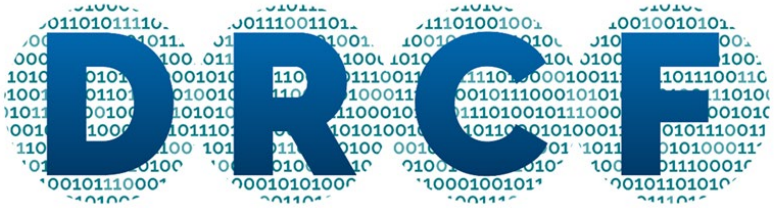


Digital Regulation Cooperation Forum

Ofcom
making communications work for everyone

ico.
Information Commissioner's Office

Online safety and data protection

A joint statement by Ofcom and the Information Commissioner's Office

25 November 2022

Executive summary

As the bodies responsible for regulating data protection and online safety in the UK, the Information Commissioner's Office (ICO) and Ofcom are both committed to protecting people online.

We want to see online services do more to keep users safe and protect their privacy. In 2021, more than three in four over-13-year-olds reported having at least one harmful online experience in the previous four weeks,[1] while fewer than three in ten people trusted companies and organisations storing their personal information.[2]

We want to see organisations design their online services with both privacy and safety in mind. There are strong synergies between these objectives. For example, online services that fail to protect users' personal information could leave them vulnerable to being identified or targeted, having their location tracked, or being sent harmful communications.

We recognise that there are sometimes tensions between safety and privacy. For example, to protect users' safety online, services might need to collect more information about their users, the content they view and their behaviour online. To protect users' privacy, services can and should limit this data collection to what is proportionate and necessary.

Take age assurance. Online services can use age assurance to identify children in order to uphold their privacy and safety, for example making sure geolocation is switched off or that children don't access harmful content. However, this should not be used as a pretext for excessive tracking of users' online habits. Such data collection should be limited to what is necessary to accurately classify a user as a child.

After the Online Safety Bill passes, relevant online services will need to comply with both online safety and data protection rules. There can be no space for services to argue that they could not comply with new online safety requirements, because of data protection rules, or vice versa. We will be working hand-in-hand to make sure users of online services are protected.

The ICO and Ofcom have worked effectively together for many years. We share similar principles in our approach to regulation: transparency, accountability, proportionality and consistency, and a commitment to taking action where it is most needed. By aligning our approaches, we believe we can safeguard people more effectively while also minimising the cost of compliance with our regimes.

Our collaboration has deepened since 2020, when the ICO launched the Children's code and Ofcom took on powers to regulate UK video-sharing platforms (VSPs). We worked together closely to ensure that our respective guidance was aligned, making it easier for VSPs to comply with both regimes. We are working together closely to share intelligence and tackle non-compliance.

[1] The Online Experiences Tracker (2021/22): Summary report. https://www.ofcom.org.uk/research-and-data/online-research/internet-users-experience-of-harm-online

[2] Information Rights Strategic Plan: Trust and Confidence June 2021. https://ico.org.uk/media/about-the-ico/documents/2620165/ico-trust-and-confidence-report-290621.pdf

We co-founded the Digital Regulation Cooperation Forum with the Competition and Markets Authority the same year, with the Financial Conduct Authority joining subsequently. Through the forum we have worked together to research attitudes to tools such as age assurance, align positions on the regulation of algorithmic processing, and examine future developments such as the metaverse.

Our partnership is now stepping up another gear, in anticipation of Ofcom taking on new duties in 2023 under the Online Safety Bill. Our ambitions are twofold:

1. We want **users of online services** to have confidence that their safety and privacy will be upheld and that we will take prompt and effective action when providers fail in their obligations.

2. We want **providers of online services** of all sizes to comply with their obligations and to continue to innovate and grow, supported by regulatory clarity and free from undue burden.

To do this, we will maximise coherence between the data protection and online safety regimes and work together to promote compliance with them:

- **Maximising coherence**: We will ensure that our policies are consistent with each other's regulatory requirements and guidance and take into account each other's perspective. We will seek solutions that enhance users' safety and preserve their privacy. Where there are tensions between privacy and safety objectives, we will provide clarity on how compliance can be achieved with both regimes.

Ofcom will prepare codes of practice and guidance for online services on compliance with the online safety regime and will consult the **ICO**, amongst others, in the preparation of these.

The **ICO** will prepare guidance on data protection expectations for online services deploying safety technologies (e.g. age assurance, content moderation) and will consult **Ofcom**, amongst others, in its preparation.

- **Promoting compliance**: We will work together to help industry comply with both online safety and data protection requirements, with a particular emphasis on supporting innovators to thrive and small businesses to grow. We will take action against services that don't meet their obligations, sharing information and intelligence as appropriate and coordinating approaches to compliance and enforcement.

This joint statement sets out how we will work together in more detail. We will reaffirm our cooperation through a renewed memorandum of understanding, which we will update in the coming year in light of Ofcom's new responsibilities under the Online Safety Bill.

1. Introduction

Data protection and online safety are both fundamental issues for users of online services. In 2021, over six in ten (62%) UK internet users reported that they had experienced at least one instance of potentially harmful behaviour or content online in the previous four weeks.[1] Moreover, 77% of the UK public say that protecting their personal information is essential to them.[2]

About Ofcom

Ofcom is the UK's regulator for the communications services that we use and rely on each day, with the stated aim of making communications work for everyone. One of Ofcom's key strategic goals for 2022/23 is establishing regulation of online safety,[3] by using existing powers to regulate video-sharing platforms[4] (VSPs) as well as continuing preparations to implement new online safety regulation being established through the Online Safety Bill (the Bill).[5] Introduced in the UK Parliament on 17 March 2022, the Bill is currently undergoing parliamentary scrutiny. We have approached our discussion here based on the current drafting of the Bill and the broad principles it sets out.[6]

The Bill sets rules for sites and apps such as social media and messaging platforms, as well as other services that people use to share content online, and search engines. These companies will have new duties to protect UK users by assessing and responding to risks of harm. The Bill will also require providers of online pornography to ensure children are not normally able to encounter pornographic content. Ofcom will give guidance and set out codes of practice on how regulated services can comply with their duties, and in many areas Ofcom will be required by statute to consult the ICO on relevant data protection requirements. Recommended measures in codes of practice must be designed in light of the importance of protecting the privacy of users and must, where appropriate, incorporate safeguards to protect users' privacy.

Regulated user-to-user and search services must be able to demonstrate that they have had regard to the importance of protecting users from a breach of statutory provisions or rules of law concerning privacy (including data protection law) when deciding on and implementing their safety measures and policies to comply with their duties of care under the Bill.[7] If services follow recommended measures in

[3] Ofcom's plan of work 2022/23: Making communications work for everyone. https://www.ofcom.org.uk/consultations-and-statements/category-2/plan-of-work-2022-23

[4] VSPs are a type of online video service where users can upload and share videos with members of the public, such as Snapchat, TikTok and Twitch. Ofcom was given powers to regulate VSPs in autumn 2020 under transposed EU law which was implemented through Part 4B of the Communications Act 2003. In October 2021, we published guidance for VSPs established in the UK: see Video-sharing platforms: Ofcom's plan and approach.

[5] The Online Safety Bill was was introduced into Parliament in March 2022. A further version of the Bill, as amended at Committee stage in the House of Commons, was published on 28 June 2022.

[6] This statement is based on our current understanding of the Bill as it stands, and the insight we have gained from our joint discussions and input from stakeholders. As the Bill continues its passage through Parliament, we will continue to develop our common understanding of the links with data protection.

[7] Privacy duties on user-to-user services are set out in clause 19 of the Bill, and those for search services are contained in clause 29. Both must have regard to the importance of protecting users from privacy breaches. Category 1 user-to-user services (the highest reach services with the highest risk functionalities) must also publish an assessment of the impact on freedom of expression and privacy of any measures adopted to comply with their online safety duties.

codes which incorporate safeguards to protect users' privacy, they will be treated as complying with these duties.

About the ICO

The ICO is the UK's independent regulator established to uphold information rights in the public interest, covering a range of relevant legislation. The UK data protection regime requires online service providers to use, share and innovate with personal data responsibly and holds them accountable for their practices. It requires that online service providers use people's data safely, securely and transparently, building public trust in these services.

Current relevant UK data protection legislation includes the Data Protection Act 2018, the UK General Data Protection Regulation, and the Privacy and Electronic Communications Regulations 2003. Together these provide a risk-based framework for making sure the processing of personal data respects the fundamental rights and freedom of individuals, including the right to privacy. Organisations processing personal data, including to meet their obligations under the online safety regime, must comply with the data protection principles[8] and make sure users are able to exercise their personal data rights.[9] Organisations need to consider the risks involved in their processing of personal data and implement proportionate safeguards to mitigate the risk of harm to the individuals whose personal data they are processing.

The processing of children's personal data requires particular care. The ICO's Children's Code is a statutory code of practice under the Data Protection Act 2018 that applies to online services that are likely to be accessed by children.[10] It applies to many apps, programs, search engines, websites, streaming services and online games, including services likely to come within scope of the online safety regime.

The code addresses how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the development needs of, children. It sets out standards which online services should meet in order to provide better privacy protections for children. If services do not conform to the code, they are likely to find it more difficult to demonstrate compliance with data protection law.

Our shared vision

The online world is changing, and with it the regulatory landscape. Ofcom and the ICO will work together to provide a clear and coherent regulatory landscape for online services that is proportionate,

[8] More detail can be found in the ICO's guide to data protection. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles

[9] Users' data protection rights are set out in Article 12-22 of the UK GDPR. More detail can be found in the ICO guide to data protection. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

[10] Age appropriate design: a code of practice for online services. https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

transparent and outcome-focused, and to regulate in a way that helps online service providers comply with their legal obligations and create safe and trusted online spaces. Our shared ambition is twofold:

1. We want **users of online services** to have confidence that their safety and privacy will be upheld and that we will take prompt and effective action when providers fail in their obligations.

2. We want **providers of online services** of all sizes to comply with their obligations and to continue to innovate and grow, supported by regulatory clarity and free from undue burden.

This statement is primarily intended for online service providers that are likely to be regulated under the online safety regime, but it will also be of interest to other stakeholders as an indication of our joint direction of travel. It sets out our shared views on:

- The links between data protection and online safety;
- The requirement that online service providers comply with both online safety regulation and data protection regulation; and
- How we already work together to promote regulatory coherence, how we plan to further deepen our existing strong links, and how we will support compliance with our respective regimes.

2. Links between online safety and data protection

Online safety and data protection can interact in a variety of ways. The design of online services can help to enhance users' privacy and online safety - though there is also the risk that some features or functionalities that enhance privacy could have a negative impact on online safety, or vice versa. Some tools and technologies to detect and limit the spread of illegal and harmful content require collection of user data. If online services don't have appropriate data protection measures in place there is a risk that data collected about users for online safety purposes could be used in privacy-intrusive ways, or the data could be processed insecurely leading to a security breach. Equally, services that minimise the amount of user data they collect may find that they are constrained in the choice of safety solutions they can use.

One way to think about how online safety and data protection considerations interact is by looking at the end-to-end journey of how people use online platforms, and how the platforms deal with content.[11] There is likely to be interplay between online safety and data protection in a number of areas. These include signing on to online services, user participation in online services, and analysing content and identifying harmful activity.

Signing in to online services

The type of personal information that users must provide to access platforms varies. Some online services offer access to content without the need to subscribe or create a profile, while others might require users to create a profile or verify certain information about themselves (for example, their name, age and contact email address) before they can access services or specific types of content.[12] Some services might offer users tools for people to verify their identity so other users of the service have some assurance that they are who they say they are. In relation to protecting children, age assurance measures can be used in order to stop children below a certain age accessing services or age-inappropriate content.[13]

The collection, use and storage of this personal information is regulated by data protection law. For example, when services verify user identity or age, services should only collect the personal information from users that is necessary for this purpose. Where a service needs to make sure its users are over a qualifying age, its data collection should be limited to ensuring that the user is above that age, rather than collecting and processing their exact age. Any further use of personal data for an unconnected purpose is allowed only where the new purpose is compatible with the original purpose, user consent

[11] Ofcom has conducted some more detailed research on online user journeys. See https://www.ofcom.org.uk/research-and-data/online-research/asparc-model-of-online-platforms

[12] Many online services set a minimum age for use of the service. For example, popular social media services such as Facebook, Instagram, TikTok, Snapchat, Twitter and YouTube have a minimum age of 13.

[13] Age assurance is a broad term that refers to the spectrum of methods that can be used to be informed about a user's age online. The term may also be used to refer to the level of confidence that a platform has in the age of its users. This is discussed further in Ofcom's guidance for video sharing platforms on measures to protect users from harmful material. https://www.ofcom.org.uk/online-safety/information-for-industry/vsp-regulation/guidance-protecting-users-from-harmful-material

has been given to the new purpose or there is another provision in law allowing the service to carry out the processing.

User participation in online services

One way in which online service providers present content is by using content recommendation algorithms, or systems which aim to rank or return content that matches a user's perceived interests. A large number of factors are used in order to do this, including information that constitutes the user's personal data. The ways in which algorithms work can lead to a range of different outcomes for users, including directing users to content that they will interact with for longer, or encouraging users to engage with content posted by their friends. But they can also lead to harmful content being amplified.

Where personal data is used to determine the content served to users, data protection law will apply. For example, services need to be transparent about the way in which they process personal data in order to make content recommendations[14]. This extends to data processing in connection with the online safety measures that are incorporated into their content recommendation systems, such as identifying vulnerable users who could be placed at risk by certain types of content.

More specifically, online services that process children's data will have to conform to the standards of the ICO's Children's Code, including standard 5 on detrimental use of data. They should make sure their use of content recommendation algorithms does not involve processing children's data in ways that have been shown to be detrimental to their wellbeing or that go against industry codes of practice, other regulatory provisions, or government advice.

Analysing content and identifying harmful activity

There is a range of different measures which can be used by online services to promote online safety and minimise the risks of users encountering content which is illegal or harmful and contrary to their terms of service. This includes automated content classification systems, which use algorithms designed to identify and classify whether content is illegal or harmful. Some platforms might also choose to use techniques which seek to analyse patterns of potentially harmful user behaviour (for example where people seek to contact potentially vulnerable users, such as children, who are not otherwise known to them, or with a view to looking at patterns of use that might indicate use of a 'bot').

Where platforms use automated processes to link identifiable individual users to potentially illegal or harmful activity, data protection law requires that information linked to individuals or to their accounts is processed responsibly and fairly. For example, services must be transparent about how they use personal data to make decisions, use no more personal data than is necessary to do so, and ensure that the processes that link users to illegal activity do so with an acceptable level of accuracy. Processing personal data is unlikely to be necessary if a service can achieve its purpose of identifying users carrying out illegal or harmful activity by some other less intrusive means, or by processing less personal data.

[14]The transparency requirements of data protection law are discussed in more detail in the ICO's guidance for organisations on transparency under the UK GDPR. https://ico.org.uk/for-organisations/accountability-framework/transparency/

These examples are not intended to be comprehensive, and other interactions between online safety and data protection will occur. A key focus of our work together will be to map out the interactions in more detail.

3. Working together

Ofcom and the ICO have worked effectively together for many years. We share similar principles in our approach to regulation: transparency, accountability, proportionality and consistency, and a commitment to taking action where it is most needed. Most recently, we have collaborated on issues including:

- VSP regulation and the ICO's Children's code;
- age assurance; and
- DRCF-facilitated joint projects, such as on algorithms and end-to-end encryption.

Our culture of collaboration across the various areas of our remits is formalised through a memorandum of understanding (MOU).[15] The MOU sets out the roles and functions of each regulator, our powers and duties, the principles of cooperation and the purposes and the legal bases for sharing information with one another. We will review the MOU in the coming year in light of Ofcom's new responsibilities under the Online Safety Bill.

VSP regulation and the ICO's Children's code

Introduced on 1 November 2020,[16] the VSP framework sets rules with which UK-established VSPs must comply to protect users from the risk of viewing videos and advertising containing harmful material, and to uphold certain standards around advertising.[17] In particular, all notified VSPs must take appropriate measures to protect:

- all users from videos that are likely to incite violence or hatred against particular groups;
- all users from videos which include content which would be considered a criminal offence under laws relating to terrorism; child sexual abuse material, and racism and xenophobia; and
- under-18s from videos containing pornography, extreme content and other material which might impair their physical, mental or moral development.[18]

VSP regulation works in tandem with data protection regulation and the ICO's Children's Code. During the development of the VSP regime, the ICO and Ofcom worked together closely to make sure our respective guidance was aligned, making it easier for online services to comply with both regimes. Since then, we have further strengthened our operational links, established open communications, and shared knowledge to build our related expertise. We are now working together closely to share intelligence on non-compliance and consider potential solutions.

---

[15] https://www.ofcom.org.uk/__data/assets/pdf_file/0027/165933/mou-ico-ofcom.pdf

[16] Part 4B of the Communications Act 2003. https://www.legislation.gov.uk/ukpga/2003/21/part/4B

[17] The Advertising Standards Authority has been designated to administer day-to-day regulation of VSP-controlled advertising, with Ofcom as a statutory backstop regulator. See Statement: The regulation of advertising on video-sharing platforms. https://www.ofcom.org.uk/consultations-and-statements/category-1/regulation-of-advertising-on-vsp

[18] Guidance for video sharing platforms on measures to protect users from harmful material. https://www.ofcom.org.uk/online-safety/information-for-industry/vsp-regulation/guidance-protecting-users-from-harmful-material and Guidance for providers on advertising harms and measures, https://www.ofcom.org.uk/consultations-and-statements/category-1/guidance-vsp-harmful-material-measures

We have built on the foundation provided by the ICO-Ofcom MOU to agree a framework for our collaboration at working level in relation to VSPs specifically, and are putting in place a joint working framework to govern this work. We plan to hold joint workshops to consider examples of potential overlaps in our supervision and enforcement activities, to develop appropriate ways of working together on these.

Age assurance

Developing an aligned approach to age assurance has been a priority for our joint work to protect children online. Age assurance measures can be used by online services to identify the age of their users, and tailor their services or protect users from harmful material, depending on their age. When using age assurance tools, services must treat users' data appropriately to comply with data protection law.

Project teams from Ofcom and the ICO focusing on age assurance meet regularly to update each other on our regulatory activity, findings from relevant research, and our priorities in this area. Our ultimate aim for this engagement is to ensure a coherent approach to age assurance across our regimes.

Recently, we published joint research into children's and parents' attitudes to age assurance. [19] The research identified that most parents were positive about the concept of age assurance, but this could conflict with their desire for control and flexibility in parenting. It also found that families saw age assurance as most important for activities traditionally associated with age restrictions, but found those age restrictions to be less meaningful, and largely arbitrary, on social media and games platforms. Finally, broad support among parents and children for the principle of age assurance was tempered by concerns about privacy, parental control, children's autonomy and the usability of specific age assurance methods.

We will use this research to help build a shared understanding of privacy, trust, and effectiveness as they relate to users' engagement with age assurance tools and to ensure that our regulation delivers appropriate protections for young users while also protecting their privacy.

In the next phase of work, we plan to commission joint research into the accuracy of a range of age-assurance technologies. The findings of this research will allow our two organisations to better understand what we can reasonably expect of regulated services when it comes to age assurance, enabling us to make sure our guidance to industry is consistent and coherent.

Coordinating our activities in this way has driven efficiencies by allowing us to streamline our respective research programmes, avoid duplication and achieve a better understanding of age assurance with our combined resources. Ongoing knowledge sharing on age assurance will be a key strand of our future work on interactions between the online safety and data protection regimes, and where relevant will be taken into account in Ofcom's codes of practice and ICO guidance.

[19] Families' attitudes towards age assurance, research commissioned by the ICO and Ofcom (Revealing Reality). https://www.ofcom.org.uk/about-ofcom/how-ofcom-is-run/organisations-we-work-with/drcf

The Digital Regulation Cooperation Forum

Our two organisations work closely within the Digital Regulation Cooperation Forum (DRCF), which was established to promote coherence between regulatory regimes, collaboration on projects and capability building across regulators.[20]

For example, members of the DRCF are working together to continue improving our understanding of end-to-end encryption, to inform a joined up regulatory approach. In July, Ofcom and the ICO joined forces with the Financial Conduct Authority to hold a roundtable on end-to-end encryption.[21] This brought together voices from the digital technology industry, academia, civil society and the legal profession. The discussion covered a range of themes, including the importance of establishing common terminology and the benefits of regulators providing industry with greater clarity about their expectations.

Other areas of collaboration as part of the DRCF include joint work to promote improvements in algorithmic transparency, assess the implications of emerging technologies and enable deeper knowledge sharing across teams working on similar issues. These are set out in the DRCF Plan of Work for 2022/23.[22]

[20] DRCF Terms of Reference. https://www.gov.uk/government/publications/drcf-terms-of-reference/terms-of-reference

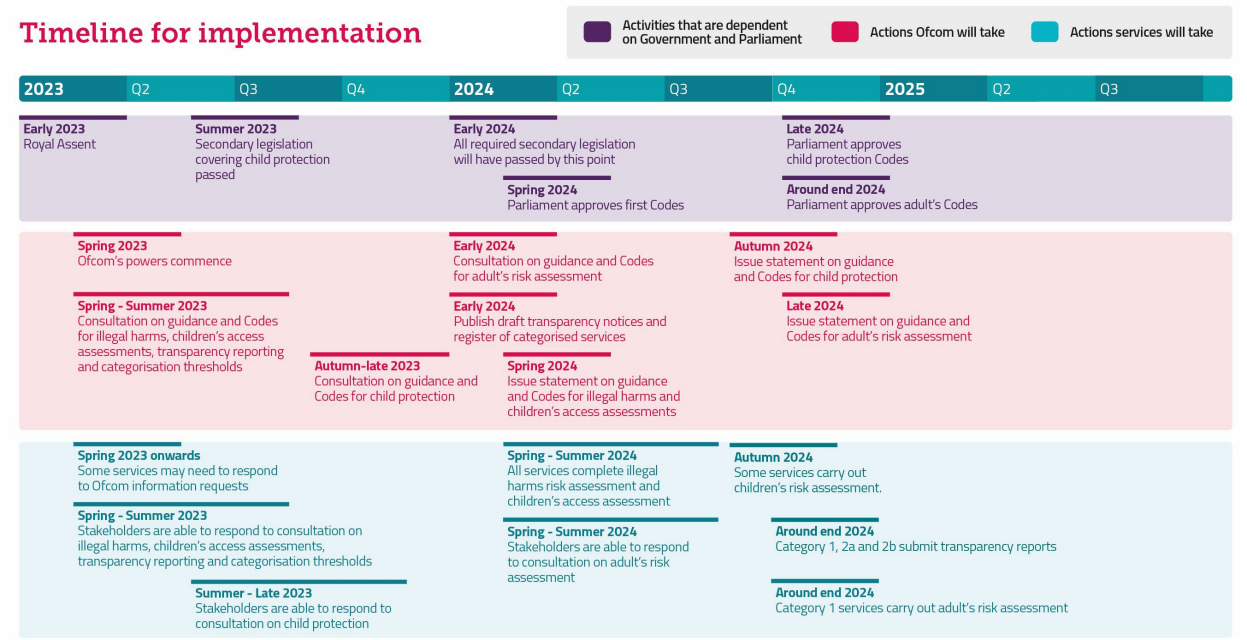
[21] DRCF roundtable on end-to-end encryption, hosted by the FCA, the ICO and Ofcom: summary report. https://www.gov.uk/government/publications/drcf-roundtable-on-end-to-end-encryption-hosted-by-the-fca-the-ico-and-ofcom-summary-report

[22] Digital Regulation Cooperation Forum plan of work for 2022/23. https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-2022-to-2023

4. Next steps

On 6 July 2022 Ofcom published a roadmap setting out plans for implementing online safety regulation, including initial timelines for each element of the regime (see Figure 1, below).[23] These plans are based on the Bill as introduced in the UK Parliament on 17 March 2022, and a planning assumption that the Online Safety Act will pass by early 2023.

Figure 1. Implementation of online safety regulation



As set out in our roadmap, once our powers come into force following Royal Assent we will move quickly to implement the regime, with a particular focus initially on the elements of the regime relating to illegal content and protecting children from harmful content.

- **Protecting people from illegal content.** Ofcom expects to consult on draft codes and risk assessment guidance in Spring 2023, with the first illegal content codes of practice likely to be issued around mid-2024. Services will need to comply with the safety duties in the Bill regarding illegal content once these codes come into force.
- **Protecting children from harmful content**. Ofcom expects to consult on draft child protection codes on harms to children in autumn 2023 and expects to issue final guidance and codes on harms to children in Autumn 2024. Services will need to comply with the safety duties in the Bill regarding protection of children once these codes come into force.

[23] Online Safety Bill: Ofcom's Roadmap to regulation. https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation

Ofcom and the ICO will work together throughout this roadmap process and beyond, to maximise coherence between the data protection and online safety regimes and to promote compliance with them both.

Maximising coherence

We will work together to ensure that our policies are consistent with each other's requirements and guidance. Where possible, we will seek solutions that enhance users' safety and preserve their privacy. Where there are tensions between privacy and safety objectives, we will provide clarity on how compliance can be achieved with both regimes.

Ofcom will engage with the ICO from an early stage in developing its proposals for the various codes and guidance required by the Bill in order to understand the data protection implications that may arise. The ICO must be consulted on the codes, and on guidance that is relevant to its remit under the Bill. Where appropriate, the ICO's formal responses to these consultations will be published.[24]

The ICO will publish its own expectations on how safety technologies that use personal data – such as user verification, user profiling, behaviour identification and content moderation – should be developed in line with data protection law. These will complement its existing Commissioner's Opinion on data protection expectations for age assurance technologies.[25] The ICO will consult Ofcom, among others, on this guidance ahead of relevant parts of the online safety regime coming into force.

Promoting compliance

Online service providers will need to collect, hold and process personal data in order to be able to assess and manage the risks of online harm in line with new online safety duties. The ICO and Ofcom will expect online service providers that are in scope of the online safety regime to meet both their online safety and data protection responsibilities. It should be feasible to develop and apply measures to meet online safety obligations, including technological solutions, in ways that conform to data protection law.

We will work together as necessary to take action against services that don't meet their obligations, sharing information and intelligence as appropriate and coordinating approaches to compliance and enforcement. We will set clear expectations for industry as to what organisations have to do to comply with both data protection law and the online safety regime, as applicable.

We will support industry to comply with their online safety and data protection requirements, with a particular emphasis on supporting innovators to thrive and small businesses to grow. Where services require more detailed guidance, for example when implementing particularly novel or risky technologies, we will consider how best to engage with online services of all sizes to allow them to

[24] The guidance documents on which the ICO must be consulted, under the Bill, are the following: guidance on the record keeping and child access assessment duties (clause 49), user identity verification guidance (clause 58), transparency reporting (clause 65), regulated provider pornographic content guidance (clause 69), the risk assessment guidance for industry (clause 85), guidance on CSEA/terrorism notices (clause 108), the guidance on Ofcom's enforcement powers (clause 130) and any guidance on researcher access (clause 137).

[25] Age assurance for the Children's code. https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/

develop products that respect both regimes and deliver benefits for users. We are already committed to supporting innovation in our regulatory approaches.

Ofcom recognises that the online safety regime represents a significant change for many businesses and we are committed to supporting online services through the transition. In particular, Ofcom will focus on supporting smaller services and tackling the risk of any undue burden of compliance. Drawing on the experience of the ICO and other DRCF partners, Ofcom will provide guidance tailored to services' needs and will carry out research and engagement with them to shape the design of its future support tools. Ofcom will explore how digital resources can help streamline the journey towards compliance, while delivering better safety outcomes for users.

The ICO has an existing suite of bespoke guidance services to help innovators comply with their data protection obligations under the UK GDPR. These will be available to services seeking to manage high data protection risk or deploy innovative technologies in meeting their online safety obligations. They include the Innovation Hub, which provides expert data protection advice and supports the development of innovative new products in a privacy-respecting way. The ICO also offers its Regulatory Sandbox, which provides support throughout the design and development of new, innovative products, and which has previously provided support on the development of age assurance in relation to the Children's code.

Conclusion

Alongside our individual support measures, Ofcom and the ICO will together develop a clear plan for how we jointly support small and emerging firms through the regulation they need to comply with. We will seek to:

- align our regulatory approach where it makes sense to do so, and acknowledge where we pursue different statutory duties and remits;
- minimise duplication and streamline regulatory processes where possible;
- provide clear guidance for online service providers that takes account of the requirements of both regimes, particularly where the regimes may be in tension, or where additional input on issues within either Ofcom's or the ICO's remits might be required; and
- share information on supervisory and enforcement action where appropriate, to reduce the regulatory burden on firms.

To achieve this, we will need to:

- build and maintain a common understanding of the areas of overlap and tension between our respective regimes;
- engage with industry to understand the practical challenges of complying with both regimes;
- collaborate closely in developing our policy stances and guidance documents; and
- establish effective processes to maintain mutual awareness of our supervisory and enforcement actions.

Ofcom and the ICO share common principles and overall aims when it comes to protecting people online. We will work together to maximise coherence between our regimes and promote compliance.

This will give organisations the certainty they need to invest. innovate and grow, whilst providing a safe and privacy-respecting online experience for users.