Memorandum of Understanding between the Information Commissioner and Ofcom

Introduction

1. This Memorandum of Understanding (MoU) establishes a framework for cooperation and information disclosure between the Information Commissioner (**"the Commissioner"**) and the Office of Communications (**"Ofcom"**), collectively referred to as **"the participants"** throughout this document. In particular, it sets out the broad principles of collaboration and the legal framework governing the disclosure of relevant information and intelligence between the participants. The shared aims of this MoU are to enable closer working between the participants, including the exchange of appropriate information, so as to assist them in discharging their regulatory functions.

2. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the Commissioner or Ofcom. The participants have determined that they do not exchange sufficient quantities of personal data to warrant entering into a separate data sharing agreement, but this will be kept under review.

The role and function of the Information Commissioner

3. The Commissioner is a corporation sole appointed under the Data Protection Act 2018 (DPA) to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

4. The Commissioner is empowered to take a range of regulatory action, including for breaches of the following legislation:

- Data Protection Act 2018 ("DPA");
- UK General Data Protection Regulation (UK GDPR);
- Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR");

- Freedom of Information Act 2000 ("FOIA");

- Environmental Information Regulations 2004 ("EIR");

- Environmental Protection Public Sector Information Regulations 2009 ("INSPIRE Regulations");

- Investigatory Powers Act 2016;

- Re-use of Public Sector Information Regulations 2015;

- Enterprise Act 2002 ("EA");

- Network and Information Systems Regulations ("NIS Regulations"); and

- Electronic Identification, Authentication and Trust Services Regulation ("eIDAS").

5. Article 57 of the UK GDPR and Section 115(2)(a) of the DPA place a broad range of statutory duties on the Commissioner, including monitoring and enforcement of the UK GDPR, promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes outlined in paragraph 4 above.

6. The Commissioner's regulatory and enforcement powers include:

    - conducting assessments of compliance with the DPA, UK GDPR, PECR, eIDAS, the NIS Directive, FOIA and EIR;

    - issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;

    - issuing enforcement notices, warnings, reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of data protection legislation and other information rights obligations;

    - administering fines by way of penalty notices in the circumstances set out in section 155 of the DPA;

    - administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the Commissioner);

    - issuing decision notices detailing the outcome of an investigation under FOIA or EIR;

- certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA or EIR; and

- prosecuting criminal offences before the Courts.

7. Regulation 31 of PECR, as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, also provides the Commissioner with the power to issue enforcement and monetary penalty notices where organisations breach PECR.

Functions and powers of Ofcom

8. Ofcom is the independent national regulatory authority for the UK's communications industries, with responsibilities across broadcasting (television and radio), telecommunications, video-on-demand, online services, spectrum and postal services. Ofcom is also a national competition authority with concurrent powers with the Competition and Markets Authority (CMA) to enforce competition law and consumer protection laws in relation to communications matters.

9. Ofcom's principal duties, set out in the Communications Act 2003 (CA), are to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition.[1]

10. Ofcom has functions and powers that enable a range of regulatory action, including:

    - promoting media literacy under section 11 CA;

    - setting and enforcing conditions under sections 45-52 of the CA;

    - regulating online safety duties of user-to-user services, search services and regulated pornographic providers under the Online Safety Act 2023 (OSA);

    - conducting market studies in relation to communications matters under the EA and CA;

    - applying ex post competition law in relation to communications matters under the EA and the CA;

    - enforcing certain consumer regulation under Part 8 of the EA;

[1] In carrying out these functions, among other things, Ofcom has the objective to secure the adequate protection of citizens from harm presented by content on regulated online services through the appropriate use of systems and processes designed to reduce the risk of such harm by regulated providers.

- enforcing requirements relating to net neutrality under Articles 3, 4 and 5 of the Open Internet Access Regulation 2015 and the Open Internet Access (EU Regulation) Regulations 2016;

- enforcing requirements for premium rate telephone services under the Regulation of Premium Rate Services Order 2024 and the CA; and

- taking action against persistent misuse of electronic communications networks and services under ss.128-130 CA. Ofcom can take action under these provisions where it has reasonable grounds for believing that a person has persistently misused an electronic communications network or service in any way that causes, or is likely to cause, unnecessary annoyance, inconvenience or anxiety to another person.

Information sharing

11. The purpose of the MoU is to enable the participants to disclose relevant information which enhances their ability to exercise their respective functions, whilst maintaining each participant's statutory obligations with respect to confidential information under the relevant legal frameworks.

12. This MoU should not be interpreted as imposing a requirement on either participant to disclose information in circumstances where doing so would breach their statutory responsibilities. In particular, each participant will ensure that any disclosure of personal data pursuant to these arrangements fully complies with both the UK GDPR and the DPA. The MoU sets out the potential framework for information disclosure, but it is for each participant to determine for themselves that any proposed disclosure is compliant with the law.

Principles of cooperation and disclosure

13. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, the participants will:

    - Exchange information for the shared purpose of facilitating the exercise of each other's functions, including (but not limited to) potential breaches of the legislation regulated by the other participant.

    - Communicate regularly to discuss matters of mutual interest and seek to work together to find appropriate ways to effectively protect consumers. This may involve engagement on the development of potential policy interventions, the implementation of new or

updated policies, application and interpretation of rules and/or guidance as well as participating in multi-agency groups to address common issues and threats; and

- Consult one another on any issues which might have significant implications for the other organisation.

14. The participants will comply with the general laws they are subject to, including, but not limited to, local data protection laws; the maintenance of any prescribed documentation and policies; and comply with any governance requirements in particular relating to security and retention, and process personal data in accordance with the statutory rights of individuals.

Legal bases for disclosing information

15. The statutory functions of each participant govern the legal framework, and legal basis, for disclosing information with the other participant. However, the participants acknowledge that there may also be a range of legislative restrictions on each participant's ability to disclose information under this MoU.

16. This MoU is not intended to provide an exhaustive list of the statutory gateways for disclosing information between the participants, but sets out general principles that may be relevant to how the participants jointly interpret their statutory powers to disclose information with each other in line with their shared goals, the process for disclosing information, and the potential restrictions on their ability to disclose information.

Information disclosed by Ofcom to the Commissioner

17. The Commissioner's statutory function relates to the legislation set out at paragraph 4, and this MoU governs information disclosed by Ofcom to assist the Commissioner to meet those responsibilities. To the extent that any such disclosed information comprises personal data, as defined under the UK GDPR and DPA, Ofcom is a data controller so will ensure that it has a lawful basis to disclose it and that doing so would otherwise be compliant with the data protection principles. It will also ensure that disclosing the information in question is consistent with its legal powers.

18. In addition to Ofcom's general powers to disclose information where it is satisfied that it is not prohibited from disclosing information by virtue of a statutory restriction, a number of statutory gateways also exist for Ofcom to disclose information with the Commissioner, which must be considered on a case-by-case basis, including (but not limited to):

a. Section 131 of the DPA may provide both the lawful basis, from a data protection perspective, and the legal power for Ofcom to disclose information to the Commissioner. Under this provision, Ofcom is not prohibited or restricted from disclosing information to the Commissioner by any other enactment or rule of law provided it is *"information necessary for the discharge of the Commissioner's functions"*.

b. Where Ofcom has obtained information in exercise of competition functions exercisable concurrently with the CMA, the legal power for disclosing such information with the Commissioner may be found in Part 9 of the EA, in particular sections 239 and 241.

c. While section 393 CA and section 56 of the Postal Services Act 2011 primarily prohibit Ofcom from disclosing information obtained in the exercise of its functions, each sets out limited exceptions where disclosure of information is permitted in certain circumstances. For example, Ofcom may disclose such information for the purpose of facilitating the carrying out by the Commissioner of its functions under the DPA and PECR: see section 393(2)(b) and The Communications Act 2003 (Disclosure of Information) Order 2014.

Information disclosed by the Commissioner to Ofcom

19. The Commissioner, during the course of his activities, will receive information from a range of sources, including personal data. He will process all personal data in accordance with the principles of the UK GDPR, the DPA and all other applicable legislation. The Commissioner may identify that information he or she holds, which may include personal data, ought to be disclosed with Ofcom as it would assist them in performing their functions.

20. Section 132(1) of the DPA states that the Commissioner can only disclose confidential information with others if there is lawful authority to do so. In this context, the information will be considered confidential if has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, discharging his functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources. This therefore includes, but is not limited to, personal data.

21. Section 132(2) of the DPA sets out the circumstances in which the Commissioner will have the lawful authority to disclose such information, including with Ofcom. The circumstances include where it is:

- with the consent of the individual or of the person for the time being carrying on the business (section 132(2)(a) DPA;

- necessary for the purpose of the Commissioner discharging the Commissioner's functions (section 132(2)(c) DPA);

- for the purposes of criminal or civil proceedings (section 132(2)(e) DPA); or

- necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 132(2)(f) DPA).

22. In disclosing information in accordance with section 132(2), the Commissioner will make a general assessment whether disclosing the information is necessary for one or more of Ofcom's functions. In particular, where the information proposed for disclosure with Ofcom amounts to personal data, the Commissioner will consider whether it is necessary to provide it in an identifiable form in order for Ofcom to perform its functions, or whether disclosing it in an anonymised form would suffice. Such an assessment by the Commissioner will be informed by discussions with Ofcom on the purposes for which it is being disclosed.

23. If information to be disclosed by the Commissioner was received by him in the course of discharging his functions as a designated enforcer under the EA, any disclosure will be made in accordance with the restrictions set out in Part 9 of the EA.

Other information sharing

24. Where either participant discloses information amounting to sensitive processing for law enforcement purposes under section 35(4) or 35(5) of the DPA, that participant will only do so in accordance with an appropriate policy document as outlined by section 42 of the DPA.

25. Where either participant receives a request for information under data protection legislation, FOIA or EIR, and where the information being sought under that request includes information obtained from, or disclosed by, the other participant, the receiving participant will comply with its obligations under the relevant legislation and any applicable guidance. The decision to disclose or withhold the information (and therefore any liability arising out of that decision) remains with the receiving participant, either as data controller in respect of that data or the public authority that holds the information under FOIA or EIR (depending on the nature of the information being sought).

Method of exchange

26. Appropriate security measures will be agreed to protect information transfers in accordance with the sensitivity of the information and any classification that is applied by the sender.

Confidentiality and data breach reporting

27. Where confidential material is disclosed between the participants it will be marked with the appropriate security classification.

28. Where one participant has received information from the other, it will consult with the other participant before passing the information to a third party or using the information for the purposes of an enforcement or other legal proceeding.

29. Where confidential material obtained from, or disclosed by, the originating participant is wrongfully disclosed by the participant holding the information, that participant will bring this to the attention of the originating participant without delay. This is in addition to obligations to report a personal data breach under the UK GDPR and/or DPA where personal data is contained in the information disclosed.

30. The participants acknowledge that Ofcom is bound by a number of statutory confidentiality requirements that may limit its ability to disclose information with the Commissioner, including section 393 CA and section 116 OSA, that respectively prohibit the disclosure of confidential information received in the exercise of its functions (whether or not marked as sensitive) and the disclosure of information received from or relating to intelligence services. In particular, the participants acknowledge that disclosure in breach of section 393 CA is a criminal offence.

General coordination

31. The participants are committed to working closely together to ensure effective regulatory coordination where regulatory interests overlap. This should support coherent regulation such that each regulator can deliver its respective statutory objectives, maximising synergies and avoiding incoherence or duplication.

32. The participants will take a flexible and efficient approach to implementing and operating the arrangements set out in this MoU, to ensure that coordination is manageable and optimised. The participants will have regular bilateral meetings to support coordination.

Public communications and press releases

33. Public communications on matters involving both parties will, as far as is reasonably practicable, be coordinated between the ICO and Ofcom in advance, to support consistency. Where appropriate and relevant, the ICO and Ofcom will also consult with their respective partner agencies and bodies, such as the Digital Regulation Cooperation Forum (DRCF).
34. Where appropriate, the ICO and Ofcom will seek to amplify and reinforce each other's messages via our respective communications channels.
35. All communications, whether related to a specific issue or more generally, will be mindful of the need to set out the distinct roles of the ICO and Ofcom.

Other forms of support

36. In addition and separate to the arrangements set out above, the participants may provide each other with more informal support to enable them to carry out their respective functions, including but not limited to:

    - answering each other's queries from time to time;
    - providing each other with information or views on a specific policy area or sector;
    - providing each other with training on a specific area of policy;
    - collaborating in the publication of joint statements on a specific policy area; and
    - collaborating in supervision and enforcement matters (insofar as the regulatory frameworks permit) where online safety and data protection overlap and provide areas of common interest.

37. Such support may be requested and provided in connection with the exercise of a specific function or more generally. In this regard, both participants will act reasonably in the circumstances, including by providing sufficient time and information for requests for support to be responded to fully and effectively and for the relevant staff to be engaged.

Status of this MoU

38. The arrangements set out in this document are without prejudice to other statutory requirements for regulatory coordination. This MoU is not intended to have legal effect.

Duration and review of the MoU

39. The participants will monitor the operation of this MoU and will review it biennially.

40. Any minor changes to this memorandum identified between reviews may be agreed in writing between the participants.

41. Any issues arising in relation to this memorandum will be notified to the point of contact for each organisation.

Key contacts

42. The participants have both identified a key person who is responsible for managing this MoU:

William Malcolm **Information Commissioner's Office** Address: Wycliffe House, Water Lane, Wilmslow, SK9 5AF	**Oliver Griffiths** **Ofcom** Address: 2a Southwark Bridge Road, London, SE1 9HA

43. Those individuals will maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose. They will also seek to identify any difficulties in the working relationship, and proactively seek to minimise the same.

Signatories

William Malcolm
Information Commissioner's Office

Date: 06/05/2026

Veronica Branton
Corporation Secretary
Ofcom
Date: 07/05/2026