Witness Name: Mr Paul Arnold MBE
Statement No: WITN0453001
Dated: 14 May 2026

THE NOTTINGHAM INQUIRY

FIRST WITNESS STATEMENT OF MR PAUL ARNOLD MBE

I, Paul Arnold MBE, will say as follows:-

INTRODUCTION

1. I am the interim chief executive[1] and Deputy Commissioner of the Information Commissioner's Office (ICO). I was appointed to the role of interim chief executive in June 2025, and have been a Deputy Commissioner since March 2017.

2. I am based at the ICO's head office: Wycliffe House, Water Lane, Wilmslow, Cheshire, United Kingdom SK9 5AF.

3. I am responsible for the executive leadership and management of the organisation, including ensuring that the ICO discharges its functions efficiently, effectively and in accordance with its statutory duties. In my capacity as a Deputy Commissioner, I exercise authority delegated by the

[1] Data Protection Act 2018, Schedule 12A, Para 25

Information Commissioner. See para 9 below for the details on the statutory mechanisms for delegated authority

4. This witness statement is made to assist the Nottingham Inquiry with the matters set out in the Rule 9 Request dated 20 April 2026. For the purposes of this statement, where I reference the ICO, this will include reference to the Information Commissioner and the Information Commissioner's Office.

Key Message

5. I welcome the opportunity to provide evidence to the Inquiry. I recognise the significance of its work, which arises from a deeply tragic set of events, and I hope that this statement assists the Inquiry in its careful consideration of the issues before it. The ICO stands ready to support the need to identify lessons clearly, particularly where they relate to the protection of the public and ensuring responsible and effective data sharing by those tasked with safeguarding individuals.

6. The ICO has, over many years, placed considerable emphasis on enabling responsible data sharing across sectors, particularly in contexts involving safeguarding, public protection and multi agency working. The ICO has consistently sought to ensure that those on the front line understand both how and when they can share personal data lawfully, and have the confidence to do so where appropriate. In some circumstances organisation may be under legal obligations to share data and where this is the case data protection law does not act as a barrier to sharing. The ICO has addressed these points through the development and publication of statutory codes of practice, the provision of practical guidance, ongoing engagement with relevant stakeholders, and direct regulatory support to organisations. This work has been underpinned by a clear and consistent message that data protection law provides a framework to support safe and proportionate data sharing, rather than acting as a barrier to it.

7. In line with that position, I do not consider that there are inherent legal barriers within the data protection framework that prevent appropriate data sharing in the public interest. However, as reflected in the ICO's established position, the existence of a legal framework alone is not sufficient to ensure effective practice. There must be continuous effort and vigilance across government, the regulator, and the sectors responsible for sharing data in practice.

8. Achieving the right outcomes depends on maintaining an appropriate organisational culture, ensuring that staff are properly trained and supported, and putting in place effective systems, governance and accountability mechanisms.

9. Addressing the non-legal barriers - whether cultural, technical or operational - requires a sustained and coordinated approach to ensure that the framework operates as intended in protecting the public.

BACKGROUND

The Information Commissioner and the Information Commissioner's Office

10. The role of the Information Commissioner is that of a corporation sole[2] and is currently occupied by John Edwards, who was appointed in January 2022. The Information Commissioner's Office is a non-governmental public body which is made up of officers and staff appointed by the Commissioner.[3] All formal powers and duties rest with the Commissioner which he can, and has, delegated as appropriate.[4]

[2] Data Protection Act 2018, Schedule 12, para 1(1)
[3] Data Protection Act 2018, Schedule 12, para 5
[4] Data Protection Act 2018, Schedule 12, para 6(2), and ICO website "ICO Scheme of Delegations"

11. The ICO is the regulator for data protection,[5] e-privacy,[6] freedom of information[7] and a number of other digital regulatory areas.[8]

12. Whilst the ICO is an independent regulator, it is accountable to the UK Parliament and the public for the outcomes it achieves. The Department for Science, Innovation and Technology is the ICO's sponsoring department within the UK Government.

The Data Protection Regime in the UK

13. The Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK GDPR) form the key data protection legislation within the UK.

14. The UK GDPR is derived from European Union (EU) law, having been retained[9] and amended[10] in UK law during the process of the UK leaving the EU. The DPA also builds upon the obligations under the UK GDPR,[11] which provides the Information Commissioner with specific information gathering and enforcement powers to carry out his role, and sets out the process under which the Commissioner is appointed as the UK data protection regulator.[12] The DPA also sets out distinct regulatory regimes for law enforcement[13] processing and intelligence services processing.[14]

---

[5] Data Protection Act 2018 and The United Kingdom General Data Protection Regulation (UK GDPR)
[6] The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)
[7] The Freedom of Information Act 2000 (FOI)
[8] The ICO has additional duties and powers in respect of the following: The Environmental Information Regulations 2004, INSPIRE Regulations 2009, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS), the Re-use of Public Sector Information Regulations 2015, The Network and Information Systems Regulations 2018, and the Investigatory Powers Act 2016
[9] The European Union (Withdrawal) Act 2018, s2
[10] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
[11] The Data Protection Act Part 2
[12] The Data Protection Act Part 5, s114 and Schedule 12
[13] The Data Protection Act 2018, Part 3
[14] The Data Protection Act 2018, Part 4

15. The UK GDPR applies to all organisations (with limited exclusions outlined below), including public authorities, private companies, charities and voluntary bodies, insofar as they process personal data in the course of their activities. The UK GDPR does not apply to processing carried out for purely personal or household activities, nor to processing within scope of Parts 3 or 4 of the DPA (law enforcement and intelligence services) detailed below.

16. The UK GDPR is underpinned by a number of key data protection principles set out in Article 5. These include that personal data must be processed lawfully, fairly and in a transparent manner; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and, where necessary, kept up to date; retained only for as long as necessary; and processed in a manner that ensures appropriate security. Controllers are also required to demonstrate accountability for compliance with these principles.

17. In order for processing to be lawful, organisations must identify an appropriate lawful basis under Article 6 UK GDPR. Where more sensitive categories of personal data are processed, including data relating to health or criminal convictions, additional conditions must be satisfied under Articles 9 and 10 UK GDPR and the DPA.

18. The UK GDPR and DPA has been subject to legislative change under the Data (Use and Access) Act 2025. One of the changes which has been brought in is to introduce a new lawful basis for the processing of personal data. This basis is called recognised legitimate interests (RLI). This is a distinct basis from the existing legitimate interest basis and is intended to apply in a limited number of prescribed circumstances where processing is deemed to be in the public interest.

19. RLI may be relied upon where the processing falls within one of a defined set of "recognised" purposes, including crime prevention, safeguarding, emergencies, national security and certain disclosures to support public

functions. Organisations are not required to carry out a balancing test between their interests and those of the data subject, as the law deems such processing to be in the public interest; however, they must still demonstrate that the processing is necessary and complies with the wider requirements of the UK GDPR. It is likely in the context of data sharing for safeguarding purposes, that public bodies would be able to rely on this new lawful basis. Reliance on RLI is likely to reduce time and friction in processing personal data which is in the public interest, however, prior to the legislative reforms, legitimate interests would still have been available as a lawful basis for processing safeguarding information, including sharing such information with other bodies as necessary.

20. Processing by competent authorities for criminal law enforcement purposes is subject to Part 3 of the DPA and is therefore not governed by the UK GDPR[15].

21. Processing by the intelligence services and qualifying competent authorities are subject to Part 4 of the DPA and is therefore not governed by the UK GDPR[16].

22. Part 3 DPA is underpinned by core data protection principles which broadly mirror those under the UK GDPR, requiring that personal data be processed lawfully and fairly; collected for specified and legitimate law enforcement purposes; adequate, relevant and not excessive; accurate and kept up to date where necessary; retained for no longer than necessary; and processed securely.

23. Competent authorities are also subject to obligations of accountability, including maintaining appropriate records and being able to demonstrate compliance with these requirements.

---

[15] For further information – see ICO website – guidance "Guide to Law Enforcement Processing"
[16] For further information – see ICO website – guidance "Guide to Law Enforcement Processing"

24. Part 3 DPA seeks to balance the effective discharge of law enforcement functions with the protection of individuals' rights, ensuring that personal data is handled in a manner which maintains public confidence while enabling policing and public protection activities to be carried out effectively.

SUBSTANTIVE EVIDENCE

ICO guidance and engagement on data sharing - overview

25. The ICO has issued guidance and statutory codes to support organisations in complying with their obligations under UK GDPR and the DPA, including assisting organisations to share data safely and in line with the law.

26. This includes, in particular, the ICO's Guide to the UK GDPR[17], the Data Sharing Code of Practice [WITN0453002] issued under section 121 of the DPA 2018, and sector specific guidance addressing the handling of personal data in complex operational environments[18]. These materials are intended to provide practical assistance on the application of the data protection framework.

27. In addition to guidance and the Data Sharing Code of Practice, the ICO undertakes work to engage with stakeholders including sector representative bodies, and organisations directly.

28. The Information Commissioner, members of the Executive team and a wide range of staff across the ICO have carried out engagements promoting our data sharing resources. Examples of this engagement is as follows:

- On 7 May 2026, the ICO spoke at the Vulnerability Registration Service dispelling myths about blockers to data sharing to support vulnerable people.

[17] See ICO website – UK GDPR guidance and resource – this provides a suite of guidance and resources for organisations relating to the processing of personal data.
[18] See ICO website, "Data Sharing" - a suite of guidance has been written to assist organisations with data sharing

- In 2023, an ICO ET member spoke at the Disclosure and Barring Service annual conference. The key message was that data protection was not a barrier to sharing data and that the ICO has practical information to help you share data.
- In March 2025 ICO staff presented at a Religious Life Safeguarding Service conference again setting out that data protection is not a barrier to sharing information.
- November 2022, ICO colleagues spoke at the Department for Education's (DfE) Data Protection Conference.
- February 2021, ICO staff spoke at an LGA webinar about the need to share data, the code of practice and other data sharing materials.

29. ICO guidance and supporting engagement carries a simple message that data protection law provides a framework for data sharing, and is not a barrier. This is a message that the ICO has consistently communicated, from appearances at select committees(discussed in more detail at paras 81-84), to stakeholder engagement and other media. The ICO also carries out engagement with relevant sectors about good practice and tackling some of the misconceptions around data sharing.

30. Data sharing plays a prominent part in the ICO's annual Data Protection Practitioners Conference that had over 6881 attendees in 2025. The online conference includes workshops and seminars that focus on making data sharing accessible for those working on the frontline in organisations.

31. The ICO has actively sought media coverage for our advice on data sharing, for example both the Independent[19] and The Times[20] have written articles about this subject.

[19] See the Independent website "Information Commissioner urges people to share data to protect at-risk children" dated 14 September 2023
[20] See The Times Higher Education website "There is no legal conflict between protecting data and students' lives" dated 11 January 2024

Data sharing guidance and resources – more detail

32. The Data Sharing Code of Practice is the spine of our data sharing resource page (data sharing hub)[21]. ICO codes of practice do not create new legal duties, but provide statutory guidance on how to comply with the UK GDPR and DPA. The ICO must take relevant codes into account when exercising its enforcement powers, so organisations failing to consider or departing from guidance provided in a code can weigh against an organisation. Courts must also take codes into account where relevant, meaning they carry evidential weight in litigation even though breach of a code is not itself unlawful.

33. The data sharing hub provides a range of resources to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way. Resources include a range of guidance along with checklists, case studies, videos, information on data sharing agreements, a template data sharing request form, a toolkit for sharing data with law enforcement authorities and a data sharing myths buster [WITN0453003].

34. The ICO's data sharing myth buster was created to dispel common "myths" which the ICO had seen around data sharing. The guidance [WITN0453003] starts by stating:

> "*Many organisations have been sharing data successfully, but there seems to be a belief by some in the public and private sectors that data protection law is a barrier to doing this. This belief is unfounded.*"

35. The myth busting guidance then sets out a common myth followed by a factual explanation to assist the user to undertake the data sharing within the regulatory framework [WITN0453003]. The myths include "*Personal data can't be shared in emergency situations*", "*Data protection law prevents organisations from sharing sensitive personal data with the police or other law*

[21] See ICO website – For organisations – UK GDPR guidance and resources – Data sharing – for full list of guidance and resources

enforcement authorities" and "*Consent is always needed to share people's data with another organisation*".

36. The ICO website also has advice, and a sample template [WITN0453010], for creating a data protection impact assessment (DPIA) to help organisations decide whether it is appropriate to share data, and whether it would be compliant with the law. Most of our products and toolkits include advice relevant to all organisations, from the code itself to guidance on privacy enhancing technologies (PETs).

37. The ICO has also produced specific advice, including on sharing data to safeguard children. The data sharing hub also includes advice about sharing data in an emergency with two pieces of guidance aimed at sharing data in an emergency at university or college or at work.

38. The ICO's 10 step guide to sharing information to safeguard children [WITN0453011] is intended to be accessible to a wide range of people who work with children and young people. The emphasis is on what organisations need to put in place to ensure staff know how to safely share data share, i.e. training, systems and entering into data sharing agreements. The introduction of the guide states that:

> '*Data protection law allows you to share information when required to identify children at risk of harm and to safeguard them from harm' and 'It will never breach UK data protection law to share all the information you need to with an appropriate person or authority in order to safeguard a child.*'

39. The Commissioner recorded a short video[22] that clearly states that people should not fear regulatory action from the ICO where they share data in good faith; this video has had 3,300 views.

[22] UK Information Commissioner: data sharing to safeguard children | Videos & Movies on Vimeo – recorded video – link included

40. Following the HM Coroner for City of London's Prevention of Future Deaths Report, the ICO worked with bereaved parents to produce guidance [WITN0453012] aimed at universities and colleges relating to sharing of data where there is a safeguarding concern around a young person. The guidance states:

> '*...we are aware that, sometimes, universities and colleges are hesitant to share students' personal data in an urgent or emergency situation, citing data protection as the problem. That should not be the case*'.

Information Sharing Between Public Authorities and Law Enforcement Agencies

41. The data protection regime does not prohibit the sharing of personal data between public authorities, including with police forces or vice versa. Rather, it provides a structured framework within which such sharing must take place.

42. The ICO has consistently emphasised that data protection law is an enabling regime which permits data sharing where it is necessary and proportionate. This message is found across our suite of guidance to organisations and law enforcement agencies. For example, in the ICO's Sharing personal data with law enforcement authorities guidance [WITN0453004], the first paragraph of the guidance states:

> "*The UK GDPR does not prevent you sharing personal data with law enforcement authorities who are discharging their statutory law enforcement functions. The UK GDPR and the DPA 2018 allow for this type of data sharing where it is necessary and proportionate.*"

43. The ICO's statutory Data Sharing Code of Practice also reiterates this message in respect of law enforcement agencies sharing personal data with other organisations where necessary. This states:

"...data protection law does not prevent appropriate data sharing when it is necessary to protect the public, to support ongoing policing activities, or in an emergency for example" [WITN0453002, page 69].

Public bodies sharing personal data with law enforcement agencies

44. The ICO's Data Sharing Code of Practice makes clear that public authorities may share personal data where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or where it is necessary for compliance with a legal obligation. In urgent situations, including those involving risks to life or serious harm, the "vital interests" lawful basis may also apply. The Code further emphasises that a failure to share data where appropriate may be as harmful as excessive disclosure [WITN0453002 page 9 and page 88].

Police forces sharing data with public bodies

45. In relation to law enforcement agencies, data sharing is often undertaken pursuant to Part 3 of the DPA. The ICO's Data Sharing Code of Practice makes clear that section 36(4) DPA permits such sharing where the processing is "authorised by law". In those circumstances, the competent authority must identify a clear legal basis for the disclosure (which may include statute, common law, or other recognised legal powers) and ensure that any onward processing complies with the UK GDPR and Part 2 of the DPA 2018, including the identification of an appropriate lawful basis. For policing bodies, this will typically require consideration of whether the sharing aligns with a legitimate policing purpose.

ICO's overall messages on data sharing for safeguarding

46. The ICO's Data Sharing Code of Practice and associated guidance recommend that organisations adopt formal data sharing agreements where regular or large-scale sharing takes place. These agreements are not mandatory in all circumstances but are regarded as good practice and should

set out, amongst other matters, the purpose of the sharing, the lawful basis relied upon, the categories of data involved, retention arrangements, and security measures.

47. Data shared should be limited to what is necessary to achieve the relevant purpose, and organisations should ensure that appropriate technical and organisational measures are in place to prevent unauthorised or excessive disclosure.

48. The ICO's guidance has also been referenced in sector specific guidance and government guidance. For example, the ICO's 10 step guide to sharing information to safeguard children is referenced in the Government's Information sharing: advice for safeguarding practitioners guidance [WITN0453013]. The Government's guidance notes:

> *"Data protection legislation (the Data Protection Act 2018 (the DPA 2018) and UK General Data Protection Regulation (UK GDPR)) does not prevent the sharing of information for the purposes of safeguarding children, when it is necessary, proportionate and justified to do so. In fact, data protection legislation provides a framework which enables information sharing in that context. The first and most important consideration is always whether sharing information is likely to support the safeguarding of a child."*

49. The applicable data protection framework requires organisations to exercise judgement, supported by clear policies and governance, when sharing personal data. The ICO provides guidance, draft documents and engagement to assist in this process.

50. Provided that data sharing is necessary, proportionate, and carried out in accordance with the applicable statutory regime, it is capable of being undertaken lawfully and in a manner that supports effective multi agency working.

Use of the ICO resources and tools

51. The ICO has a programme of evaluation work[23] however, the ICO has not carried out a formal evaluation of our data sharing code and data sharing hub. Evidence from the ICO's web analytics tool suggests there have been approximately 40,000 visits to data sharing guidance products over the period April 2025-March 2026.

52. Most of the ICO's resources are created following extensive engagement and sometimes formal calls for views or consultations with stakeholders. As part of producing the statutory Data Sharing Code of Practice the ICO held both a call for views and then consulted on a draft version. A summary of responses was published on our website [WITN0453005]. Feedback included requesting more case studies and more information on sharing data with law enforcement organisations. Subsequent resources have responded to this feedback.

53. The ICO also receives informal and usually positive feedback from DPOs that have used the resources in the data sharing hub.

54. The ICO's 10 step guide to sharing information to safeguard children was informed by a wide range of engagement. This included the DfE, Children's Commissioner, NSPCC, Coram, Girl Guides and safeguarding leads within schools. Informal feedback when attending or speaking at conferences has also been positive. The ICO has also worked directly with families who have been impacted by issues around data sharing to produce guidance to ensure timely and lawful data sharing to safeguard people [WITN0453012]

55. Whilst not specifically about data sharing resources, the Data Controller Study 2025[24], found that 75 per cent of respondents reported that ICO resources provide clarity about what the law requires.

---

[23] See ICO website under "Evaluation and other impact"
[24] See ICO website "Data Controller Study 2025" – interactive dashboard and supporting reports and evidence.

The role of the Data Protection Officer (DPO)

56. Under Part 3 of the Data Protection Act 2018, police forces are required to appoint DPO. Similarly, under the UK GDPR, an organisation is required to appoint a DPO where it is a public authority or body (other than courts acting in their judicial capacity), or where its core activities involve large-scale monitoring of individuals or large-scale processing of special category or criminal offence data.

57. The DPO forms part of the broader accountability framework and is intended to support the organisation in demonstrating compliance with data protection obligations. The ICO expects DPOs to be involved in setting up data sharing agreements and frameworks, and to ensure that appropriate training is in place allowing lawful sharing to occur.

58. The DPO's core role is to inform and advise the organisation and its personnel on their legal obligations, and to monitor compliance with the data protection regime, including through oversight of internal policies, training, and audit activity. In this way, the role operates as a central mechanism for embedding data protection compliance within operational decision making.

59. The DPO must be independent, appropriately qualified and adequately resourced, and must report to the highest level of management within the organisation. The DPO must be able to perform their functions without conflict of interest or undue influence, and must be involved in a timely manner in all issues relating to the protection of personal data. These requirements are intended to ensure that the DPO is able to provide objective oversight of data processing activities. Further guidance on DPOs can be found on the ICO website.

Regulatory Action taken by the ICO in the last 10 years relating to data sharing between public bodies

60. The ICO's Retention Policy requires information relating to formal regulatory activity to be retained for a period of six years. Some of the detail below has therefore been produced in consultation with internal stakeholders and has been verified from external sources.

61. In 2018, the ICO issued an Enforcement Notice to the Metropolitan Police Service in relation to its 'Gangs Matrix', a database that recorded intelligence related to alleged gang members. The ICO found that, while there was a valid purpose for the database to tackle violent gang crime, it was being used unlawfully as it didn't properly distinguish between victims of crime and offenders and was being shared more widely than was necessary. The information contained within the matrix was shared across London Boroughs and impacted on people's access to housing and jobs. The ICO found that this had the potential to cause distress to a disproportionate number of young black men.[25]

62. A Civil Monetary Penalty was also issued to London Borough of Newham linked to the "Gangs Matrix" but relating to an unredacted disclosure of personal data from the database being disclosed to multi agency stakeholder in 2017.[26] Due to ICO policies on retention of documents, I am unable to provide further details relating to this case.

63. In 2023, the ICO issued a reprimand to Police Service of Northern Ireland (PSNI) after they failed to have appropriate measures in place to prevent unlawful sharing of personal data, including criminal data, with the United States Department of Homeland Security (DHS). The investigation found that this processing fell outside of the well-established and lawful processes that PSNI had in place for sharing personal data with foreign law enforcement partners and lacked adequate oversight and governance.[27]

---

[25] See ICO website – "Metropolitan Police gangs matrix"
[26] See Newham Council's website - "Newham Council response to Penalty Notice from Information Commissioner's Office"
[27] See ICO website – "Police Service of Northern Ireland (PSNI)" under Enforcement Action

64. In 2024, Dover Harbour Board and Kent Police were each issued with a reprimand for the use of social media distribution groups, initially created in WhatsApp but later migrated to Telegram. The distribution groups were used by multiple UK police forces and international law enforcement agencies for the purpose of combatting vehicle crime. The distribution groups were created by an officer from the Port of Dover Police using his personal mobile phone without organisational oversight or compliance with data protection legislation.[28]

Reported data breaches

65. Section 170 of the Data Protection Act 2018 makes it a criminal offence to knowingly or recklessly obtain, disclose, or retain personal data without the consent of the data controller.

66. The ICO's approach to breaches reported in these circumstances, where reasonable and appropriate, is to let data controllers complete their internal disciplinary processes and investigations, and to provide advice and support to them while those processes are underway. Once data controllers have completed their internal investigations, the ICO may receive referrals from data controllers in respect of individuals they have identified, who are alleged to have unlawfully obtained personal data, which the ICO will then review ahead of the potential commencement of criminal investigations.

67. The ICO has received two data breach reports relating to potential unlawful access of the medical records of six patients who were involved in the Nottingham attack. These reports were made to the ICO in early 2025.

68. No formal referrals have been made by the data controller in respect of individuals suspected of a possible offence under the Data Protection Act 2018. However, the ICO is continuing to provide advice and assistance to the

[28] See ICO website – "Dover Harbour Board" under Enforcement Action and "Chief Constable of Kent Police" under Enforcement Action

controller during their internal processes, and the ICO will action any subsequent referrals, as and when they arrive.

69. Whilst the breach reports remain open, it is possible that the patients whose records were accessed were deceased at the time of unauthorised access. As the UK Data Protection regime only applies to the personal data of living individuals, the ICO does not have jurisdiction to investigate breaches of data which relate to deceased individuals.

70. The ICO does not hold any records of any other data breaches being reported in respect of the events connected to the Nottingham Inquiry, save for those outlined above. The ICO's retention period for records of reported data breaches is 2 years. This means any reports made before this date, where the ICO has not taken action, will have been destroyed.

The impact of the regulatory landscape on data sharing between public bodies

71. The current data protection legislation provides a practical framework to support the sharing of data, and should not inhibit the sharing of personal data where it is appropriate to do so.

72. The data sharing regulatory landscape is shaped by the ICO's code of practice. This practical guidance sets out how to share data and it is explicit that it 'demonstrates that the legal framework is an enabler to responsible data sharing and busts some of the myths that currently exist'.

73. The ICO has engaged with a wide range of organisations across different sectors on a regular basis and their feedback helps us prioritise our work. This includes formal consultations, for example when producing the statutory code of practice as set out above. The ICO has also engaged with a wide range of stakeholders to understand sharing of personal data. For example:

- The ICO has ongoing and regular engagement with key policing bodies, including the National Police Chief's Council (NPCC), the Independent Office for Police Conduct (IOPC), the Metropolitan Police Service (MPS), and other forces, at both operational and senior levels. Part of this engagement is to understand the issues facing these bodies in sharing data and providing advice in that regard.

- Police and local government have formed multi-agency groups (police, social services, health, and other support services) to identify causes of violence, including domestic violence and also public violence, with a view to providing support for affected individuals. These violence reduction units (VRU) were experiencing difficulties where some parties were reluctant to share data, for example with police, citing data protection law as the reason. The ICO also worked with Humberside Police VRU, and in autumn 2023 presented to a large group of multi-agency partners, to reassure them that data protection provided the enabling framework for this data sharing, it was not a blocker to it.

74. The ICO has worked with police bodies consistently over the years. In December 2019 the Commissioner of the Metropolitan Police raised concerns with the ICO that data protection legislation was perceived by police forces to be a barrier to data sharing. As a result of this discussion, the ICO wrote to all Chief Constables asking for examples of when data protection was cited as a barrier to sharing data in an investigation [WITN0453006]. After receiving responses to the letter and comprehensive engagement with police forces, the ICO didn't find any substantive reports of data protection legislation being a blocker to sharing, but did find other factors including the use of consent, developing data sharing agreements with public sector partners and cultural issues including a lack of confidence and lack of knowledge. The engagement led to the ICO including additional content in the data sharing code and producing a law enforcement tool kit which is on our data sharing hub.

75. The ICO has also worked with the Chief Medical Officer and National Data Guardian to issue a joint call to action[29] to all health and care staff urging them to share data with confidence. The call to action includes guidance, training materials and a straightforward video, with the Commissioner, that states that data protection isn't a barrier to sharing data.

76. In 2021 the ICO met with members of NHSX's (now NHS Digital) Data Protection Officer network to understand the data sharing challenges experienced by health and care providers. This work led to the development of a number of case studies which were published on the ICO's website[30] addressing the challenges identified in the survey.

77. The ICO also carries out assessments of whether organisations are following good data protection practices in the form of audits[31]. Audits can be carried out with public and private companies, public authorities, and government departments. The majority of audits are carried out consensually, but the ICO has powers to undertake compulsory audits under Assessment Notices.

78. The ICO focuses our audit activity on areas where it feels it can have the biggest impact and on those organisations who would benefit the most from an independent assessment of their data protection practices. The ICO publishes summaries of audits[32] and, where appropriate, overview reports to share trends and themes that have been identified (for example from audits carried out in a particular sector) to help other organisations learn lessons from the ICO's work

79. ICO audits can cover a variety of scope areas, focusing on various aspects of data protection compliance, including data sharing. Examples of recent audit recommendations that have been made in relation to data sharing include:

[29] See joint call to action on NHS England Website – Link included as link contains video
[30] ICO website – see data sharing – "Case studies and examples"
[31] For more detail on audits undertaken by the ICO – see ICO website under advice and services "Audits"
[32] See ICO website "Audits and overview reports"

improving training for staff who make data sharing decisions; creating or improving data sharing agreements with third parties; improving recording and logging decisions and sharing and improving the mapping data flows.

80. In November 2021 the ICO issued its report "*COVID-19 and information rights: reflections and lessons learnt from the Information Commissioner*" [WITN0453007, Page 5]. The Commissioner noted:

> *'We didn't need to change the law to allow for nationwide test and trace systems, or to allow for the data sharing that was necessary to support the vulnerable. These key principles also provided the safeguards the public still expected to be in place – transparency, fairness, necessity, and proportionality – backed by an independent regulator to hold organisations to account.'*

ICO public positions regarding data sharing

81. The Information Commissioner (Both the current Commissioner, John Edwards, and the previous Commissioner, Elizabeth Denham) has provided both written and oral evidence to the House of Lords Public Services Committee, under the Chair of Baroness Armstrong· which was looking at the issues facing public service professionals in sharing and receiving personal data.

82. The Information Commissioner noted in his oral evidence on 25 January 2023 [WITN0453008, Page 1] that "*there is a common phenomenon in jurisdictions with similar legislation, which is that a degree of mythology creeps up around the legislation: that it is there to prevent information sharing.*"

83. The Commissioner went on to state "*My office plays an important role in providing guidance on how to share information safely and reassuring the public that sharing can be done responsibly, but leadership needs to be shown in other domains as well, including across central government, to set*

examples and expectations of public services, both at central and local government level." [WITN0453008, Page 2]

84. The Information Commissioner also gave evidence to the Angiolini Inquiry Part 1, which examined the circumstances that led to the Sarah Everard's murder by a police officer. The Information Commissioner provided a witness statement to the Inquiry addressing some aspects of data sharing [WITN0453009]. The Part 1 report noted the following:

> *"Some cite data privacy and protection laws as a reason not to share information. However, in a discussion with the Information Commissioner, John Edwards, the Inquiry was assured that data protection law recognises that there are legitimate reasons for information-sharing, particularly given the powers attributed to police officers. Indeed, Mr Edwards suggested that data protection law is widely misunderstood and misconstrued, and highlighted a failure of training in this regard."*[33]

85. The ICO has produced and promoted a range of resources to help organisations share data as outlined earlier within this statement. The ICO is clear that data protection law does not create a barrier to data sharing, but our work with organisations has highlighted that there are other reasons which can result in reluctance to share data.

86. Over the years the ICO has noted that the barriers which prevent data sharing are not legislative, but rather a result of misunderstandings within organisations as to how data protection law applies. The ICO has previously shared this view, including with Parliament.

87. The ICO has provided guidance, resources, engagement and audits, and used its enforcement powers in this area, applying its full regulatory tools to assist organisations with lawful data sharing. However, organisations are also

[33] See Angiolini Enquiry Part 1 report – Para 4.320

accountable for their compliance with data protection legislation[34]. Organisations are required to put in place the appropriate technical and organisational measures[35] to ensure they implement the data protection principles effectively and safeguard people's rights. This includes ensuring staff receive training on data protection, which should show where and when personal data can be shared lawfully when necessary.

88. The Commissioner's foreword to the data sharing code states:

> *'This code demonstrates that the legal framework is an enabler to responsible data sharing and busts some of the myths that currently exist. But we cannot pretend that a code of practice is a panacea to solve all the challenges for data sharing. Or that targeted ICO engagement and advice will solve everything. There are other barriers to data sharing, including cultural, technical and organisational factors. Overcoming these will require more than just the ICO; it will require a collective effort from practitioners, government and the regulator.'* [WITN0453002 page 7 and 8]

89. In February 2021 the Information Commissioner wrote to Baroness Armstrong following an appearance at the public services select committee. The letter highlighted the following:

> *"...the task of reducing barriers to data sharing is too big to be undertaken by one body in isolation. It needs a cooperative and coordinated effort from stakeholders across society. We see this as a partnership between government, parliament, the regulator, and those sectors at the frontline of data sharing. The ICO cannot lead the work. This is due to our status as regulator; there is a need for us to strike a balance between our role of giving advice and support to organisations undertaking data sharing, and*

[34] Law enforcement – Part 3 s34(3) DPA, non law enforcement – UK GDPR Art 5(2)
[35] Law enforcement - Part 3 s57 DPA, non law enforcement – UK GDPR Art 25

our need to take appropriate action to protect the data rights of citizens if there is a breach of the law."

90. The message within this letter remains accurate today and I reiterate those points. Frontline organisations should be confident that the legal framework enables them to share data for the purposes of safeguarding individuals. The ICO continues to support responsible data sharing and our guidance seeks to provide clarity to organisations on these issues.

STATEMENT OF TRUTH

I believe the content of this statement to be true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief of its truth.

Signed: GRO-B

Dated: 14 May 2026

Index to First Witness Statement of Paul Arnold MBE

Number	URN	Document Description
1	WITN0453002	The Data Sharing Code of Practice
2	WITN0453003	Data sharing myths busted
3	WITN0453004	Sharing personal data with law enforcement authorities – ICO
4	WITN0453005	Data sharing code call for views summary of responses
5	WITN0453006	ICO Letter to Chief Constables
6	WITN0453007	Covid-19-report
7	WITN0453008	Public service committee evidence
8	WITN0453009	John Edwards Witness Statement
9	WITN0453010	Annex B of the Data Sharing Code: Sample Template
10	WITN0453011	ICO 10 step guide to sharing information to safeguard children
11	WITN0453012	Sharing personal data in an emergency – a guide for universities and colleges
12	WITN0453013	Gov.uk – Information advice for safeguarding practitioners