Memorandum of Understanding between the Information Commissioner and the Investigatory Powers Commissioner

Introduction

1. This Memorandum of Understanding (MoU) establishes a framework for cooperation and information sharing between the Information Commissioner (**"the IC"**) and the Investigatory Powers Commissioner (**"the IPC"**), collectively referred to as **"the Parties"** throughout this document. In particular, it sets out the broad principles of collaboration and the legal framework governing the sharing of relevant information between the parties. The shared aims of this MoU are to enable closer working between the Parties, including the exchange of appropriate information, so as to assist them in discharging their regulatory functions. Any reference to the Information Commissioner shall include his statutory successors.

2. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the IC or the IPC. The parties 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 IC is a corporation sole appointed under the Data Protection Act 2018 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 IC is empowered to take a range of regulatory action 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;
- Security of Network and Information Systems Directive (NIS Directive); and
- Electronic Identification, Authentication and Trust Services Regulation (eIDAS).

5. Article 57 of the UK GDPR and section 115(2)(a) of the DPA 2018 place a broad range of statutory duties on the IC, 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 IC'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 IC with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of PECR including automated telephone calls made without consent, live telephone calls which have not been screened against the Telephone Preference Service, and unsolicited electronic messages (Regulations 19, 21 and 22 of PECR respectively).

Functions and powers of the Investigatory Powers Commissioner

8. The IPC is an independent statutory office holder established by the Investigatory Powers Act 2016 to provide oversight and authorisation of the use of investigatory powers by the intelligence agencies, police forces and other public authorities. The IPC is supported by the Investigatory Powers Commissioner's Office ('IPCO' - an arm's length body) consisting of a team of Judicial Commissioners (JC), authorising officers, inspectors and other staff. The IPC may delegate his functions to the Judicial Commissioners and his staff. The IPC is further supported by the Technology Advisory Panel, whose activities fall outside the scope of this MoU.

9. Further information about the IPC's responsibilities can be found on IPCO's website at: https://www.ipco.org.uk/

Purpose of information sharing

10. The purpose of the MoU is to facilitate the parties to share relevant information and experience which enhances their ability to exercise their respective functions. Since agreeing our previous MOU there have been legislative changes that affect the processing of personal data by IPCO, and in particular notification of serious data breaches

to the ICO, which the parties are intending to reflect as part of this MoU.

11. This MoU should not be interpreted as imposing any requirement on either party to disclose information. In particular, each party must ensure that any disclosure of personal data pursuant to these arrangements fully complies with the UK GDPR, the DPA 2018 and the Investigatory Powers Act 2016. The MoU sets out the potential legal framework for information sharing, but it is for each party to determine for themselves that any proposed disclosure is compliant with the law.

Principles of cooperation and sharing

12. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, each Party will alert the other to any potential breaches of the legislation regulated by the other organisation which is discovered in the exercise of their respective functions, and provide relevant and necessary supporting information.

13. In accordance with section 235A(4) of the Investigatory Powers Act 2016, where a personal data breach has been reported to the IPC under subsection (2), this must be disclosed to the IC. The IC will then assess whether the breach is serious, and if so, notify the IPC.

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

- maintain a working liaison through a nominated point of contact to discuss regularly matters of mutual interest (this may involve participating in multi-agency groups to address common issues and threats)- see Annex A for points of contact;
- Consult one another on any issues which might have significant implications for the other organisation, including sharing draft policy positions where appropriate; and
- Conduct joint audits/inspections where appropriate, providing expertise in relation to relevant areas of responsibility.

15. The Parties will comply with Government security policy relating to the processing of data unless this is incompatible with the discharge of their statutory functions.

Lawful basis for sharing information

Information shared by the IPC with the IC

16. The IC's statutory functions relate to the matters referred to at paragraph 4, and this MoU governs information shared by the IPC to assist the IC to meet those responsibilities. To the extent that information which the IPC proposes to share comprises personal data (as defined under the UK GDPR and DPA 2018), the IPC is a Data Controller and so must ensure that it has a lawful basis to share it and that doing so would otherwise be compliant with the data protection principles.

17. Section 232(2) of the Investigatory Powers Act 2016 provides that the IPC or a JC may provide advice or information to a public authority in relation to matters for which the IPC/JC is responsible. Additionally, the IC's information gateway in section 131 of the Data Protection Act 2018 means that the IPC is able (but not required) to share information with the IC which is necessary for the IC to discharge his functions, without breaching any enactment or rule of law which would otherwise prohibit or restrict that disclosure.

Information shared by the IC with the IPC

18. The IC, 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 2018 and all other applicable legislation. The IC may identify that information he holds, which may include personal data, ought to be shared with the IPC as it would assist them in performing their functions and responsibilities.

19. Section 132(1) of the DPA 2018 states that the IC can only share confidential information with others if there is lawful authority to do so. In this context, the information will be considered confidential if it has been obtained, or provided to, the IC in the course of, or 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. Section 132(2) of the DPA 2018 sets out the circumstances in which the IC will have the lawful authority to share that information with the IPC. In particular, it will be lawful in circumstances where:

- The sharing was necessary for the purpose of the IC discharging his functions (section 132(2)(c));
- The sharing was made for the purposes of criminal or civil proceedings, however arising (section 132(2)(e)); or
- The sharing was necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 132(2)(f)).

20. The IC will therefore be permitted to share information with the IPC in circumstances where he has determined that it is reasonably necessary to do so in furtherance of one of those grounds outlined at paragraph 19. In doing so, the IC will identify the function of the IPC with which that information may assist, and assess whether that function could reasonably be achieved without access to the particular information in question. In particular, where the information proposed for sharing with the IPC amounts to personal data the IC will consider whether it is necessary to provide it in an identifiable form in order for the IPC to perform its functions, or whether disclosing it in an anonymised form would suffice.

21. If information to be disclosed by the IC was received by him in the course of discharging his functions as a designated enforcer under the Enterprise Act 2002, any disclosure shall be made in accordance with the restrictions set out in Part 9 of that Act.

22. Where information is to be disclosed by either party for law enforcement purposes under section 35(4) or (5) of the DPA 2018 then they will only do so in accordance with an appropriate policy document as outlined by section 42 of the DPA 2018.

23. The IPC is not subject to the Freedom of Information Act 2000 (FOIA) and is listed as a body dealing with security matters under s.23 FOIA. Any information that relates to, or is supplied by, IPCO and is held by the IC is exempt from disclosure under FOIA. Where a request for the disclosure of information is received and unless it would be inconsistent with legal obligations (other than under FOIA), the recipient of the request will seek the views of the other Party, where the information being sought under the request includes information obtained from, or shared by, the other Party. However, the decision to disclose or withhold the information (and therefore any liability arising out of that decision) remains with the party in receipt of the request as Data Controller in respect of that data.

Method of exchange

24. Appropriate security measures shall 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

25. Where confidential material is shared between the Parties it will be marked with the appropriate security classification and, where appropriate, handling conditions.

26. Unless it would be inconsistent with its legal obligations, where one Party has received information from the other, it will use it best endeavours to consult with the other Party before passing the information to a third party or using the information in an enforcement proceeding or court case.

27. In the unlikely event that confidential material obtained from, or shared by, the originating Party is wrongfully disclosed by the receiving Party, this Party will bring this to the attention of the originating Party without delay. This is in addition to obligations to report a personal data breach under the UK GDPR and/or DPA 2018 where personal data is contained in the information disclosed.

Duration and review of the MoU

28. The Parties will monitor the operation of this MoU and will review it every two years.

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

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

Signatories

Deputy Commissioner	**Chief Executive Investigatory Powers Commissioner's Office**
 Date: 11/09/25	 Date: 1 August 2025

Annex A

Key contacts

1. The parties have both identified a single point of contact for this MoU:

2.

Information Commissioner's Office	**Investigatory Powers Commissioner's Office**
[redacted] – Group Manager Public Affairs Sectors Email: [redacted]@ico.org.uk Telephone: [redacted] Address: Wycliffe House, Water Lane, Wilmslow, SK9 5AF	[redacted] – Head of Policy Email: [redacted]@ipco.org.uk Telephone: [redacted] Address: PO Box 29105, London, SW1V 1ZU

3. The nominated points of contact for each party 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 ways to continuously strengthen the Parties' working relationship.

This MoU updates the version published in 2021.

Version control (to be removed on publication)

Version	Date	Author	Change Description
0.1	28/10/2019	MN	IPCO has been added as the partner organisation
0.2	22/11/2019	AS	Minor revisions and comments in preparation for sending to IPCO
0.3	09/03/2020	AS	Further additions/comments following IPCO input
0.4			IPCO amends
0.5	24/09/20	AS	Accepted comments from IPCO where agreement ahead of final circulation within ICO.
0.6	29/09/20	AS	Final ICO amends following legal review.
1.0	December 2020		Final version
2.0	May 2025		Updated following amendments to the IPA 2016.