How 2BeSafe Can Support KCSIE 2026

Contents

Introduction 3
KCSIE 2026 and the Curriculum 4
Mapping to KCSIE 4Cs 5
Progression of 4Cs and 2BeSafe at a Glance 7

Introduction

This document sets out how 2BeSafe can help support a school to meet some of their duties under Keeping Children Safe in Education (KCSIE) 2026 in relation to the **curriculum aspect of it**. It is intended for the designated safeguarding lead, the computing and RSHE leads, governors, and anyone reviewing the school's safeguarding curriculum.

KCSIE is statutory safeguarding guidance, not a curriculum. It requires schools to teach children how to keep themselves and others safe, including online, and to treat online safety as a running theme across policy, training and curriculum planning. 2BeSafe makes a substantial contribution to the online safety part of that duty. It should be noted that it sits alongside, and does not intend to replace, the school's Relationships and Health Education programme.

All information contained in this document is guidance only. It is important that schools make informed decisions on meeting KCSIE 2026 standards by using their existing systems and reference appropriate DfE documentation.

KCSIE 2026 and the Curriculum

Teaching related expectations within KCSIE 2026 are detailed mainly in Part Two, under Opportunities to Teach safeguarding and Online Safety.

In the context of what 2BeSafe is and how it supports some aspects of KCSIE 2026 aims, this document will show mapping of the following updated 4Cs framework of risk (paragraph 165) , which schools should use to shape lessons, discussions and classroom rules:

Risk Category	What KCSIE 2026 Specifies	What to Address at Primary Age
Content	Exposure to illegal, inappropriate, or harmful content (e.g. physical violence, misinformation, fake news, conspiracy theories).	• Understanding that not everything seen online is true or real • What to do if they stumble across disturbing, scary, or adult pictures/videos.
Contact	Harmful interaction with other users or generative AI applications that simulate interaction; pressure, adults posing as children, grooming, or exploitation.	• Knowing that strangers/chatbots are not always who or what they seem • Understanding personal data boundaries • Never agreeing to meet an online contact or share private details
Conduct	Online behaviour that increases the likelihood of or causes harm (e.g. cyberbullying, making/sharing explicit or AI-generated imagery).	• Being kind online • Understanding digital footprints; recognising that mean messages or exclusion in group chats cause real harm • Not taking or sharing private images of themselves or peers.
Commerce	Risks such as online scams, in-game spending, phishing, and inappropriate advertising.	• In-game purchases, pop-ups, clicking suspicious links, and recognizing scams in games or apps.

Mapping to KCSIE 4Cs

The table below shows where 2BeSafe objectives explicitly address each of the four online risk areas named in KCSIE 2026. **Note that other sessions may include these risk areas as the nature of 2BeSafe provides revisiting and cross over between lessons and themes.**

KCSIE 2026 risk	2BeSafe evidence
Content: misinformation, disinformation, conspiracy theories	Y2 Managing Online Information S4–5: real, true or made up Y3 Managing Online Information S4–5: belief, opinion and fact Y4 Managing Online Information S4, S6: popularity is not truth; fake news and altered photographs Y5 Managing Online Information S2, S8–9: being sceptical; effects of fake news; hoaxes Y6 Managing Online Information S4, S7, S9–10: opinions presented as facts; misinformation and disinformation
Content: racism, prejudice and harmful representation	Y5 Managing Online Information S7: how stereotypes are amplified and reinforced online Y6 Self-Image and Identity S1: evaluating and challenging content about gender, race, religion, disability and culture
Content: upsetting or inappropriate content	Y1 Managing Online Information S3; Y3 Managing Online Information S6: getting help from a trusted adult Y6 Managing Online Information S11: identify, flag and report inappropriate content
Contact: grooming and people posing as someone else	Y2 Online Relationships S1: risks of communicating with people not known offline Y3 Online Relationships S2–3: “knowing” and trusting someone online Y4 Self-Image and Identity S3: others can pretend to be someone else Y5 Online Relationships S2: some people may want to do harm, and it is not the child’s fault

KCSIE 2026 risk	2BeSafe evidence
Contact: generative AI that simulates people (new in 2026)	Y2 Managing Online Information S3: voice assistants are not real people Y4 Managing Online Information S2: search for information within a wide group of technologies and make a judgment on accuracy Y4 Managing Online Information S5: technology designed to act like or impersonate living things (bots), benefits and risks Y5 Online Reputation S1: Search for information about an individual online and summarise the information Y5 Online Relationships S1: give examples of technology specific forms of communication (including AI)
Conduct: making and sharing images	Y3 Online Relationships S6: giving and gaining permission before sharing images and videos Y6 Online Relationships S3: unintended consequences, such as screen-grabs Y6 Online Relationships S4: taking or sharing inappropriate images, even if someone says it is okay
Conduct: online bullying	Online Bullying strand, Reception to Year 6 (19 objectives) Y5 Online Bullying S2: when “banter” is experienced as bullying Y6 Online Bullying S1–2: capturing evidence and reporting in different contexts
Commerce: advertising, gambling-style features, scams	Y3 Managing Online Information S3; Y4 Managing Online Information S3: buying and selling online; persuasive selling and in-app purchases Y5 HWL S4: in-app purchases and loot boxes Y5 Managing Online Information S5–6: targeted adverts; sponsored or boosted content Y6 P&S S5: scams and phishing Y6 HWL S3; Y6 Managing Online Information S6: persuasive design

Progression of 4Cs and 2BeSafe at a Glance

KCSIE expects teaching to be age and stage appropriate. This overview shares what children will learn in each area as they move through the school.

Area	Reception	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Content	Knows the internet is a place to find information.	Knows online content can be liked or disliked, real or make believe; tells a trusted adult about upsetting content.	Tells real from made up; knows some online information is untrue; recognises worrying issues and how to get help.	Separates fact, opinion and belief; understands age restrictions; shows how to get help with upsetting content.	Judges probable accuracy across platforms; explains fake news and altered photographs; knows popularity does not equal truth.	Applies scepticism; evaluates trustworthiness; understands stereotypes, hoaxes and the effects of fake news; weighs online health information.	Critically evaluates representations of groups; tells misinformation from disinformation; uses age-rating systems; flags and reports content.
Contact	Can say “no”, “please stop”, “I’ll tell”; knows the internet is used to communicate; knows who to trust with personal information.	Recognises people online may upset someone; communicates with known people with adult support; asks before sharing personal information.	Knows people may act differently online; risks of contact with people not known offline; right to say no under pressure; voice assistants are not real people.	Understands “knowing” and “trusting” someone online versus liking them; shares only with trusted people; can change their mind about trust.	Uses safe strategies in livestreaming and gaming; knows others can pretend to be someone else, including friends; knows bots can impersonate living things.	Knows some people online may want to cause harm and that it is not their fault; blocks abusive users; knows when to tell a trusted adult.	Keeps asking until they get help; uses privacy settings on apps and services.

Area	Reception	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Conduct	Knows some people are unkind online and how this feels; knows we can put information online.	Behaves kindly online; asks permission; knows information can stay online and be copied.	Knows what bullying is and that victims are not to blame; asks before sharing about others; knows online information lasts.	Explores identity and self-representation; knows words can hurt; gives and gains permission before sharing images and videos.	Recognises bullying through images, video and chat; tells healthy from unhealthy behaviour; considers how posts affect others and reputation.	Knows when "banter" becomes bullying; knows identity can be copied or altered; knows reporting routes and helplines; supports others.	Captures evidence and reports; respects boundaries; understands screen-grabs and sharing inappropriate images even if someone says it is okay; builds a positive reputation.
Commerce	Not yet introduced.	Not yet introduced.	Asks a trusted adult before clicking "yes", "agree" or "accept".	Knows the internet is used to buy and sell; knows connected devices collect and share information.	Recognises advertising, offers, in-app purchases and pop-ups; knows services seek consent to store data; knows the digital age of consent.	Understands in-app purchases and loot boxes, app permissions and data sharing, targeted adverts and sponsored or influencer content.	Identifies scams and phishing; knows about terms and conditions; understands persuasive design, influence, manipulation and targeted news.

Area	Reception	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Foundation skills	Rules for safe, healthy technology use; devices that access the internet; owning their own work.	Passwords protect information; finding information with search and voice; saving and naming work.	Using passwords and keywords; navigating webpages; connected devices at home; others own their work.	Screen time and its effects; keeping passwords private; key phrases and autocomplete; copying is unfair.	Technology as a distraction; limiting time; internet use is monitored; checking ownership before reuse.	Strong passwords; benefits and limits of search tools; wellbeing strategies; when reuse is acceptable.	Managing passwords and updates; how search engines rank results; managing pressures; referencing sources.