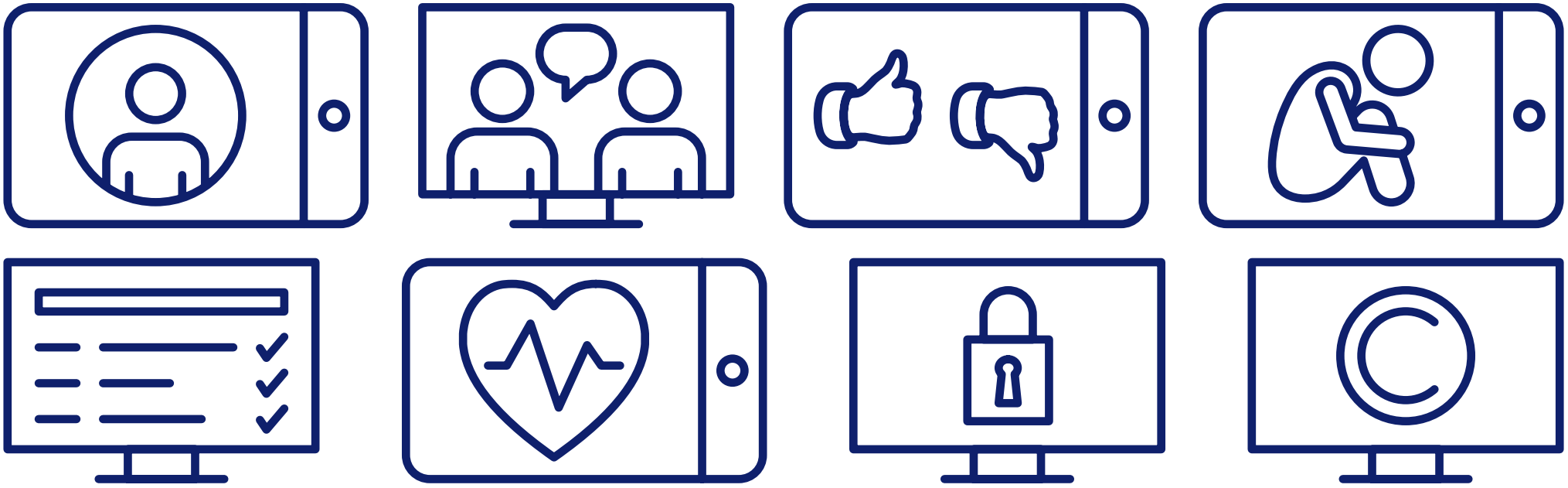
Start here

Education for a Connected World

A framework to equip children and young people for digital life



UKCCIS

UK COUNCIL FOR **CHILD INTERNET SAFETY**

Today's children and young people are growing up in a digital world. 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 skills and understanding 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, and what skills they need to be able to navigate it safely.

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.

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 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 UKCCIS Education Working Group.

UKCCIS 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 UKCCIS Education Working Group brings together leading organisations in online safety in education: Barnardo's, CEOP (the child protection command of the National Crime Agency), Childnet, Department for Education, Kent County Council, London Grid for Learning, the NSPCC, Parent Zone, the PSHE Association, South West Grid for Learning and the UK Safer Internet Centre. It 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.**

Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and how media impacts on gender and stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

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 and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

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 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.

Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation and ethical publishing.

Health, well-being and lifestyle

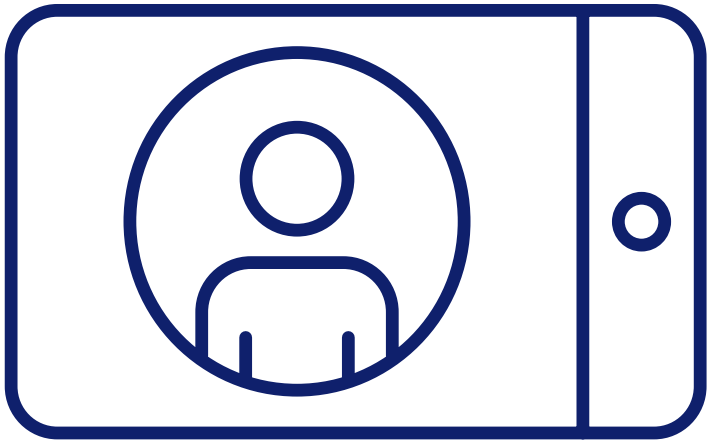
This strand explores the impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

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.

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.



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and how media impacts on gender and 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

Early years - 7	7 - 11	11 - 14	14 - 18
I can recognise that I can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who asks me to do something that makes me feel sad, embarrassed or upset.	I can recognise that there may be people online who could make me feel sad, embarrassed or upset.	I can explain how other people's identity online can be different to their identity in real life.	
I can explain how this could be either in real life or online.	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.	I can describe ways in which people might make themselves look different online.	
		I can give examples of issues online that might make me feel sad, worried, uncomfortable or frightened; I can give examples of how I might get help.	

Self-image and identity

Early years - 7	7 - 11	11 - 14	14 - 18
I can explain what is meant by the term 'identity'.	I can explain how my online identity can be different to the identity I present in 'real life'.	I can explain how identity online can be copied, modified or altered.	I can describe ways in which media can shape ideas about gender.
I can explain how I can represent myself in different ways online.	Knowing this, I can describe the right decisions about how I interact with others and how others perceive me.	I can demonstrate responsible choices about my online identity, depending on context.	I can identify messages about gender roles and make judgements based on them.
I can explain ways in which and why I might change my identity depending on what I am doing online (e.g. gaming; using an **avatar**; social media).			I can challenge and explain why it is important to reject inappropriate messages about gender online.
			I can describe issues online that might make me or others feel sad, worried, uncomfortable or frightened. I know and can give examples of how I might get help, both on and offline.
			I can explain why I should keep asking until I get the help I need.

Self-image and identity

I can give examples of how the internet and social media can be used for positive self-promotion.	I can reflect on and assess the role that digital media plays in my life and give clear examples of where it benefits my lifestyle.	I can explain how online images can help to reinforce stereotypes.
I can explain how people can curate and experiment with their identity online and why they might wish to do this.	I can explain how presenting myself in different ways online carries both benefits and risks and I can describe and assess what these could be.	I can describe some of the pressures that people can feel when they are using social media (e.g. peer pressure, a desire for peer approval, '**FOMO**').
I am aware that my own personal online activity, history or profile (my '**digital personality**') will affect the type of information returned to me in a search or on a social media stream, and intended to influence my beliefs, actions and choices.	I can explain strategies to reduce potential risks.	I can explain how personal images can be **photo-manipulated**.

Self-image and identity

Early years - 7	7 - 11	11 - 14	14 - 18
I can explain how online content can influence the way that people behave; I can evaluate different factors and their impact.	I can demonstrate ways I can use the internet and social media for positive self-promotion including enhancing employment prospects.	I can describe the laws governing online sexual content.	I can describe and assess the creative benefits and ethical drawbacks of digital manipulation.
I can explain how online content can be shaped to influence behaviour and body image (e.g. fashion, pornography, **lifestyle sites**).	I can recognise, assess and if necessary challenge the social norms and expectations that influence how I represent myself online (e.g. profile pictures, shared content) and how it might differ according to gender, culture or social group.	I can describe and critically assess ways in which viewing online sexual content can influence expectations and behaviour in relationships; I can assess how unrealistic or unreciprocated expectations could damage a relationship or be abusive.	I can explain and assess the importance of purpose and context in evaluating digitally edited personal images.
I can give examples of media which are designed to influence behaviour.		I can identify online role models who manage a positive identity and give examples from my own research/experience to support my understanding.	
I can explain what is meant by **artificial intelligence (AI)**; I can assess how AI may affect my present and future life (including my career choices).	I know how to appropriately challenge negative comments or expectations concerning my online identity.		
	I make positive contributions to other's self-identity, where appropriate (e.g. avoiding negative comments or positive commentary on profile pictures).		

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 and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online relationships

Early years - 7	7 - 11	11 - 14	14 - 18
I can recognise some ways in which the internet can be used to communicate.	I can use the internet with adult support to communicate with people I know.	I can use the internet to communicate with people I don't know well (e.g. email a penpal in another school/ country).	
I can give examples of how I (might) use technology to communicate with people I know.	I can explain why it is important to be considerate and kind to people online.	I can give examples of how I might use technology to communicate with others I don't know well.	

Online relationships

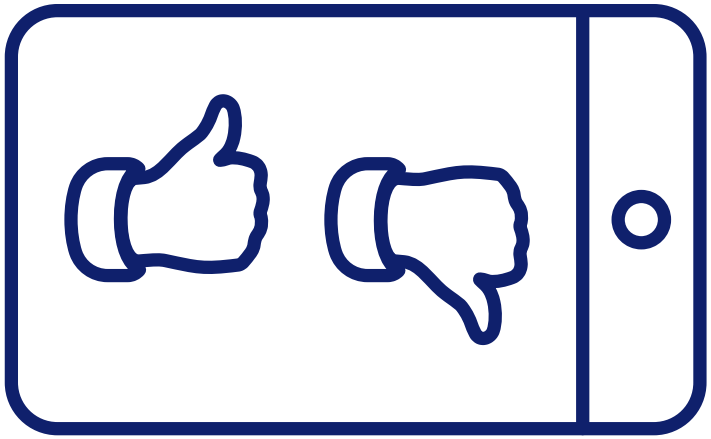
Early years - 7	7 - 11	11 - 14	14 - 18
I can describe ways people who have similar likes and interests can get together online.	I can describe strategies for safe and fun experiences in a range of online social environments.	I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my/our fault.	I can show I understand my responsibilities for the well-being of others in my online social group.
I can give examples of technology-specific forms of communication (e.g. **emojis**, **acronyms**, **text speak**).	I can give examples of how to be respectful to others online.	I can make positive contributions and be part of online communities.	I can explain how impulsive and rash communications online may cause problems (e.g. flaming, content produced in live streaming).
I can explain some risks of communicating online with others I don't know well.		I can describe some of the communities in which I am involved and describe how I collaborate with others positively.	I can demonstrate how I would support others (including those who are having difficulties) online.
I can explain why I should be careful who I trust online and what information I can trust them with.			I can demonstrate ways of reporting problems online for both myself and my friends.
I can explain how my and other people's feelings can be hurt by what is said or written online.			
I can explain why I can take back my trust in someone or something if I feel nervous, uncomfortable or worried.			
I can explain what it means to 'know someone' online and why this might be different from knowing someone in real life.			
I can explain what is meant by 'trusting someone online'. I can explain why this is different from 'liking someone online'.			

Online relationships

I can explain how and why people who I communicate with online may try to influence others negatively and can offer examples. e.g. **grooming**; **radicalisation**; **coercion**.	I can describe the benefits of communicating with a partner online.	I can identify the challenges raised by both unhealthy and healthy online sexual behaviour.
I can explain strategies for assessing the degree of trust I place in people or organisations online.	I can explain how relationships can safely begin (on-line dating), develop, be maintained, change and end online.	I can explain what is meant by sharing explicit images, the different terms used for this, and a range of possible outcomes.
I can describe the initial signs of potentially problematic situations e.g. **grooming**, cyberbullying.	I can give examples of how to make positive contributions to online debates and discussions.	I can give examples of how harmful online sexual behaviour can occur and can critically assess the potential harm.
I can assess when I need to take action and explain what to do if I am concerned about an online relationship.	I can give examples where positive contributions have effected change in an online community (e.g. **Gamergate**, gaming communities, social media).	I can demonstrate strategies to gain help and report concerns for myself and others.

Online relationships

Early years - 7	7 - 11	11 - 14	14 - 18
I can describe how online technology allows access to and communication with culturally diverse communities beyond my immediate social group.	I can describe the laws that govern online behaviour and how they inform what is acceptable or legal (e.g. **sexting** (and related terminology), **trolling**, **harassment**, **stalking**).	I can explain how laws governing online behaviour vary depending on country and culture.	I can give examples of how I might mobilise online communities to support ideas/ projects or campaigns (e.g. **crowdsourcing** expertise for a project; developing a **Kickstarter** campaign to create social/financial support for an idea; amplifying political voice).
I can give examples of how I adapt my behaviour to engage positively with those groups taking into account gender, cultural sensitivity, political and religious beliefs etc.	I can give examples from my own media research of historical cases to support my understanding	I can explain the difference between freedom of expression and legal accountabilities and can discuss appropriate balance between them.	
I can assess when the use of technology has become controlling (e.g. using location apps to monitor and manipulate). I can explain why this is abuse, what I would say and do, and how I could get support.	I can describe actions I could take if I or someone else experiences or is targeted by illegal online behaviour.	I can explain the term '**whistle-blowing**' and evaluate when such action may be appropriate or inappropriate.	
		I can give examples from my own media research/ experience to support my understanding.	



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 me can last for a long time.
	I can describe what information I should not put online without asking a trusted adult first.	I know who to talk to if I think someone has made a mistake about putting something online.

Online reputation

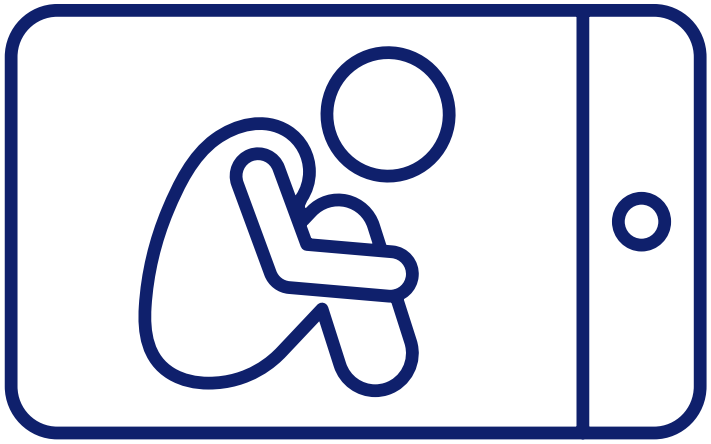
Early years - 7	7 - 11	11 - 14	14 - 18
I can search for information about myself online.	I can describe how others can find out information about me by looking online.	I can search for information about an individual online and create a summary report of the information I find.	I can explain how I am developing an online reputation which will allow other people to form an opinion of me.
I can recognise I need to be careful before I share anything about myself or others online.	I can explain ways that some of the information about me online could have been created, copied or shared by others.	I can describe ways that information about people online can be used by others to make judgments about an individual.	I can describe some simple ways that help build a positive online reputation.
I know who I should ask if I am not sure if I should put something online.			

Online reputation

I can describe and assess the benefits and the potential risks of sharing information online.	I can explain and give examples of how what I write online can also affect my school, family or social group, or future opportunities.	I can monitor my online reputation and can take clear steps to ensure that it promotes a positive image.
I can describe what is appropriate to say and do in different online settings/ platforms (e.g. opinions, values, information, shares, 'likes', 'forwards').	I can explain strategies to manage and protect my 'digital personality'.	I can identify some of the key laws governing online behaviour and reputation and the potential criminal implications of breaking them.

Online reputation

Early years - 7	7 - 11	11 - 14	14 - 18
I can explain the importance of my online reputation (especially to my future career) and can describe ways of managing this.	I can build an online presence using a range of technologies that provide a positive representation of who I am, listing attributes others may find valuable (e.g. job/university application profiles).	In cases where my online reputation may be viewed negatively, I am able to offer reasons and provide context as to why it may not always reflect who I am.	I can describe and assess the benefits of the laws that govern online behaviour and reputation.
I can describe how to effectively challenge content that influences my reputation negatively. I can explain what the limitations of this can be.			I can differentiate between ethical and legal issues (e.g. libel, slander, racism, homophobia, **injunction**, **trolling**).
			I can use my own media research to give relevant examples.



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 give examples of bullying behaviour and how it could look online.
I can offer examples of how this can make others feel.		I understand how bullying can make someone feel.
		I can talk about how someone can/would get help about being bullied online or offline.

Online bullying

Early years - 7	7 - 11	11 - 14	14 - 18
I can explain what bullying is and can describe how people may bully others.	I can identify some online technologies where bullying might take place.	I can recognise when someone is upset, hurt or angry online.	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 describe rules about how to behave online and how I follow them.	I can describe ways people can be bullied through a range of media (e.g. image, video, text, **chat**).	I can describe how to get help for someone that is being bullied online and assess when I need to do or say something or tell someone.	I can identify a range of ways to report concerns both in school and at home about online bullying.
	I can explain why I need to think carefully about how content I post might affect others, their feelings and how it may affect how others feel about them (their reputation).	I can explain how to block abusive users.	
		I can explain how I would report online bullying on the apps and platforms that I use.	
		I can describe the helpline services who can support me and what I would say and do if I needed their help (e.g. **Childline**).	

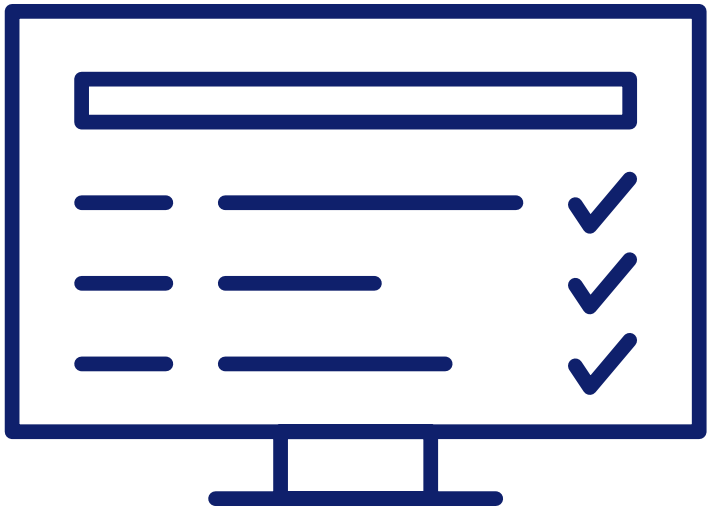
Online bullying

I can describe how bullying may change as we grow older and recognise when it is taking place online.	I can recognise online bullying can be different to bullying in the physical world and can describe some of those differences.	I can explain how cruelty and unpleasant comments can escalate quickly online.
I can describe a range of different bullying types and behaviours and assess when these are occurring (e.g. homophobic, racist, gender, exclusion).	I can demonstrate how I would intervene (and how I would assess if this should be directly or indirectly) to support others who are experiencing difficulties online.	I can explain the concept of disinhibition online and can explain how this can be problematic.
I can identify and demonstrate actions to support others who are experiencing difficulties online.	I can give examples of effective strategies which might help myself or others.	I can explain and assess a variety of routes to report bullying both in school and at home that include: **social reporting**, **peer support**, **anonymous routes** and **helpline services**.
		I can describe some of the laws that govern online behaviour and bullying and the potential implications of breaking them.
		I can explain what actions I can take if I believe these laws have been broken.

Online bullying

11 - 14	14 - 18
I can assess and apply a range of more sophisticated strategies to deal with extreme forms of bullying (e.g. trolling and harassment in online forums).	I can demonstrate how I would affect positive change in the online groups to which I belong when bullying behaviours arise.
I can identify and explain some of the laws that criminalise activity related to online bullying (e.g. Computer Misuse Act; Protection from Harassment Act; Communications Act).	I can give examples of effective strategies that might achieve this (e.g. counter-narrative).

Early years - 7	7 - 11	11 - 14	14 - 18
I can explain my criteria for distinguishing between online bullying and good-natured teasing (**banter**) online. I can offer examples to differentiate between them.	I can identify bullying behaviours in a variety of online contexts (including the workplace) and can work cooperatively with others online to challenge those behaviours and prevent them recurring.		
I can identify and assess behaviours that might be seen as bullying in different online contexts (e.g. close friend groups vs public **forums**) and adjust my own behaviour accordingly.			



Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation and ethical publishing.

Managing online information

I can talk about how I can use the internet to find things out.	I can use the internet to find things out.	I can use keywords in search engines.
I can identify devices I could use to access information on the internet.	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 give simple examples of how to find information (e.g. **search engine**, **voice activated searching**).	I can describe and demonstrate how to get help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable worried or frightened.	I can explain what **voice activated searching** is and how it might be used (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 true.

Managing online information

Early years - 7	7 - 11	11 - 14	14 - 18
I can use key phrases in search engines.	I can analyse information and differentiate between 'opinions', 'beliefs' and 'facts'. I understand what criteria have to be met before something is a 'fact'.	I can use different search technologies.	I can use search technologies effectively.
I can explain what **autocomplete** is and how to choose the best suggestion.	I can describe how I can search for information within a wide group of technologies (e.g. social media, image sites, video sites).	I can evaluate digital content and can explain how I make choices from search results.	I can explain how search engines work and how results are selected and ranked.
I can explain how the internet can be used to sell and buy things.	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 key concepts including: data, information, fact, opinion belief, true, false, valid, reliable and evidence.	I can demonstrate the strategies I would apply to be discerning in evaluating digital content.
I can explain the difference between a 'belief', an 'opinion' and a 'fact'.	I can explain that some people I 'meet online' (e.g. through social media) may be computer programmes pretending to be real people.	I understand the difference between online **mis-information** (inaccurate information distributed by accident) and **dis-information** (inaccurate information deliberately distributed and intended to mislead).	I can describe how some online information can be opinion and can offer examples.
	I can explain why lots of people sharing the same opinions or beliefs online does not make those opinions or beliefs true.	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 explain how and why some people may present 'opinions' as 'facts'.
		I can explain what is meant by a '**hoax**'. I can explain why I need to think carefully before I forward anything online.	I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how I might encounter these online (e.g. advertising and 'ad targeting').
		I can explain why some information I find online may not be honest, accurate or legal.	I can demonstrate strategies to enable me to analyse and evaluate the validity of 'facts' and I can explain why using these strategies are important.
		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 either by accident or on purpose).	I can identify, flag and report inappropriate content.

I can explain how online 'market places' can enable small businesses or individuals to do business within a global market.

I can assess the benefits and limitations of online commerce.

I can explain the term '**connectivity**': the capacity for connected devices ('internet of things') to collect and share information about me with or without my knowledge (including microphones, cameras and **geolocation**). I can describe how this can affect me.

I can use various additional tools to refine my searches (e.g. search filters: size, type, usage rights etc.).

I can explain how to use search effectively and use examples from my own practice to illustrate this.

When I publish online content, I am aware of how that content can be interpreted by others.

I can explain how 'liking', 'sharing' or 'forwarding' online content can change people's opinions of me (e.g. contribute to my online reputation).

I can navigate online content, websites or social media feeds using more sophisticated tools to get to the information I want (e.g. menus, **sitemaps**, **breadcrumb-trails**, site search functions).

I can explain how **search engine rankings** are returned and can explain how they can be influenced (e.g. commerce, sponsored results).

I can explain how social media can amplify, weaken or distort the apparent strength, validity, or popularity of an idea, belief or opinion by being shared between and reinforced by like-minded individuals; (e.g. an '**echo-chamber**').

I can explain how online anonymity may permit some people to express extreme views or abusive comments; I can assess how social media may create the impression that more people hold these views than actually do.

I can explain how contributors to social media may be '**social bots**'.

I can refine search phrases with additional functions (e.g. **+, AND, " ", NOT, * wildcard**).

I can use a range of features to quality assure the content I access online (e.g. **hits**, **likes**, comments).

I can analyse and evaluate the reliability and validity of online information based on content as well as appearance.

Managing online information

Early years - 7	7 - 11	11 - 14	14 - 18
I can recognise when and analyse why online content has been designed to deliberately mislead or misinform (e.g. **fake news** or **propaganda**).	I can identify and describe some of the laws governing online illegal content and that they may vary from country to country.	I can explain ways my own personal online choices, history and profile will be increasingly affecting the type of information returned to me in a search, on a social media stream or through targeted advertising or political messages. I can describe ways of recognising and assessing such targeting.	I can describe the process I use to make ethical choices to ensure my own online content is appropriate, responsible and contributes to a positive online culture. I can give examples of this from my own publishing.
I can differentiate between genuine news sites and fake (or imitation) news sites with similar web addresses.	I can give examples from my own media research of incidences when those laws have been broken.	I can recognise when articles or stories on-line are **satire** and not a true account of real events or people's behaviour.	
I can recognise and assess why some online content can be potentially harmful and can identify illegal content.	I can describe what is meant by 'big data' and 'data analytics' and how political parties, commercial and other organisations use these. I can evaluate the ethics of such use.	I can describe ways of identifying when online content has been sponsored, either commercially (e.g. **vloggers**) or politically (e.g., extremism, ideological persuasion) and analysing and evaluating their validity.	
I can demonstrate the appropriate routes if I need to report illegal content.	I can assess and manage how and what I contribute to 'big data'.	I can describe how and why individuals or organisations may saturate online media with selective information and misinformation to deliberately confuse or divide populations.	
	I can assess how my developing '**digital personality**' might affect (focus or limit) the type of information returned to me in a search or on a social media stream.	I can analyse online material to identify when this is happening and who might benefit.	
	I can explain how and why I could be targeted for sophisticated information or disinformation intended to influence my beliefs, actions and choices (e.g. **gas-lighting**, **information operations**).		
	I can explain strategies I would use to analyse and evaluate the validity and credibility of information I receive.		

Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle. 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 explain rules to keep us safe when we are using technology both in and beyond the home.	I can explain simple guidance for using technology in different environments and settings.
I can give some simple examples.	I can give examples of some of these rules.	I can say how those rules/guides can help me.

Health, well-being and lifestyle

Early years - 7	7 - 11	11 - 14	14 - 18
I can explain why spending too much time using technology can sometimes have a negative impact on me; I can give some examples of activities where it is easy to spend a lot of time engaged (e.g. games, films, videos).	I can explain how using technology can distract me from other things I might do or should be doing.	I can describe ways technology can affect healthy sleep and can describe some of the issues.	I can describe common systems that regulate age-related content (e.g. **PEGI**, **BBFC**, parental warnings) and describe their purpose.
	I can identify times or situations when I might need to limit the amount of time I use technology.	I can describe some strategies, tips or advice to promote healthy sleep with regards to technology.	I can assess and action different strategies to limit the impact of technology on my health (e.g. **night-shift mode**, regular breaks, correct posture, sleep, diet and exercise).
	I can suggest strategies to help me limit this time.		I can explain the importance of self-regulating my use of technology; I can demonstrate the strategies I use to do this (e.g. monitoring my time online, avoiding accidents).

Health, well-being and lifestyle

I recognise and can discuss the pressures that technology can place on me and how/ when I think I should respond.	I can assess the benefits of and potential problems with sites or apps that intend to promote positive well-being (e.g. **wellness apps**, **fitness trackers**, meditation/ relaxation apps).	I can identify online content and/or groups that promote unhealthy coping strategies (e.g. suicide, eating disorders, self-harm).
I can give some examples of those pressures (e.g. immediate response on social media and messaging apps; always available; invasive; rapid engagement).	I can demonstrate criteria for assessing and differentiating between health sites that offer unbiased, accurate and reliable health information from those promoting a product or agenda.	I can identify and assess some of the potential risks of seeking help or harmful advice from these sites.
I can describe strategies to identify and assess when peers may need support and describe ways to assist peers who may be experiencing difficulties.	I can describe the criteria I would use to help me evaluate the benefit technology and apps may have to me.	I can identify who I would talk to if I thought someone was at risk of being influenced by such sites.
I can explain how I might recognise that I need support to control my use of technology and who might provide that support.		

Health, well-being and lifestyle

Early years - 7	7 - 11	11 - 14	14 - 18
From my own research, I can identify and assess features that might indicate that a site or social group could negatively impact on well-being.	I can describe the laws around age related access to certain types of online content (e.g. gaming; gambling; alcohol/drugs related; sexual content) and assess their benefits and limitations.	I can analyse mechanisms providers might use to regulate/ advise on age-related online access:(e.g. **age verification**, **terms and conditions**, parental controls).	I can analyse well-being issues experienced by others in the wider news from my own online research.
I can offer strategies to identify and evaluate help from established respected sites or organisations that may be more helpful.		I can assess and comment on the benefits and effectiveness of these.	I can construct strategies that may have assisted with those cases I have identified.
		I can identify and demonstrate how to action effective routes for reporting concerns about age-related content issues.	I can analyse and identify opportunities and risks that may arise from technologies (e.g. **VR**, **AR**, **AI**) that could impact on health and well-being.

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

Early years - 7	7 - 11	11 - 14	14 - 18
I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location).	I can recognise more detailed examples of information that is personal to me (e.g. where I live, my family's names, where I go to school).	I can describe how online information about me could be seen by others.	
I can describe the people I can trust and can share this with; I can explain why I can trust them.	I can explain why I should always ask a trusted adult before I share any information about myself online.	I can describe and explain some rules for keeping my information private.	
	I can explain how passwords can be used to protect information and devices.	I can explain what passwords are and can use passwords for my accounts and devices.	
		I can explain how many devices in my home could be connected to the internet and can list some of those devices.	

Privacy and security

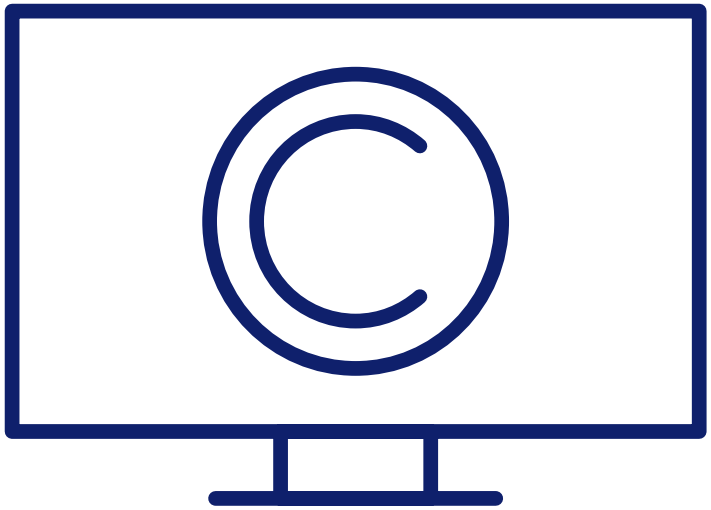
Early years - 7	7 - 11	11 - 14	14 - 18
I can give reasons why I should only share information with people I choose to and can trust. I can explain that if I am not sure or I feel pressured, I should ask a trusted adult.	I can explain what a strong password is.	I can create and use strong and secure passwords.	I use different passwords for a range of online services.
I understand and can give reasons why passwords are important.	I can describe strategies for keeping my personal information private, depending on context.	I can explain how many free apps or services may read and share my private information (e.g. friends, contacts, likes, images, videos, voice, messages, **geolocation**) with others.	I can describe effective strategies for managing those passwords (e.g. **password managers**, acronyms, stories).
I can describe simple strategies for creating and keeping passwords private.	I can explain that others online can pretend to be me or other people, including my friends.	I can explain how and why some apps may request or take payment for additional content (e.g. in-app purchases) and explain why I should seek permission from a trusted adult before purchasing.	I know what to do if my password is lost or stolen.
I can describe how connected devices can collect and share my information with others.	I can suggest reasons why they might do this.		I can explain what app permissions are and can give some examples from the technology or services I use.
	I can explain how internet use can be monitored.		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**).

Privacy and security

I can explain how and why it is important to always ensure I make safe and secure online payments.	I can explain how to manage security software (e.g. anti-virus, **security patches**, adware blockers) on my devices and understand why regular updates are important.	I can assess how secure sites are that store my content and can identify appropriate sites to inform my choices (e.g. **https**, **Verisign**).
I can explain that online services have **terms and conditions** that govern their use. I can give examples from some common online services that illustrate how they impact on a user and analyse these to make informed choices.	I can demonstrate ways in which I can change my browser settings to make my online browsing more secure (e.g. cookie permissions, **do-not-track-me**, password storage, **incognito**).	I can explain how and assess when more secure use may require more advanced password management (e.g. **dual-factor authentication**, regular rolling, security questions, **captcha**, **biometrics**).
I can explain what malware is and give some examples of how it operates and what the impact could be on a device or user (e.g. **viruses**, **trojans**, **ransomware**).	I can explain app permissions and analyse them to make informed choices on which apps I use.	I can explain how to manage and report issues if I discover or suspect a device has been compromised or I (or someone I know) are the victim of a scam (e.g. phishing, identity theft, ransomware).
I can explain what **cookies** are and can give examples of how my online browsing can be tracked and used by others (e.g. **adware**).	I can explain how the security of devices connected to the internet may be compromised e.g. **webcams**, monitors, phones or toys - I can demonstrate actions I can take to minimise such compromise (e.g. covering cameras on computers when not in use).	
I can identify commercial content and **scams** (e.g. pop-ups, **spam**) and can discuss simple strategies to manage such content (e.g. **pop-up blockers**, **junk folders**, **unsubscribing**).		
I can explain how my internet use is often **monitored** (e.g. by my school or internet service provider).		

Privacy and security

11 - 14	14 - 18
I can undertake informed debate concerning the conflict between national security and personal privacy.	I can explain how the security of data in a network can be compromised internally or externally and give examples of how this might occur (e.g. **DDOS**, **proxy-bypass**, **distro**, **hacking**). I can describe actions that can minimise risks.
I can describe how data drawn from users of online services can be used or sold to inform other services and organisations. I can give examples of this.	I can explain why networks require secure management and can give examples of services that support this (e.g. **firewalls**, **VPN**, user monitoring).
I can demonstrate additional ways to protect and manage data on my devices (e.g. **"find my phone"**; **remote access**; **remote data deletion**).	I can explain the value of regular data backup in system recovery, and can give examples of and demonstrate effective practice in how this might be achieved (e.g. **removable media**, **cloud**).
I can describe key aspects of the law governing data use (e.g. **DPA**, **GDPR**) and, from my own media research, can give examples of those laws and their impact (e.g. **RTBF**, data breaches).	I can describe how and where to report a personal data breach.
I can assess how those laws can vary depending on country and can give examples of some of the differences and issues they might raise.	I can describe anonymous access services (e.g. **TOR**, **Guerilla Mail**, **DuckDuckGo**) and can give examples of how they may be used in both positive and negative contexts.
I can identify and assess when data needs to be transferred securely and can describe strategies to achieve this (e.g. **encryption**, **secure services**).	I can explain the concepts **'dark web'**, **'deep web'** and **'closed peer sharing'** and can critically assess the issues associated with the use of such services.
	I can explain why it is essential to recognise and follow my future employer's online security policy and protocols.



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

Early years - 7	7 - 11	11 - 14	14 - 18
I know that work I create belongs to me.	I can explain why work I create using technology belongs to me.	I can describe why other people's work belongs to them.	
I can name my work so that others know it belongs to me.	I can say why it belongs to me (e.g. 'it is my idea' or 'I designed it').	I can recognise that content on the internet may belong to other people.	
	I can save my work so that others know it belongs to me (e.g. filename, name on content).		

Copyright and ownership

Early years - 7	7 - 11	11 - 14	14 - 18
I can explain why copying someone else's work from the internet without permission can cause problems.	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 assess and justify when it is acceptable to use the work of others.	I can demonstrate the use of search tools to find and access online content which can be reused by others.
I can give examples of what those problems might be.	I can give some simple examples.	I can give examples of content that is permitted to be reused.	I can demonstrate how to make references to and acknowledge sources I have used from the internet.

Copyright and ownership

I know that commercial online content can be viewed, accessed or downloaded illegally.	I understand the concept of software and content licensing.	I understand **Creative Commons Licensing** protocols.
I can give some examples of illegal access (e.g. illegal **streaming**, **pirate sites**, **torrent sites**, peer-to-peer sharing) and the associated risks.	I can explain the principles of **fair use** and apply this to case studies.	I can demonstrate simple ways in which I can protect my own work from copyright theft.
I can accurately define the concept of plagiarism.	I can identify the potential consequences of illegal access or downloading and how it may impact me and my immediate peers.	I can evaluate the possible impact of legal and illegal downloading on those people who create online content and the consequences for the wider community.
I can use this definition to evaluate my own use of online sources.	I can explain why controlling copyright of my content may be limited when using social media, website and apps.	

Copyright and ownership

I can apply Creative Commons Licensing to my own work.	I can demonstrate how I can protect my own work from copyright theft.	I can explain key aspects of copyright law and, from my own media research, give examples of where that law has been applied to online content.	I can give examples of how organisations representing creative industries challenge and monitor online copyright theft and can outline and evaluate resulting outcomes.
I can apply the principles of fair use to my own work and that of others.	I can explain the effects of plagiarism within my own work and assess the impact it can have on accrediting achievement.	I can explain the wider implications of copyright theft on content production and the availability of content (e.g. loss of revenue, emerging artists, new content development).	
I can give examples of where I have done this.			

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.
acronyms	An abbreviation of a sentence using the first letter of each word. Online users may use acronyms as a quick way to convey thoughts, actions or sentiments e.g. LOL (Laugh Out Loud).
adware	Software which automatically displays or downloads advertising material such as banners or pop-ups when a user is online.
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. **The UK Digital Economy Act 2017** requires sex, gambling, gaming and alcohol related sites to have age verification systems in place to protect both adults and children.
AI (artificial intelligence)	The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.
anonymous 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.
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 a user is typing.
avatar	An icon or image to represent a user online on social media, in video games or other services.
banter	Teasing or joking talk. While much banter is good-natured, there is a risk that bullying behaviour can be excused as 'banter'.

Back to last page

Glossary

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. 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.
breadcrumbs trail	A graphical control element used as 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.
captcha	A computer programme designed to tell the difference between a human and an automated programme. It is often used to prevent spam messages or fraudulent activity.
chat	Informal communication via text or messaging platforms which often uses conventions such as emojis, acronyms or text-speak.
Childline	Confidential helpline service for children and young people in the UK managed by the NSPCC.
closed peer sharing	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.
cloud computing	Storing and accessing data and programs over the Internet instead of a computer's hard drive.
coercion	The process by which one person convinces another to engage in behaviour and actions to the benefit of the coercer.
connectivity	The capacity for 'connected' devices to share data about individuals or groups on-line. Individuals may or may not be aware that this is data is being collected and shared, or how it is being used.
cookies	Text files retained on computers by browsers, containing information on user activity on specific websites.

Back to last page

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.
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.
dark web	The dark web forms a small part of the deep web. It is heavily encrypted and masks the ISP of its users. The dark web frequently attracts criminal activity. Sometimes the term 'deep web' is mistakenly used to refer to the dark web.
deep web	The deep web is the part of the Web not indexed by search engines, e.g. online banking pages. These pages are often hidden behind logins and are usually encrypted.
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.
digital personality	Created as individuals' on-line 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.
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.

Back to last page

Glossary

DPA	The **Data Protection Act 1998**, which governs the collection, processing, storage and distribution of personal data in the UK, overseen by the **Information Commissioner's Office**. Soon to be superseded by the EU General Data Protection Regulations or **GDPR**.
dual-factor authentication	A type of multi-factor authentication, providing an extra layer of security. It requires not only a password and username but also something unique to that user such as personal information, a code sent to a device, or a physical token.
DuckDuckGo	An example of a search engine which does not track users.
emoji	A small image or icon used to convey an idea 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 encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies intelligible content to a would-be interceptor.
fair use	Any copying of copyrighted material done for a limited and "transformative" purpose, such as to comment upon, criticize, or parody a copyrighted work. Such uses can be undertaken without permission from the copyright owner. In other words, 'fair use' is a defence against a claim of copyright infringement.
fake news	A news item which is claimed to have been fabricated. Allegations of 'fake news' have been used to discredit accurate news items.

Back to last page

Glossary

find my phone	An operating system feature 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. Third party apps such as **Prey** and **Android Lost** provide similar functions.
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 people can 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. Also, depending on the access level of a user or the forum set-up, a posted message might need to be approved by a moderator before it becomes visible. Forums have a specific set of jargon associated with them; example: a single conversation is called a "thread", or topic. A discussion forum is hierarchical or tree-like in structure: a forum can contain a number of subforums, each of which may have several topics. Within a forum's topic, each new discussion started is called a thread, and can be replied to by as many people as so wish.
Gamergate	A controversial online movement concerned with ethics in gaming and gaming journalism, born out of heated discussions around game developers, gender and relationships between the game industry and game journalists.

Back to last page

Glossary

gas-lighting	Information and disinformation disseminated in such quantities that people become confused and disempowered and no longer trust their own judgements; they struggle to differentiate between information founded on fact and disinformation. 'Gas-lighting' can be a deliberate strategy employed to discredit or disrupt credible sources of information in order to further a particular agenda.
GDPR	The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is 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).
geolocation	the identification or estimation of the real-world geographic location of an object, such as a radar source, mobile phone, or Internet-connected computer terminal.
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	Accessing or changing secure information over the internet without permission. 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**, the **Professionals Online Safety Helpline**.
hits	Instances in which a webpage or site has been viewed.

Back to last page

Glossary

hoax	A fictional story circulated on-line, frequently intended to shape people's beliefs or opinions. Hoaxes can appear increasingly credible as they are repeatedly forwarded on-line.
https	The secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted.
in-app purchases	The purchase of goods and services from an application on a mobile device, such as a smartphone or tablet.
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.
information operations	Actions taken on-line 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.
junk folders	A tool used for filtering electronic junk e-mail out of a user's inbox within a private or commercial e-mail account.
Kickstarter	A crowdfunding website which enables users to contribute money towards projects such as music, games or technology developments.
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.

Back to last page

Glossary

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.
misinformation	Inaccurate information distributed by accident.
monitored	Usually used to refer to internet traffic which is logged by a service provider or organisation e.g. school.
night-shift mode	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 exists on most mobile devices and can be activated automatically during sleeping hours.
password managers	A password manager assists in generating and retrieving complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand.
peer support	Occurs when people provide knowledge, experience, emotional, social or practical help to each other. It commonly refers to an initiative consisting of trained supporters (although it can be provided by peers without training), and can take a number of forms such as peer mentoring, reflective listening (reflecting content and/or feelings), or counselling.
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.
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.
photo-manipulation	Altering a photo so that features are added, removed or appear differently. This may be done through the use of an app e.g. a camera filter or software e.g. Photoshop.

Back to last page

Glossary

pirate sites	Sites which provide links to download online content such as films, music, games and software illegally without payment. Example is The **PirateBay**.
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	Unsolicited content linked to many online services, usually web, that offer additional services linked to that content. 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.
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.
radicalisation	The process by which a person comes to support terrorism and forms of extremism leading to terrorism.
ransomware	A type of malicious software from cryptovirology which threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Back to last page

Glossary

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, diskettes, USB drives. Removable media makes it easy for a user to move data from one computer to another.
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	Fictional stories circulated online intended to shame individuals, corporations, government, or society itself into improvement. They are intended to be humorous and not as literal accounts of behaviour or events.
scams	Online scams are schemes to extort money via online communications, e.g. through fake websites or emails.
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.

Back to last page

Glossary

security patches	A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bug fixes and improving the usability or performance.
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.
sitemaps	A list of pages of a website accessible to crawlers or users.
social bot	Automated software which generates content through a social media account, presenting that account as if it is operated by a real person.
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.

Back to last page

Glossary

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. Recent work by the UK Children's Commissioner has set about simplifying some of the main social media platforms into more accessible formats.
text speak	A written language used in text messages and online messages which uses abbreviations for commonly known phrases and does not follow standard conventions of spelling, punctuation or grammar.
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.
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 cyber-thieves and hackers trying to gain access to users' systems.
trolling	The public 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.
unsubscribing	To cancel a subscription to an electronic mailing list or online service.
URL	Uniform Resource Locator. A URL is the address of a specific webpage or file on the Internet.
vloggers	A video blog or video log, usually shortened to vlog, is a form of blog for which the medium is video. Vlog entries often combine embedded video (or a video link) with supporting text, images, and other metadata. Entries can be recorded in one take or cut into multiple parts. Vlogs are particularly popular on YouTube. Video logs (vlogs) also often take advantage of web syndication to allow for the distribution of video over the Internet using either the RSS or Atom syndication formats, for automatic aggregation and playback on mobile devices and personal computers.

Back to last page

Glossary

VeriSign Secured	The VeriSign Secured seal indicates that a website has been verified and certified as secure by Symantec.
viruses	A computer virus is a type of malicious software program ("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	A programme, script or tool that searches the internet for information, images or material based on words spoken by a user.
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)	The computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special electronic equipment, such as a helmet with a screen inside or gloves fitted with sensors.
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.

Back to last page

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

SWGfL drama resource – With Friends Like These

WebWise

Online relationships

Barnardos – Real Love Rocks

Brook and CEOP – Digital Romance

CEOP – Thinkuknow

Childnet et al – Project deSHAME

Childnet – Crossing the Line PSHE Toolkit

Disrespect Nobody

NSPCC, Children's Commissioner and Middlesex University – '…I wasn't sure if it was normal to watch…'

PSHE Association – Sex and Relationship Education (SRE) for the 21st century

Online reputation

Barclays LifeSkills – Online reputation and social networking

Childnet – Online Reputation Checklist

MediaSmart – Promoting Ethical Behaviour Online: My Virtual Life

SWGfL – Digital Literacy and Citizenship

Online bullying

Anti-Bullying Alliance

BullyingUK – Cyberbullying

Ditch the Label

European Schoolnet – ENABLE

Stop Speak Support

The Diana Award – Anti-bullying Ambassadors

Managing online information

Childnet – Trust Me

Google Search Education

Ofcom – Children's media literacy

Health, well-being and lifestyle

Childline

Girlguiding – Girls' Attitudes Survey

Vodafone and ParentZone – Digital Parenting Magazine

Young Minds – Resources

Privacy and security

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

ICO – Resources for schools

The European Handbook for Teaching Privacy and Data Protection at Schools

Copyright and ownership

Childnet – Music, Film, TV and the Internet

Cracking Ideas

Creative Commons

FACT report – Cracking down on digital piracy

Get It Right From a Genuine Site

SWGfL – Digital Literacy and Citizenship

Further information and resources:

Barnardos

CEOP – Thinkuknow

Childline

Childnet International

Kent County Council – collation of online safety resources

LGfL – London Grid for Learning

NSPCC – Share Aware

Parent Info

ParentZone

PSHE Association

South West Grid for Learning

UKCCIS

UK Safer Internet Centre

UK COUNCIL FOR **CHILD INTERNET SAFETY**

This document has been produced in partnership with:

Believe in children Barnardo's

CEOP A National Crime Agency command

Childnet International

Department for Education

Department for Digital, Culture, Media & Sport

Kent County Council

LONDON GRID FOR LEARNING

NSPCC

parentZONE MAKING THE INTERNET WORK FOR FAMILIES

PSHE Association

SWGfL Education that Clicks

UK Safer Internet Centre