ANNEX A: GAPS BETWEEN OFCOM'S ANALYSIS OF CAUSES AND IMPACTS OF ONLINE HARM PROPOSED MITIGATIONS: ILLEGAL HARMS (*including new animal cruelty offence) AND PROTECTION OF CHILDREN COMBINED

In our response to Ofcom's illegal harms consultation, we provided a table analysing how far harm arising from the functionalities that it identified in its risk register (volume 2) were mitigated by specific measures in the codes (annex 7). The approach Ofcom takes in its protection of children's consultation is broadly similar to that proposed in the illegal harms consultation - though this caveated by many references throughout the documents that the responses to the latter have not yet been taken into account and further updates will follow. It is not clear, however, whether these will have a material impact on the approach to both sets of codes.

We have carried out the same analysis on the children's consultation as we did previously and updated our table to combine the results from both for ease of reference. As we set out in the introduction to the previous document, we would expect that Ofcom's decisions on which measures to include in their codes of practice would reflect the level of risk threat that the functionalities identified in the risk register pose. We would also reiterate here our acknowledgement that the work that has gone into the risk registers themselves - volume 3 in the children's consultation, volume 2 in the illegal harms - is thorough and analytical. But - with specific reference to the new material - this assessment (again) does not flow through to the mitigation measures in the codes of practice for user-to-user services (annex 7) and search (annex 8), which as previously focus primarily on content takedown and measures to deal, ex-post, with primary priority content (PPC), priority content (PC) or non-designated content (NDC). The exception to this is the measures - much publicised in Ofcom's press material and communications around the launch of the consultation - relating to recommender systems.

The following tables provide detailed analysis on the individual functionalities, the number of offences (for the illegal harms codes) or types of content (for the children's codes) where Ofcom identifies that particular functionality is a contributory factor, and the appearance (or not) of mitigating measures relating to this functionality in the codes of practice for user to user and search services for both duties. A summary "at a glance" table is provided for U2U (pages 3-6) and search (p7-8). Supporting tables for user-to-user services (from p9) and search services (pp21-25) provide more detail and extracts from Ofcom's consultation materials. We have divided the measures in both sets of codes into "ex ante" and "ex post", the latter largely applying to measures relating to content moderation and takedown when either illegal content or PPC, PC or NDC has been identified on a service. While we have used the term "ex ante" in relation (generally speaking) to the non-takedown measures, the measures identified are focused on the presence of specific content (either illegal or designated) on the service (or the search functionality enabling users to find it) so are not what we would term "safety by design" measures. These we would classify as biting at a systemic level separate to the nature of the particular types of content (e.g. business model, default settings or measures that are not directed to a particular type of content for eg rebalancing weighting in recommender tools).

COMPARISON OF RISK REGISTER FUNCTIONALITIES WITH USER-CODE OF PRACTICE MITIGATIONS (Annex 7): SUMMARY TABLE

Functionality	**Illegal harms offences**	**Children's PPC, PC or NDC**	**Code of practice: ex ante mitigations**		**Code of practice: ex post mitigations**	
	17 in total (updated with animal cruelty offence & s127(1))	9 in total	Illegal harms	Children	Illegal harms	Children
Content: posting, commenting, hyperlinks, including images and video	17	9	Limited to user controls measures (eg muting, blocking): 9A, 9B	Limited to user controls measures (eg muting, blocking, disabling comments): US2, US3	Content moderation & takedown: 4A-F	Content moderation & takedown: CM1-CM7 Limited: Signposting children to support when they a) report content (all services); b) post or repost content (large, risky services); US3, US4
Reposting or forwarding content	7	4	None	None	Limited: reference to "limiting time"	None
Livestream & live audio	10	7	None	None	None	None
Use of hashtags	5	8	None	None	None	None
Editing visual content	9	4	None	None	None	None
Screen capturing or recording	1	2	None	None	None	None

Functionality	**Illegal harms offences**	**Children's PPC, PC or NDC**	**Code of practice: ex ante mitigations**		**Code of practice: ex post mitigations**	
	17 in total (updated with animal cruelty offence & s127(1))	9 in total	Illegal harms	Children	Illegal harms	Children
User tagging	5	3	None	None	None	None
User profiles	11	4	Limited to user controls: 9A, 9B	Limited to user controls: US2, US3	None	None
User connections	10	8	Limited to default settings, user controls: 9A, 9B	Limited to default settings, user controls: US2, US3	None	None
Stranger pairing	N/A	1	N/A	N/A	None	None
User search	2	1	None	None	None	None
User groups	10	4	None	None	None	
User base profile	3	7	None	Significant measures via age assurance (AA1-6) though no differentiation for age ranges within this	Limited: references in 4E, 5B	None
Recommender systems	13	8	None	Significant new	Limited: A6 ("limited	Not applicable:

Functionality	**Illegal harms offences**	**Children's PPC, PC or NDC**	**Code of practice: ex ante mitigations**		**Code of practice: ex post mitigations**	
	17 in total (updated with animal cruelty offence & s127(1))	9 in total	Illegal harms	Children	Illegal harms	Children
				measure (RS1-3) covering PPC and PC, and feedback	time"), A9 safety metrics	ex-ante design choice
Group messaging	8	6	None	US1: op&#65533;on to accept or decline an invite to a group chat	None	None
Encrypted messaging	11	3	None	None	None	
Direct messaging	16	6	Limited to user controls: 9A, 9B Plus 7A: Default settings for child users where services are high risk for CSAM	Limited to user controls: US2, US3	None	
Ephemeral messaging	N/A	2	N/A	None	N/A	None
Anonymous user profiles	16	5	9C has recommendations re user labelling schemes, but this is	None	None	None

Functionality	**Illegal harms offences**	**Children's PPC, PC or NDC**	**Code of practice: ex ante mitigations**		**Code of practice: ex post mitigations**	
	17 in total (updated with animal cruelty offence & s127(1))	9 in total	Illegal harms	Children	Illegal harms	Children
			only limited to services at risk of fraud or the foreign interference offence			
Fake user profiles	14	4	As above 9C	None	None	None
Business model - inc small, fast-growing services; ad revenue	7	3	None	None	None	None
Payment facility	2	0	None		None	
User location	4	1	Included in A7 default settings measures, but only limited to services at high risk of grooming		None	
UGC search facility	5	3	None		None	Limited: Signpost children to support services when they search for harmful content (high or medium risk): US5
Posting goods or services for sale	8	0	None		None	
Building lists or directories	2	0	None		None	

COMPARISON OF FUNCTIONALITIES WITH SEARCH CODE OF PRACTICE MITIGATIONS (ANNEX 8): SUMMARY TABLE

NB the analysis of the search functionalities that cause harm is less detailed and presented in a different way to the evidence in the user-to-user sections of both consultations.

Functionality	**Illegal harms**	**Children's PPC, PC or NDC**	**Code of practice: ex ante mitigations**		**Code of practice: ex post mitigations**	
			Illegal harms	Children	Illegal harms	Children
Typing in searches for illegal / specified content	8	Not defined	Limited: provision of warnings for CSAM searches; and provision of suicide prevention information in relation to suicide/self-harm searches	None	Search moderation & takedown: 4A-F - these measures largely replicate the user-to-user content moderation measures but with 4A applying to deindexing or deranking illegal content. An additional deindexing measure applies to CSAM URLS (4G)	Equivalent as for illegal harms: Measures SM1-7
Ranking	-	N/A	None	None	As above	As above.
Reverse image search	1	Not defined	None	N/A	None	N/A
Search prediction or personalisation	3	Not defined	None	N/A	Limited: requires action when there	Limited: offer users means to

Functionality	Illegal harms	Children's PPC, PC or NDC	Code of practice: ex ante mitigations		Code of practice: ex post mitigations	
					is a user report that predictive search suggestions are directing users to priority illegal content	easily report predictive search suggestions relating to PPC and PC (SD1); provide crisis information in response to searches relating to suicide, self-harm and eating disorders (SD2)
Revenue models	2	Not defined	None	None	None	None
Commercial profile/size	-	Not defined	None	None	None	None
Gen AI/chat bots	-	Not defined	None	None	None	None

COMPARISON OF ILLEGAL HARMS IDENTIFIED FUNCTIONALITIES (VOLUME 2 and FURTHER CONSULTATION) WITH CODE OF PRACTICE MITIGATIONS (ANNEX 7) - USER TO USER SERVICES - FULL TABLE

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
CONTENT FUNCTIONALITIES			
Posting content	**Terrorism** **Grooming*** **CSAM** **Suicide & self-harm*** **Harassment, stalking, threats and abuse*** **Hate offences*** **Controlling or coercive behaviour*** **Drugs offences** **Unlawful immigration** **Intimate image abuse** **Proceeds of crime offences** **Fraud** **Foreign Interference offence** **False communications offence** **Epilepsy trolling**	**Limited** A9 (enhanced user controls) sets out that large services at high risk of offences marked * in LH column (plus suicide/self-harm & controlling and coercive behaviour) and that hav e user profiles, and at least one of three functionalities (user connection, posting content, communication including DM and commenting on content) allow blocking or muting of users. The Government produced its own "best practice" guide for safety by design for platforms that enabled private or public interaction in 2021: https://www.gov.uk/guidance/private-and-public-channels-improve-the-safety-of-your-online-platform	**Extensive** Content is primarily dealt with in the codes via moderation: ● 4A: swift takedown ● 4B: internal content policies (only for large and multi-risk services) ● 4C: performance targets (ditto) ● 4D: prioritisation of review of content (ditto) ● 4E: resourcing ● 4F: moderator training There are specific, detailed measures re hash-matching for CSAM and detection of CSAM URLs P45: The definition table at the end of the codes says re "content"; "*For the avoidance of doubt, comments, titles and descriptions are considered to be 'content' within this definition, as are livestreaming videos or audio, and hyperlinks*."

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
Commenting on content	**Terrorism** **CSAM** **Grooming** **Suicide and self harm** **Harassment, stalking, threats and abuse** **Hate offences** **FIrearms offences** **Fraud offences** Epilepsy trolling Cyberflashing **Animal cruelty** Section 127(1): obscene content	**Limited** A9 also sets out (for services that meet the same condition as above) that users should be able to disable comments.	**Extensive (as per content above)**
Hyperlinks - eg use to direct users to more extreme content	**Terrorism** **CSAM** Suicide and self-harm **Hate offences** Drugs offences **Extreme pornography** **Foreign interference offence** Epilepsy trolling **Section 127(1): obscene content**	**None recommended**	**Extensive (as per content above)**
Reposting or forwarding content	**Suicide and self-harm** **Harassment, stalking, threats and abuse** **Intimate image abuse** Proceeds of crime offences	**None recommended.**	**Limited** Section A6 (terms of service) obliquely covers this in referring to specifying “how the provider will minimise the

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
	Foreign Interference offence Animal cruelty **Section 127(1): obscene content**		length of time" illegal content is present"
Posting images or videos	**Intimate image abuse** **Animal cruelty** **Section 127(1): obscene content**	**None recommended.**	**Extensive (as per content above)** P45: The definition table at the end of the codes says re "content"; "For the avoidance of doubt, comments, titles and descriptions are considered to be 'content' within this definition, as are livestreaming videos or audio, and hyperlinks."
Livestream	Terrorism **Grooming** **CSAM** **Suicide and self-harm** **Hate offences** **Sexual exploitation of adults** **Intimate image abuse** Fraud (sextortion) **Cyberflashing** **Animal cruelty**	**None recommended** **NB the government produced its own "best practice" guide to "safety by design" for livestreaming in 2021: https://www.gov.uk/guidance/live-streaming-improve-the-safety-of-your-online-platform**	**Limited (except as type of "content")** P45: The definition table at the end of the codes says re "content"; "For the avoidance of doubt, comments, titles and descriptions are considered to be 'content' within this definition, as are livestreaming videos or audio, and hyperlinks." This does not consider how the functionality of livestreaming is used to facilitate the offences in the first place.

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
Livestream - Sending messages via livestream	**Grooming** Animal cruelty	**None recommended**	**Limited (except as type of "content")** P45: The definition table at the end of the codes says re "content"; "For the avoidance of doubt, comments, titles and descriptions are considered to be 'content' within this definition, as are livestreaming videos or audio, and hyperlinks." This does not consider how the functionality of livestreaming is used to facilitate the offences in the first place.
Live audio	Terrorism	**None recommended**	**Limited (except as type of "content")** P45: The definition table at the end of the codes says re "content"; "For the avoidance of doubt, comments, titles and descriptions are considered to be 'content' within this definition, as are livestreaming videos or audio, and hyperlinks."
Content tagging - Eg hashtags	**Suicide and self harm** **Hate offences** **Drugs offences** **Intimate image abuse** **Epilepsy trolling**	**None recommended.**	**None recommended.**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
Screen capturing or recording	**Terrorism** **Grooming** **CSAM** Intimate image abuse Cyberflashing	**None recommended**	**None recommended**
USER FUNCTIONALITIES			
User tagging	**Harassment, stalking, threats and abuse** Controlling or coercive behaviour **Firearms offences** Foreign interference offence **Epilepsy trolling**	**None recommended.**	**None recommended.**
User profiles	**Grooming*** **Harassment, stalking, threats and abuse*** **Hate offences*** **Drugs offences** **Unlawful immigration** **Sexual exploitation of adults** **Proceeds of crime offences** **Fraud** **Epilepsy trolling** **Cyberflashing**	**Limited** A9 (enhanced user controls) sets out that large services at high risk of offences marked * in LH column (plus suicide/self-harm & controlling and coercive behaviour) and that have user profiles, and at least one of three functionalities (user connection, posting content, communication including DM and commenting on content) allow blocking or muting of users	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
		NB the Government produced its own "best practice" guide for "safety by design" for user profile functionality in 2021: https://www.gov.uk/guidance/users-account-details-and-activity-visible-to-others-improve-the-safety-of-your-online-platform	
User connections	**Terrorism** **Grooming*** **Harassment, stalking, threats and abuse*** **Controlling or coercive behaviour*** **Drugs offences** **Fraud** **Foreign Interference offence** **Epilepsy trolling** Animal cruelty Section 127(1): obscene content	**Limited** Section A7 includes recommendation (only for services at high-risk of grooming, or a large service at medium-risk of grooming) that default settings do not include children in network expansion prompts and connection lists A9 (enhanced user controls) sets out that large services at high risk of offences marked * in LH column (plus suicide/self-harm) and that have user profiles, and at least one of three functionalities (user connection, posting content, communication including DM and commenting on content) allow blocking or muting of users	**None recommended**
User search	Grooming	**None recommended**	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
	Cyberflashing		
User groups	Grooming CSAM **Suicide and self-harm** Controlling or coercive behaviour **Drugs offences** **Unlawful immigration** **Extreme pornography** **Fraud** Foreign interference offence **Animal cruelty** Section 127(1): obscene content	**None recommended**	**None recommended**
User base profile	Terrorism (demography) **Grooming, CSAM (children)** **Harassment etc (women)**	**None recommended**	**Limited** Recommendation 4E re content moderation says the services needs to take into account "the particular needs of its United Kingdom user base as identified in its risk assessment, in relation to languages." Recommendation 5B re complaints says "In designing its complaints processes for relevant complaints, including its reporting tool or function, the provider should have regard to the particular needs of its United Kingdom user base as identified in its risk assessment. This

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
			should include the particular needs of: a) children (for services likely to be accessed by children and considering the likely age of the children using that service); and b) disabled people" Neither of these address the way in which the service design might ensure that users identified in the risk assessment might be protected in the first instance from harm.
RECOMMENDER SYSTEMS			
Recommender systems	Terrorism* **Grooming/CSAM*** **Suicide and self harm*** Harassment, stalking, threats and abuse* **Hate offences*** Controlling or coercive behaviour **Drugs offences*** **Extreme pornography*** Intimate image abuse* **Foreign Interference offence*** **Epilepsy trolling** Animal cruelty **Section 127(1): obscene content**	**None recommended**	**Limited** Section A6 (terms of service) obliquely covers this in referring to specifying "how the provider will minimise the length of time" illegal content is present" Section A8 (recommender system testing) requires (but only for services that conduct test and are at a high risk of two types of the harms marked * in the LH column) that it analyse the safety metrics from its tests to understand if changes to the recommender system would increase the risk of users

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
			encountering illegal content There is no upstream requirement in the code to ensure that services to consider the design of their recommender systems in the first place.
MESSAGING FUNCTIONALITIES			
Group messaging	Terrorism **CSAM** **Suicide and self-harm** **Intimate image abuse** Intimate image abuse Fraud **Animal cruelty** Section 127(1): obscene content	**None recommended**	**None recommended**
Encrypted messaging	**Terrorism** **Grooming** **CSAM** **Drugs offences** **Sexual exploitation of adults** Intimate image abuse **Proceeds of crime offences** **Fraud** **Foreign Interference offence** **False communications offence** **Animal cruelty**	**None recommended**	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
Direct messaging	**Terrorism** **Grooming*** **CSAM** **Harassment, stalking, threats and abuse*** **Hate offences*** **Controlling or coercive behaviour*** **Drugs offences** **Firearms offences** **Sexual exploitation of adults** Intimate image abuse **Proceeds of crime offences** **Fraud** **False communications offence** **Cyberflashing** Animal cruelty	**Limited** A9 (enhanced user controls) sets out that large services at high risk of offences marked * in LH column (plus suicide/self-harm) and that have user profiles, and at least one of three functionalities (user connection, posting content, communication including DM and commenting on content) allow blocking or muting of users A7 includes recommendation (only for services at high-risk of grooming, or a large service at medium-risk of grooming) that as a default, child users should not receive messages from a non-connected user; and if the service does not have user connections, child users can actively confirm if they want to receive a direct message from someone they don't know	**None recommended**
Direct messaging - Sending images via messaging	Grooming	**Limited (see above)**	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
ANONYMOUS/FAKE ACCOUNTS			
Anonymous user profiles	Terrorism Grooming **CSAM** **Suicide and Self-Harm** **Harassment, stalking, threats and abuse** **Hate offences** Drugs offences **Firearms offences** **Extreme pornography** **Intimate image abuse** **Fraud** **Foreign Interference offence** **False communications offence** **Epilepsy trolling** Cyberflashing Animal cruelty	**Limited** A9C: user verification/labelling schemes sets out that large services at high risk of either or both of fraud and the foreign interference offence; and has user profiles under a relevant scheme (notable users or monetised scheme) should have consistently applied policies to reduce the risk of harm to users associated with that scheme. These policies should include “how the provider will treat relevant users and the content they post including recommender systems, content curation, user reporting and complaints, quality assurance, fact checking, content moderation, account security” There are no recommended measures to address the role of anonymous or fake user profiles in the list of offences in the LH column	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
		NB the Government produced its own “best practice” guide to “afety by design” for anonymous or multiple account creation in 2021; https://www.gov.uk/guidance/anonymous-or-multiple-account-creation-improve-the-safety-of-your-online-platform	
Fake Profiles	Grooming **CSAM** Suicide and self-harm **Harassment, stalking, threats and abuse** **Controlling or coercive behaviour** **Unlawful immigration** **Sexual exploitation of adults** **Intimate image abuse** **Proceeds of crime offences** **Fraud** **Foreign Interference offence** **False communications offence** **Epilepsy trolling** Animal cruelty	**Limited** A9C: user verification/labelling schemes sets out that large services at high risk of either or both of fraud and the foreign interference offence; and has user profiles under a relevant scheme (notable users or monetised scheme) should have consistently applied policies to reduce the risk of harm to users associated with that scheme. These policies should include “how the provider will treat relevant users and the content they post including recommender systems, content curation, user reporting and complaints, quality assurance, fact checking, content moderation,	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
		account security” There are no recommended measures to address the role of anonymous or fake user profiles in the list of offences in the LH column.	
MISCELLANEOUS			
Business model: ● Low capacity and early-stage services	Terrorism	**None recommended**	**None recommended/** This is an issue re the small vs large differentiation, covered elsewhere in our analysis.
Business model: ● Ad revenue	**Foreign Interference offence** **Hate Offences** **Sexual Exploitation of Adults** **Extreme Pornography** Animal cruelty **Section 127(1): obscene content** Section 127(1): obscene content	**None recommended**	**None recommended**
Payments/transactions capability	Terrorism **CSAM**	**None recommended**	**None recommended**
User location	Grooming **Harassment, stalking, threats and abuse**	**Limited** Section A7 includes	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
	Controlling or coercive behaviour **Sexual exploitation of adults**	recommendation (only for services at high-risk of grooming, or a large service at medium-risk of grooming) that as a default automated location information displays are turned off child users. This does not address the role of user location functionality wrt to VAWG.	
Editing visual media	Grooming CSAM Hate offences Controlling or coercive behaviour **Extreme pornography** Intimate image abuse Foreign interference offence **False communications offence** Epilepsy trolling	**None recommended**	**None recommended**
Downloading content	CSAM **Extreme pornography** Intimate image abuse	**None recommended**	**None recommended**
UGC content searching or filtering	Suicide and self harm Drugs offences **Firearms offences** **Extreme pornograrphy** **Proceeds of crime offences**	**None recommended**	**None recommended**

Functionality	**Related Offences** *offences in bold are where the functionality is highlighted in the introductory summary	**Code of practice: systemic or ex-ante mitigation?**	**Code of Practice: recommended ex-post mitigation?**
	Fraud Animal cruelty Section 127(1): obscene content		
Posting goods or services for sale	**Drugs offences** **Firearms offences** **Unlawful immigration** **Sexual exploitation of adults** **Extreme pornography** Proceeds of crime offences **Fraud** Animal cruelty	**None recommended**	**None recommended**
Building lists or directories	CSAM Extreme pornography	**None recommended**	**None recommended**

COMPARISON OF ILLEGAL HARM FUNCTIONALITIES (VOLUME 2 and FURTHER CONSULTATION) WITH CODE OF PRACTICE MITIGATIONS (ANNEX 8) - SEARCH SERVICES - FULL TABLE

The analysis on the functionalities related to user access to illegal content via search services is presented in a different way by Ofcom in volume 2: a high-level summary narrative that talks about functionality in relation to particular offences, rather than an offence-by-offence analysis. The table below includes some of the core narrative for each functionality in volume 2, along with a similar assessment of ex-ante or ex-post measures as per user-to-user services. NB the Government produced its own "best practice" guide for "safety by design" for search functionality in 2021: https://www.gov.uk/guidance/search-functionality-improve-the-safety-of-your-online-platform (It is not referenced by Ofcom.)

Functionality	**Related Offences**	**Code of practice: systemic or ex-ante measures?**	**Code of practice: ex-post measures?**
Typing in searches for illegal content 6T.33 Functionalities related to general search "include the underlying potential for illegal content on webpages indexed by search services to appear in, or via, search results; the features visible to users to optimise search results (such as recommended searches, autocomplete suggestions); and those which determine results behind the scenes (such as ranking algorithms) … These service characteristics are designed largely to optimise the accuracy and usefulness of	Terrorism Hate Extreme pornography CSAM Firearms offences Drugs offences Fraud Suicide and self harm	Limited 7B: provision of CSAM content warnings - applies to large general search services "The provider should employ means to detect and provide warnings in response to search requests of which the wording clearly suggests that the user may be seeking to encounter CSAM and uses terms or combinations of letters and symbols that explicitly relate to CSAM. Warnings should not be provided in response to search requests using terms which, on their face, do not relate to CSAM." 7C: provision of suicide crisis	Extensive Content is primarily dealt with in the codes via the search moderation duties Eg: 4A: The provider should have systems or processes designed to deindex or downrank illegal content of which it is aware (a 'search moderation function') - applies to all services. 4B: internal content policies (large and multi-risk) 4C: performance targets (ditto) 4D: prioritization for review (ditto) 4E: resourcing (ditto) 4F: training (ditto) Plus 4G: deindexing CSAM URLS (all services)

Functionality	Related Offences	Code of practice: systemic or ex-ante measures?	Code of practice: ex-post measures?
search results to users. Where a user is intentionally seeking out illegal content – which is considered the most likely situation in which a user would encounter content that amounts to an offence – these same optimising characteristics have the unintended consequence of helping that user encounter illegal content.		prevention information - this is to be provided in response to a) "general queries regarding suicide; and b) queries seeking specific, practical or instructive information regarding suicide methods.	
Ranking 6T.28: "General search services use proprietary algorithms ('ranking') to perform this prioritisation function. The ranking process uses factors such as how closely the search query is matched and the website's functionality and authority (the perceived value of the site's content and how often it is linked to by other sites). As with all functionalities, the ranking process is designed to provide accurate and		None recommended	Extensive (see above) 4A: The provider should have systems or processes designed to deindex or downrank illegal content of which it is aware (a 'search moderation function')

Functionality	Related Offences	Code of practice: systemic or ex-ante measures?	Code of practice: ex-post measures?
reliable content, but it can be manipulated by users to increase the likelihood of illegal content being displayed to users. For example, the tactic of keyword stuffing (filling a web page with keywords or numbers in an attempt to manipulate rankings in search results) has been identified in research looking at how easily illegal content relating to fraud can be accessed via search services."			
Reverse image search Vol 2 notes that evidence of how this is used in relation to searches to purchase drugs and that, while the evidence is limited on other offences, "it is possible that the reverse image search functionality also presents opportunities to access content relating to other prohibited items" (para 6T.36)	Drugs offences	None recommended	None recommended

Functionality	Related Offences	Code of practice: systemic or ex-ante measures?	Code of practice: ex-post measures?
Search prediction or presonalisation 6T.37 "It is reasonable to assume that these functionalities can increase the risk of accessing illegal content amounting to a range of offences, unless effective mitigations are in place to prevent this, or indexed content is blocked."	Suicide or self harm Hate Fraud	None recommended	Limited 7A: removal of predictive search suggestions (large general search services that use predictive search functionality) NB This measure only requires those services to provide a "means to easily report predictive search suggestions which they consider to direct users towards priority illegal content" NOT ex-ante measures to prevent such predictive search suggestions arising in the first place.
Revenue models - ad-based models Evidence suggests that advertisements on search services may be misused for illegal activity.	Coercive control Foreign interference offences	None recommended	None recommended
Commercial profile/size "Despite the limited evidence, we consider that *search services that are low-capacity or at an early stage in their lifecycle may face an increased risk of*		None recommended	None recommended

Functionality	Related Offences	Code of practice: systemic or ex-ante measures?	Code of practice: ex-post measures?
harm on their services" (6T.46)			
Gen AI/chat bots Volume 2 says "Research indicates that search services integrated with GenAI chatbots could be used to facilitate fraud whereby a perpetrator could covertly collect personal information including the user's name, email, and credit card information. There is also evidence illustrating how such services could be used to share malicious links and steer search results towards manipulated content." (para 6T.18)	Fraud	None recommended	None recommended