this has on online services asking for consent.

I can explain what a **strong password** is and demonstrate how to create one.

I can explain how many free apps or services may read and share private information (e.g. friends, contacts, **likes**, images, videos, voice, messages, **geolocation**) with others.

I can explain what app permissions are and can give some examples.

I can describe effective ways people can manage passwords (e.g. storing them securely or saving them in the browser).

I can explain what to do if a password is shared, lost or stolen.

I can describe how and why people should keep their software and apps up to date, e.g. auto updates.

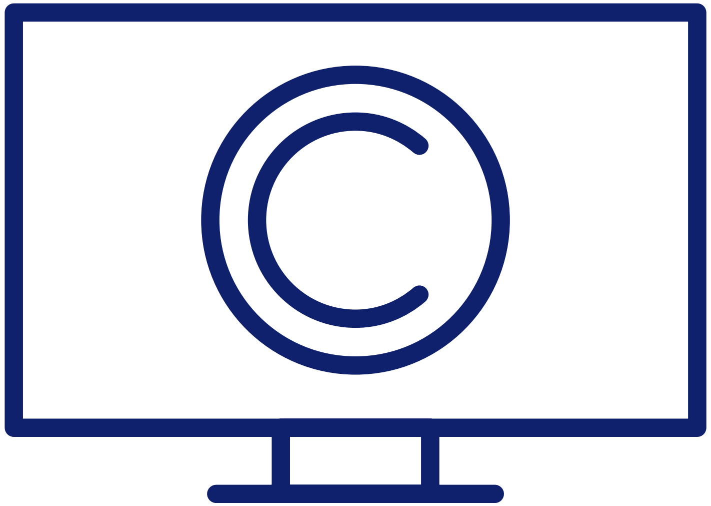
I can describe simple ways to increase privacy on apps and services that provide privacy settings.

I can describe ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content (e.g. **scams**, **phishing**).

I know that online services have **terms and conditions** that govern their use.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11



Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

Copyright and ownership

I know that work I create belongs to me.

I can name my work so that others know it belongs to me.

I can explain why work I create using technology belongs to me.

I can say why it belongs to me (e.g. ‘I designed it’ or ‘I filmed it’’).

I can save my work under a suitable title / name so that others know it belongs to me (e.g. filename, name on content).

I understand that work created by others does not belong to me even if I save a copy.

I can recognise that content on the internet may belong to other people.

I can describe why other people’s work belongs to them.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner’s experience and are achieved through learning that is matched to the readiness of the learner.

4 - 7

Copyright and ownership

I can explain why copying someone else's work from the internet without permission isn't fair and can explain what problems this might cause.

When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it.

I can give some simple examples of content which I must not use without permission from the owner, e.g. videos, music, images.

I can assess and justify when it is acceptable to use the work of others.

I can give examples of content that is permitted to be reused and know how this content can be found online.

I can demonstrate the use of search tools to find and access online content which can be reused by others.

I can demonstrate how to make references to and acknowledge sources I have used from the internet.

It is important that learning outcomes are interpreted within contexts that are relevant to the learner's experience and are achieved through learning that is matched to the readiness of the learner.

7 - 11

Glossary

+, AND, " ", NOT, * wildcard	Additional characters used in online searches to limit, expand or determine the search results returned by a search engine. Sometimes referred to as Boolean operators.
Adware	Software which automatically displays or downloads advertising material such as banners or pop-ups when a user is online. Designed to generate advertising revenue.
Adware blockers	Software which will stop or block unwanted banner ads or pop-ups from appearing. Some of these adware blockers are available as browser plug-ins. (See also pop-up blockers)
Ad targeting	The term covers a range of strategies used by companies to make ads more visible. This includes consideration about where on the page an ad is placed in order to get maximum visibility or clickability as well as basing the placements of ads on a user's behaviour, profile data (e.g. gender, age, location) or purchasing history etc. Ads are targeted to audiences with specific traits.
Age verification	Age verification mechanisms allow the age of a customer or service user to be checked by the service provider using sources such as credit cards, birth records etc.
AI (artificial intelligence)	Computer programmes which can think, learn, make decisions, solve problems and mimic human cognition meaning they are able to perform tasks such as visual perception, speech recognition, decision-making, and translation between languages.
Anonymity	This describes situations where a person's true identity is unknown. This is often achieved by adopting pseudonyms or omitting identifiable information from an online presence.
Anonymous reporting routes	A mechanism which allows users to report safeguarding issues anonymously, generally though an online facility which offers users the choice to enter contact details or not. Anonymous routes are often effective in engaging wider populations around online incidents, and provide support for those who want to report issues but are fearful of possible repercussions.

Glossary

App permissions	When apps are downloaded the user grants certain permissions of data and information that the app is able to access. This could include access to location, camera, microphone, browsing history, contact list etc. Some are legitimate and an app will need access in order to function correctly, others less so and will be more about the acquisition of data. Users are very often unaware of the permissions that they have granted.
AR (augmented reality)	A technology which superimposes a computer-generated image over a user's real view of the world, thus providing a composite view.
Autocomplete	A feature in which an application predicts the word or words a user is typing.
Avatar	An icon, cartoon or image to represent a user online on social media, in video games or other services.
Banter	A term describing intended jovial teasing or talk amongst friends, it has the effect of creating a bond among the group. Much banter is good-natured but when banter comes into contact with the outside world, including online, those not in the group, unaware of the permissive bond between members, can only take what's being 'said' at face value. Statements that participants consider as being in jest can sound hostile, derogatory, racist. Online, without the benefit of facial expressions, body language, tone of voice and context things can easily be misinterpreted. There is a risk that bullying behaviour can be excused as 'banter'.
BBFC (British Board of Film Classification)	UK organisation charged with rating and classifying film and other forms of media in terms of age and content.
Biometrics	Metrics related to human characteristics, e.g. finger prints, facial recognition, iris / retina recognition. Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups under surveillance.
'Brand you'	This refers to the way you choose to portray yourself online including conscious decisions to keep all content shared of a similar look and feel. This is often driven by the desire to gain more likes, follows or comments or even for commercial gain.

Glossary

Breadcrumb trail	A navigation aid in user interfaces. It allows users to keep track of their locations within programs, documents, or websites, usually appearing at the top of a webpage.
Chat	Informal communication online which can be found across different services such as social media, gaming and video sharing platforms. It can be a direct message to one person or multiple people in a group chat.
Cloud	Storing and accessing data and programs over the Internet instead of a computer's hard drive. Cloud storage can be accessed on almost any device with an internet connection as it is remote storage.
Coercion	The process by which an individual or group convinces someone to engage in behaviour and actions to the benefit of the coercer.
Comments	A way of responding to content posted online usually found directly underneath the content itself.
Content creators	Someone who is responsible for contributing to information / content on any media, in this context a website, social media platform or app.
Connectivity	The capacity for 'connected' devices to share data about individuals or groups online. Individuals may or may not be aware that this is data is being collected and shared, or how it is being used.
Cookies	Data generated by a website and saved on your web browser for the purpose of storing user preferences and login details (if selected to).
Copyright theft	Sometimes referred to as piracy, copyright theft is the use of content which is protected by copyright law, without the required permissions needed to reuse it.
Counter-narrative	Content or messages which offer a positive alternative to extremist propaganda or narratives online.

Glossary

Creative Commons Licensing	An American non-profit organisation devoted to expanding the range of creative works available for others to build upon legally and to share. Several free copyright licenses (known as Creative Commons licenses) have been released to the public.
Cropping	The digital removal of unwanted outer areas of a photo, image or video.
Crowdsourcing	The practice of obtaining information or input into a task or project by enlisting the services of a large number of people, either paid or unpaid, typically via the Internet.
Cyberbullying	The use of electronic communication to bully, exclude or intimidate someone. It can be direct forms of communication or indirection 'mentions' online which someone perceives to be aimed at them.
Dark web	The dark web forms a small part of the deep web and is only accessible by special software (see also TOR). It is heavily encrypted and masks the ISP of its users meaning it frequently attracts criminal activity although there are legitimate reasons to use and access the dark web.
DDoS (Distributed Denial of Service)	A DDoS attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
Deep fake technology	A technique for combining and superimposing existing images and videos onto other images and videos. The result can convincingly present something which did not actually occur.
Deep learning	A form of artificial intelligence that mimics the workings of the human brain in processing data and creating patterns for use in decision making.
Deep web	The deep web is the part of the Web not indexed by search engines, e.g. personal online banking pages. These pages are often hidden behind logins and are usually encrypted.

Digital age of consent	This is the minimum age that children can provide their own consent to the processing of their data. The UK has set this age as 13.
Digital manipulation	Altering a photo or video so that features are added, removed or appear differently. This may be done through the use of software or an app e.g. using filters, cropping or Deep fake technology
Digital personality	Created as individuals' online activity and behaviour is monitored; collected and analysed. A person's 'digital personality' can be used by and possibly sold to unknown others in order to target tailored advertising, information and disinformation specifically intended to be attractive to the individual and to influence their beliefs and choices.
Disinformation	Inaccurate information deliberately distributed and intended to confuse, mislead or influence.
Disinhibition	A term coined by danah boyd to explain why people behave differently when they are using online technologies. They are likely to feel a lack of restraint compared to when they are communicating in person.
Distro	Operating system based on Linux which can be installed and used on another system (usually through a USB key) to bypass security and filtering.
Do-not-track-me	An app or browser extension which blocks internet trackers from collecting and subsequently sharing information.
DPA (Data Protection Act 2018)	A law which governs the collection, processing, storage and distribution of personal data in the UK, overseen by the Information Commissioner's Office. The Act is the UK implementation of the EU General Data Protection Regulation or GDPR (see also GDPR).
DuckDuckGo	An example of a search engine which does not track users.

Glossary

Emoji	A small image or icon used to convey an idea, item or emotion. These are sent instead of or alongside messages written in text on messaging services and social media.
Echo chamber	Activity, often on social media, where people of like mind reinforce a single view point to the exclusion of alternatives. An 'echo chamber' (or 'reality bubble') can create a false impression that an opinion is more widely held in society than it actually is, and can significantly strengthen people's beliefs.
Encryption	The process of converting information, messages or data into a code, especially to prevent unauthorized access. Some services offer end-to-end encryption which only allows communicating users to read messages.
Exclusion	In an online context this refers to an individual who is left out from online chats, social media groups etc. It can also refer to self-exclusion from online gambling sites.
Facial recognition	Software capable of identifying or verifying a person from a digital image or videos.
False context	When genuine content is shared with false contextual information, e.g. date, location, event or motivation.
Fair dealing	A legal term used to establish whether a use of copyright material is lawful or whether it infringes copyright. There is no statutory definition of fair dealing – it will always be a matter of fact, degree and impression in each case. The question to be asked is: how would a fair-minded and honest person have dealt with the work?
Fake news	Fake news is a form of news consisting of deliberate disinformation or hoaxes spread via traditional news media or online social media (See also hoax and disinformation).
Fake profiles	Online accounts created to look like they are from a known and reputable source.
Filters	A form of editing used on social media and editing apps to make photos and images appear more glossy and achieve a more desired look and feel.

Glossary

Find my phone	An app provided on mobile devices to allow users to geo-locate their device if lost, misplaced or stolen. Further features allow remote locking and deletion of data, image capture through the camera of the user and messaging.
Firewalls	A network security system, either hardware or software based, that uses rules to control incoming and outgoing network traffic. A firewall acts as a barrier between a trusted network and an untrusted network.
Fitness trackers	Wearable multi-sensor devices that can collect data on movement; sleep; heart rate; blood pressure which is then collated and analysed via an associate app. Examples are Fitbit; Apple Watch and Galaxy Gear.
FOMO	An acronym for 'fear of missing out', describing a user's feeling of compulsion to check their phone or social media feed at regular intervals for fear of not staying up to date with conversations or events involving their friends.
Forums	An internet forum, or message board, is an online discussion site where users hold conversations in the form of posted messages. They differ from chat rooms in that messages are often longer than one line of text, and are at least temporarily archived. Depending on the access level of a user or the forum set-up, a posted message might require approval by a moderator before it becomes visible. A forum can contain a number of sub-forums, each of which may have several topics. Within a forum's topic, each new discussion is called a thread, and can be replied to by multiple users.
Gas-lighting	False information presented to someone, making them doubt their own memory, perception and quite often, their sanity.
GDPR (General Data Protection Regulation)	A regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). This regulation has been brought into UK law under the Data Protection Act 2018.
Geolocation	The process of identifying the geographical location of a person or device by means of digital information processed via the Internet.

Glossary

GIFs	A digital animation which includes still or moving images used as a form of jovial communication (see also memes).
Grooming	The process by which an online user gains the trust of another user with the intention of doing them harm or coercing them into engaging in risky or harmful behaviour. This behaviour could occur online (e.g. sending a sexually explicit image) or offline (e.g. agreeing to meet in person).
Guerilla Mail	A temporary email service which does not require registration and which only lasts for 60 minutes.
Hacking	Gaining unauthorised access to a computer system or account. Someone who does this may be referred to as a 'hacker'. Hackers find vulnerabilities in computer systems such as poor passwords or use technical methods to 'attack' systems. Some companies employ ethical hackers to help them protect their systems.
Harassment	Intentional and repetitive behaviour against an individual, which is felt to be threatening or disturbing, or creates an intimidating, hostile, degrading, humiliating or offensive environment for the individual.
Helpline services	Online or telephone-based services providing help and support e.g. Childline or The Mix for young people, and the NSPCC helpline and the Professionals Online Safety Helpline for adults.
Hits	Instances in which a webpage or site has been viewed.
Hoax	A fictional story circulated online, frequently intended to shape people's beliefs or opinions. Hoaxes can appear increasingly credible as they are repeatedly forwarded online.
Identity ideals	Aspirational ideas about identity shared and reinforced online.
Identity theft	The fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.

Glossary

In-app purchases	The purchase of additional content or services within an app or game often by using real money but sometimes in exchange for in-game money.
Incognito	A browser setting in Chrome that allows a user to browse without recording sites visited in the browser history. Referred to as in-private browsing on other browsers such as Safari and Internet Explorer.
Influencers	Someone who promotes lifestyle ideals, products, services or events via social media platforms. Influencers tend to have large numbers of followers which makes them more attractive to companies who want to advertise particular products.
Information operations	Actions taken online by unknown people, organisations and countries to use the media (especially social media) to steer public opinion by targeting and disseminating selective information or disinformation.
Injunction	A form of a court order that compels a party to do or refrain from specific acts. A party that fails to comply with an injunction faces criminal or civil penalties, including possible monetary sanctions and even imprisonment.
Internet of things	Everyday devices which are connected together via an internet connection with the purpose of sharing data and syncing outputs / actions.
Junk folders	A place used to store spam or unwanted incoming e-mail so that it stays out of a user’s inbox.
Kickstarter	A crowdfunding website which enables users to contribute money towards projects such as music, games or technology developments.
Libel	A published false statement that is damaging to a person's reputation; a written defamation.

Glossary

Lifestyle sites	Generic term for sites which reference physical and mental health issues, including anorexia, bulimia, suicide and self-harm. Usually set up by online communities experiencing these issues and often unregulated, unlike established and verified agencies offering online support services.
Likes	"Like" buttons are often available in social media platforms to signal a response to online content viewed. Users are encouraged to respond to content to build community, but it also serves the social media provider with additional information regarding an individual's online activity, which often shapes the resultant experience they have and the content they see on that platform.
Livestreaming	The broadcasting of live video to an audience over the internet. It can also be a one-on-one live video chat.
Loot boxes	An in-game purchase consisting of a virtual container that awards players with items and modifications based on chance. Loot boxes and other microtransactions are increasingly used to improve the profitability of games that are free to play or that are paid for as an initial purchase.
Memes	An image, video, piece of text, etc., typically humorous in nature, that is copied and spread rapidly by Internet users, often with slight variations (see also GIFs).
Malware	Sometimes referred to as malicious software, malware is a program designed to damage or carry out unwanted actions on a device or computer network.
Marketplace	Online platforms, features or accounts which are designed to sell an array of products and services.
Misinformation	Inaccurate information distributed by accident and without malicious intent.
Monitored	Usually used to refer to internet traffic which is logged by a service provider or organisation e.g. school.

Glossary

Night-shift mode	A mobile device features which changes the colour temperature of the screen to decrease the amount of blue light emitted from the display. It reduces screen brightness and assists with the absorption and release of the sleep hormone Melatonin. It can be activated automatically during sleeping hours.
Nudes	A term used by young people to describe self-taken naked or semi-naked photographs or videos. These pictures are taken on an electronic device and can be shared online. The reason for taking and sharing 'nudes' is not always sexual motivated.
Online commerce	The activity of electronically buying or selling of products on online services or over the Internet.
Online identity	A social identity that an internet user establishes in online communities and websites.
Outing someone	The practice of revealing private information about an individual online. This can be the sharing of private messages or information relating to their sexuality for example.
Parody	An imitation of the style of a particular writer, artist, or genre with deliberate exaggeration for comic effect.
Peer support	When individuals use their own experiences to help other people taking a number of forms such as peer mentoring, reflective listening (reflecting content and / or feelings), or counselling.
Peer-to-peer technology (P2P)	Allows users to access media files such as books, music, movies, and games using software which locates content by searching other devices on a peer-to-peer network.
PEGI (Pan-European Game Information)	EU classification system that rates games in terms of age suitability and content. Intended to regulate the retail of games to underage purchasers.
Persuasive design	Online features that are designed to change attitudes or behaviours of users through persuasion and social influence, by drawing on psychological and social theories. E.g autoplay function on YouTube, Snapchat streaks.

Glossary

Phishing	Sending electronic communications which attempt to obtain personal details (such as usernames, passwords, bank details) by claiming to be from a legitimate source. This information may then be used fraudulently.
Pirate sites	Sites which provide links to download online content such as films, music, games and software illegally without payment.
Political agenda	An underlying political motivation for sharing content or messages.
Pop-up blockers	Prevents pop-ups from displaying in a user's browser. Pop-up blockers work in a number of ways: some close the window before it appears, some disable the command that calls the pop-up, and some alter the window's source HTML.
Pop-ups	A form of online advertising usually commercial in nature, but can also be linked to malware, viruses and pornography. Content "pops up" on screen in a second window; can be managed and limited through browser settings or third party malware apps.
Profile	The information a user shares on social media presenting some personal details to other users. It may contain images, likes, hobbies, their network of contacts, contact details etc. Profiles can be unrepresentative and misleading (see also fake profiles).
Propaganda	The deliberate provision of: • information that whilst accurate may be narrowly selected, failing to present other pertinent facts • disinformation that is not factually accurate • a combination of information and disinformation where the inclusion of valid information is intended to mask or legitimise the disinformation with the intention of influencing the choices, actions or beliefs of others.
Proxy-bypass	A third party website set up for users to bypass filtering restrictions on the network they are using. Whilst these sites are often blocked by network administrators, others proliferate rapidly and are often listed on some areas of the internet.

Glossary

Radicalisation	The process by which a person is groomed to support terrorism and forms of extremism leading to terrorism.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Remote access	The ability to access to a computer or a network from a remote location - also known as remote desktopping.
Remote data deletion	A remote wipe may delete data in selected folders, repeatedly overwrite stored data to prevent forensic recovery, return the device to factory settings or remove all programming on the device.
Removable media	Any type of storage device that can be removed from a device while the system is running e.g. CDs, DVDs, Blu-Ray disks, USB drives. Removable media makes it easy for a user to move data from one computer to another.
Reviews (fake or misleading)	A critical appraisal of a service, product or location. Reviews can be unrepresentative and misleading.
RTBF (Right to be Forgotten)	In May 2014, the European Court Of Justice ruled that EU citizens have a 'Right To Be Forgotten', enabling them to request that search engines remove links to pages containing content deemed private, even if the pages themselves remain on the internet.
Satire	The use of humour, irony, exaggeration, or ridicule to expose and criticise people's stupidity or vices, particularly in the context of contemporary politics and other topical issues.
Scams	Online scams are schemes to extort money via online communications, e.g. through fake websites or emails. Messages may be sent to create fear (e.g. pretending something has or will happen), threat (e.g. pretending a person has done something they haven't) or reward (e.g. pretending someone has won a prize).
Sceptical	Having doubt or questioning something you have seen or have been told.

Glossary

Screen-grab	Way of capturing screen content on computers and mobile devices that can later be used to support issues and assist reporting.
Search engine	A programme, script or tool which searches the internet for information, images or material based on keywords or content entered by a user.
Search engine rankings	The position at which a particular site appears in the results of a search engine query.
Secure services	Methods of communication which are encrypted or use secure protocols to protect users (see also encryption).
Sexting	The term 'sexting' describes the use of technology to share personal sexual content; it is most commonly used to refer to youth produced sexual imagery. The name comes from a word-mix of 'sex' and 'texting'. Young people tend not to use this term but may use other nicknames such as 'nudes', 'nude selfies' or imply these through the context of the message.
Sexual harassment	Unwelcome sexual advances, requests for sexual favours, and other verbal or physical unwanted conduct of a sexual nature.
Sitemaps	A list of pages of a website accessible to crawlers or users.
Slander	False and damaging statements made about an individual or organisation.
Social bot	Automated software which generates content and messages presenting as if it is from a real person.
Social media feed	A collection of content shared on social media by an account often found on the account's profile.

Glossary

Social reporting	Reporting inappropriate, unkind or unpleasant content to other friends or users online, garnering support to apply pressure to the individual posting that content.
Spam	Unsolicited messages or content sent online to a large number of users. Spam is usually sent for the purpose of advertising, phishing or spreading virus / malware.
Stalking	A persistent and unwanted behaviour that causes another person fear, distress or anxiety. It can occur on and offline and could include sending malicious or unwanted communication, following someone, sending unwanted gifts, damaging property or sexual assault. Under the Protection from Harassment Act and 1997 and the Protection of Freedoms Act 2012, stalking is a criminal offence.
Streaming	Listening to music or watching video in 'real time', instead of downloading a file to your computer and watching it later.
Strong and secure password	A sequence of three random words can make a password stronger and harder to hack e.g. FlamingoHeadMan. Special characters can also be added to improve it e.g. 42@FlamingoHeadMan A separate password should be used for a personal email account as this is usually the gateway to all other accounts.
Terms and conditions	Terms of service (also known as terms of use and terms and conditions, commonly abbreviated as TOS or ToS and ToU) are rules by which one must agree to abide in order to use a service. Many online service providers have complex T&C's that are difficult for a user to navigate and fully understand. The UK Children's Commissioner has created simplified T&C's for some of the main social media platforms.
TOR (The Onion Router)	Software enabling access to the dark web through a series of anonymous points of presence on the internet, making it difficult to track a user or individual device. Simply using TOR isn't illegal but some of the content which it allows access to is illegal.

Torrent sites	Sites offering files for download using a distributed peer-to-peer file sharing system. The programs used to download files via the BitTorrent protocol are called BitTorrent clients.
Trojans	A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by hackers trying to gain access to users' systems.
Trolling	The sending of malicious, abusive or derogatory messages by one user (a 'troll') to another user online with the intention of upsetting or harassing them, or damaging their reputation. Trolling is often anonymous.
Trusted adult	Someone who a young person has a good relationship with and has their best interests in mind. Most likely to include someone at home or in school. It is important that young people have a number of trusted adults they can go to from different areas of their lives and they may need support in identifying these.
Two-factor authentication	A type of multi-factor authentication providing an extra layer of security. It requires not only a password and username but also an additional piece of information which can often be verified through an authenticator app on a user's mobile device.
Unsubscribing	To cancel a subscription to an electronic mailing list or online service.
Upskirting	This is a colloquial term referring to the action of placing equipment such as a camera or mobile phone beneath a person's clothing to take a voyeuristic photograph without their permission. It is not only confined to victims wearing skirts or dresses and equally applies when men or women are wearing kilts, cassocks, shorts or trousers. It is often performed in crowded public places, for example on public transport or at music festivals, which can make it difficult to notice offenders.
URL	Uniform Resource Locator. A URL is the address of a specific webpage or file on the Internet.
Vloggers	A person who regularly records and posts videos online via social media or video sharing sites like YouTube. Popular vlogs include ones about lifestyle and gaming.

Glossary

Viruses	A computer virus is a type of malicious software ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Infected computer programs can include data files, or the "boot" sector of the hard drive.
Voice activated search	Also known as 'voice search' or 'voice-enabled search'. When a search tool allows the user to use a voice command to search the Internet, a website, or an app.
VPN (Virtual Private Network)	A method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet. VPNs are often used by corporations to protect sensitive data.
VR (Virtual Reality)	A simulated experience usually found within gaming that can be similar to or completely different from the real world.
Webcams	A video camera connected to the internet that allows users to broadcast live video or take and share photographs. Webcams can be used with computers and are often built into laptops, tablets and smartphones.
wellness apps	Software designed to assist or track mental and physical health. In its simplest form it can be apps that provide the right environment for relaxation or meditation; many provide the ability to be able to record emotions or feelings at key points of the day to form a record of mental health and to assist with forming strategies to support those issues.
Whistle-blowing	In the online context, whistle-blowing describes an individual's act of disseminating data or information online that others such as organisations or governments might wish to suppress.

Supporting resources, literature and research

The resources and links below provide a starting point for supporting children and young people develop the competencies detailed in the framework.

Note that many learning resources are issue-specific (e.g. sharing explicit images, bullying, protecting personal information) and so should be used in conjunction with other materials to enable children and young people to develop their understanding, skills and confidence across the competencies.

Self-image and identity

Dove Self-Esteem Project

Media Smart

Online relationships

Brook and NCA-CEOP – Digital Romance

NCA-CEOP – Thinkuknow

Childnet – PSHE toolkits

Childnet et al – Project deSHAME

Disrespect Nobody

LGfL – Undressed

NSPCC – Relationships and sex education (RSE) resources for schools

Online reputation

Barclays LifeSkills – Online reputation and social networking

Childnet – Online Reputation Checklist

Media Smart

Online bullying

Anti-Bullying Alliance

BullyingUK – Cyberbullying

Ditch the Label

Government Equalities Office Anti-homophobic, Biphobic and Transphobic Bullying Project

NSPCC Learning – Protecting children from bullying and cyberbullying

The Diana Award – Anti-bullying Ambassadors

Managing online information

Childnet – Trust Me

Google Search Education

Ofcom – Making Sense of Media

NewsWise news literacy project and resources

Health, wellbeing and lifestyle

BeGambleAware and PSHE Association – exploring risk in relation to gambling

Girlguiding – Girls' Attitudes Survey

Public Health England – Rise Above

PSHE Association – mental health and emotional wellbeing lesson plans

Young Minds - Resources

Privacy and security

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

ICO – Resources for schools

National Crime Agency – Exploring Cybercrime

NCSC – Resources for schools

Copyright and ownership

Intellectual Property Office – Cracking Ideas

Creative Commons

FACT UK

Get It Right From a Genuine Site

Further information and resources

Barnardos

Common Sense Education

Childnet

The Education People

Education Scotland

London Grid for Learning

NCA-CEOP – Thinkuknow online safety education programme

NSPCC

NSPCC Learning

Parent Info

Parent Zone

PSHE Association

South West Grid for Learning – Project Evolve programme

UKCIS

Welsh Government – Hwb

UK Council for Internet Safety

This document has been produced in partnership with:

CEOP A National Crime Agency command

Childnet International

Department for Education

Department for Digital, Culture, Media & Sport

THE EDUCATION PEOPLE

Education Scotland Foghlam Alba

HES Dedicated to education

LGfL

NSPCC

parentzone MAKING THE INTERNET WORK FOR FAMILIES

PSHE Association

SBNI Safeguarding Board for Northern Ireland

SWGfL Education that Clicks

Llywodraeth Cymru Welsh Government