

## Memorandum of Understanding between the National Cyber Security Centre and the Information Commissioner

---

### Introduction

1. This Memorandum of Understanding (MoU) establishes a framework for cooperation and information sharing between the National Cyber Security Centre (NCSC) and the Information Commissioner (the “Commissioner”), 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 and intelligence between the parties.
2. The shared aims of this MoU are to codify and enhance working between the parties, including the exchange of appropriate information, so as to assist them in discharging their functions. The MoU explains how the NCSC and the Commissioner will work together in the following areas:
  - a. The development of cyber security standards and guidance by each party
  - b. Assessing and influencing improvements in cyber security of regulated organisations
  - c. Information sharing
  - d. The NCSC supporting the Commissioner’s own cyber security
  - e. Deconfliction between the NCSC and the Commissioner in relation to incident management
  - f. Public communications and press releases
3. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the NCSC or the Commissioner.

### The NCSC’s mission

4. The National Cyber Security Centre (NCSC) is part of the Government Communications Headquarters (GCHQ) and its statutory powers and functions are those of GCHQ.
5. GCHQ is a central government department which was put on a statutory footing by the Intelligence Services Act 1994, which also sets out: GCHQ’s functions; the purposes for which those functions may be exercised; and the Director of GCHQ’s statutory responsibilities. A statutory function of GCHQ, set out at section 3(1)(b) of ISA, and relevant to the work of the NCSC is to *“provide advice and assistance about...cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown to Her Majesty’s Government in the United Kingdom or to a Northern Ireland Department or, in such cases as it considers appropriate, to other organisations or persons, or to the general public, in the United Kingdom or elsewhere”*.
6. The NCSC is the UK’s technical authority for tackling cyber threats and works to defend the UK from cyber risks, deter our adversaries and develop our cyber security capability, consistent with delivering the National Cyber Strategy. The NCSC’s activities include providing advice and assistance on cyber security to help address systemic vulnerabilities, and helping organisations increase the cyber resilience of their networks. The NCSC website provides more information about its work. The NCSC cannot single-handedly change cyber security cultures



and practices across the UK and therefore works in partnership with many others to achieve improvements.

## The Information Commissioner

7. The Commissioner is a corporation sole appointed by Her Majesty the Queen 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.
8. The Commissioner is empowered to take a range of regulatory action including for breaches of the following legislation:
  - Data Protection Act 2018 (DPA 2018);
  - 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;
  - Network and Information Systems Regulations 2018 (the NIS Regulations); and
  - Electronic Identification, Authentication and Trust Services Regulation (eIDAS).
9. Article 57 of the UK GDPR and Section 115(2)(a) of the DPA 2018 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 8 above.
10. The Commissioner's regulatory and enforcement powers include:
  - conducting assessments of compliance with the DPA 2018, UK GDPR, PECR, eIDAS, NIS Regulations, 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 2018;
  - 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.
11. 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 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).

### **The development of cyber security standards and guidance by each party**

12. The NCSC provides standards and guidance relevant to cyber security in a wide range of sectors, with a particular focus on the cyber security of organisations that carry out the most critical functions for the UK including those relevant to maintaining national security such as Government and critical national infrastructure. Some of this material is general in nature, for example around good practices in passwords, whilst others will be specific technical advice tailored to a sector or activities within a sector. An important component of the NCSC's standards and guidance is the Cyber Assessment Framework (CAF), which is available to cyber security regulators to use should they so wish. The NCSC engages with the users of the CAF and the wider regulatory community, including the Commissioner, throughout the course of its development of the CAF, and other relevant cyber security standards and guidance.
13. Should the Commissioner wish to use the CAF, NCSC will provide advice on how the CAF is intended to be used and technical support about its application. The Commissioner will provide feedback on its experience of using the CAF to inform its future development. Where appropriate and reasonably practicable, the NCSC will consult with the Commissioner about possible changes to the CAF; provide advance notice of new versions of the CAF to the Commissioner; and discuss in advance public NCSC communications on CAF changes.
14. Where the Commissioner develops or uses a framework for cyber security assessment that is based on the CAF but which diverges from it in a material way (for example, in ways other than presentational changes), the NCSC may not provide technical support. The Commissioner and the NCSC will discuss and seek to understand any reasons for divergence by the Commissioner from the Cyber Assessment Framework with a view to resolving any differences in approach, including as part of feedback provided by the Commissioner.
15. The NCSC seeks to influence the development of international standards and guidance on cyber security in a manner that supports its work with regulators in the UK. Similarly, the Commissioner contributes to international standards and guidance through working with a range of regulatory partners across jurisdictions with the purpose of further international co-operation, including in relation to cyber security. The Commissioner and the NCSC agree to inform each other about international developments and opportunities that would support their respective abilities to achieve these outcomes.



## **Assessing and influencing improvements in cyber security of regulated organisations**

16. The Commissioner considers that a key part of its work is understanding what cyber security standards have been achieved in the organisations within its remit, what changes are most urgently needed, and how these changes can be implemented.
17. Through its guidance, the Commissioner will encourage good practice and continuous improvement in cyber security amongst the organisations it regulates. For example, the Commissioner's guidance will continue to promote the application of the NCSC's technical standards and guidance, alongside other relevant good practice, and the use of NCSC-accredited training courses and assurance providers, where appropriate, to mitigate cyber risks within the organisations it regulates. The Commissioner will continue to take into account how proactive an organisation is on cyber security matters and will recognise and encourage appropriate engagement with the NCSC on cyber security matters, including the response to cyber incidents.
18. To support the Commissioner's regulatory work, the NCSC may provide cyber security advice and assistance to the Commissioner where appropriate and in accordance with the statutory functions of NCSC. The scope of the NCSC's advice and assistance to the Commissioner will be technical in nature and focuses on cyber security risk management. The NCSC's advice will be given for the purpose of supporting the Commissioner to make decisions in the context of the Commissioner's statutory functions. Such decisions taken by the Commissioner are the Commissioner's responsibility.
19. The National Cyber Strategy recognises the importance of working in partnership to successfully secure the UK in cyberspace. Consistent with this, the NCSC seeks to promote positive cyber security cultures, and to foster learning from experience and peers. The Commissioner has regard to the value the National Cyber Strategy places on partnership and collaboration when exercising the statutory functions in relation to cyber security.
20. The NCSC will invite the Commissioner to participate in the Cyber Security Regulators Forum hosted by the NCSC, as well as other relevant initiatives. The Commissioner will, subject to resource constraints, support the NCSC in such initiatives and will, where appropriate, encourage organisations to engage with the NCSC in relevant forums and working groups.

## **Information Sharing**

21. For the avoidance of doubt, the NCSC will not share information from an organisation it is engaged with due to a cyber incident with the Commissioner unless it has the consent of the organisation to do so. Disclosure of such information to the Commissioner, without consent, may be a breach of the duty of the Director of GCHQ set out in section 4(2) of the Intelligence Services Act 1994, which requires that no information is disclosed by GCHQ except so far as it is necessary for the proper discharge of GCHQ's statutory functions or for the purpose of any criminal proceedings.
22. The NCSC and the Commissioner will share information to the extent permitted by law, and as appropriate and relevant to their respective missions, statutory functions and objectives. The detail of data sharing will be provided for outside this MoU and may include, but is not limited to:

- a. The NCSC sharing relevant cyber threat information with the Commissioner, including cyber threat assessments that are likely to affect Relevant Digital Service Providers (as defined under the NIS Regulations) and other organisations regulated by the Commissioner.
  - b. The Commissioner sharing information about cyber security incidents with the NCSC (both on an anonymised, systemic and aggregated basis, and on an organisation specific basis where appropriate) to assist the NCSC's role in helping to reduce harm from cyber security incidents in the UK, and the NCSC's roles under the NIS Regulations as the UK's computer security incident response team (CSIRT), Single Point of Contact and National Technical Authority.
  - c. The Commissioner sharing information with the NCSC gathered pursuant to the Commissioner's role as a Competent Authority under the NIS Regulations to assist with the NCSC's understanding of risks in the UK's network and information systems, including (but not necessarily limited to) CAF returns, or other similar cyber security assessments the Commissioner undertakes with regulated organisations under the NIS Regulation should it not use the CAF.
23. As the NCSC is part of GCHQ, information that is directly or indirectly supplied to the Commissioner by, or that relates to the NCSC is exempt from Freedom of Information requests received by the Commissioner by virtue of Section 23 of the Freedom of Information Act 2000, and may be subject to exemption from disclosure under other information legislation. Any Freedom of Information requests made to the Commissioner for information the NCSC has supplied to the Commissioner should be referred to the NCSC.

#### ***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.
25. For example, where information being shared by the NCSC is classified as secret or above or is particularly sensitive, or is otherwise marked for limited distribution (e.g. by use of the traffic light protocol or otherwise), the NCSC and the Commissioner will agree safeguards are put in place and maintained. This may include limiting distribution within the Information Commissioner's Office to named individuals or those with appropriate security clearance, if required.

#### **The NCSC supporting the Commissioner's own cyber security**

26. The NCSC will support the Commissioner's own cyber security through the provision of technical tools and guidance. In some cases, the NCSC may be able to provide consultancy advice to the Commissioner, for example where significant changes are planned that may have implications for cyber security. The Commissioner can expect to receive NCSC support in the event it experiences a serious cyber security incident.

## **Deconfliction between the NCSC and the Commissioner in relation to incident management**

27. Where organisations report an incident to the NCSC and the NCSC identifies that the case may be legally reportable to Commissioner, the NCSC will remind organisations to be mindful of their regulatory obligations, but will not opine on whether an organisation may be under an obligation to notify nor make notifications to the Commissioner on the organisation's behalf.
28. Where organisations have notified the Commissioner of a cyber incident and it is identified through engagement with the affected organisation that the case may be a nationally significant cyber incident which is relevant to the work of the NCSC, the Commissioner will recommend and encourage the organisation to notify the NCSC.
29. Where an incident is reported to the Commissioner pursuant to the NIS Regulations, the Commissioner will make the report to the NCSC as Computer Security Incident Response Team (CSIRT) in fulfilment of its obligations under the NIS Regulations.
30. When both parties are engaged in managing a cyber security incident, the parties will seek to co-ordinate their work to the extent reasonably practicable and appropriate to minimise any disruption of the affected organisation's efforts to contain and mitigate any harm.
31. The Commissioner's incident response phase will seek to make sure organisations are able to prioritise engagement with the NCSC and/or its cyber incident response providers in the immediate aftermath of an incident to prioritise the mitigation of harm, identify the root cause of the incident, and take appropriate steps to prevent the incident reoccurring.
32. The NCSC and the Commissioner recognise that the priority for an organisation suffering an incident should be the incident's remediation and the mitigation of harm to the organisation, its customers, and the UK and its citizens more generally. Both parties will seek to ensure that their interventions align with this priority and will provide each other with feedback where they view the other's approach to intervention may have worked against it.
33. The Commissioner acknowledges that where cross government coordination in response to an incident is required, the NCSC will lead co-ordination in its role as national technical authority (alongside other government departments where appropriate). Should the Commissioner intend to issue public communications concerning an incident, it will share with the NCSC (and other relevant law enforcement and sector regulators) such communications in advance.
34. In respect of a NIS incident that affects a relevant digital service provider (as defined in the NIS Regulations), the NCSC and the Commissioner will consult each other before issuing public communications about an incident.

## **Public communications and press releases**



35. Public communications on matters involving both parties will, as far as is reasonably practicable, be agreed between the Commissioner and the NCSC in advance, to support consistency. Where appropriate and relevant, the NCSC and the Commissioner will also consult with their respective partner agencies and bodies.
36. Where appropriate, the Commissioner and NCSC will seek to amplify each other's messages and an awareness of their differing interests; promote learning, consistent guidance and standards as well as key messages on information and cyber security.



- 37. The Commissioner will on an increasing basis, continue to recognise and incentivise appropriate engagement with the NCSC on cyber security matters in its approach to regulation. Specifically, the Commissioner will publicise (on its website, in guidance, and in relevant press releases) that it looks favourably on victims of nationally significant cyber incidents who report to and engage with the NCSC and will consider whether it can be more specific on how such engagement might factor into its calculation of regulatory fines.
- 38. All communications whether related to a specific incident or more generally will be mindful of the need to set out the distinct roles of the Commissioner and the NCSC.

### Management of the MoU



- 39. Under this MOU, the parties agree to work constructively with each other. To support this, the parties agree to provide feedback from time to time on the quality of the working relationship between them and, as necessary, consider changing how they engage with each other to achieve an effective working relationship.
- 40. The parties have both identified key persons responsible for managing this MoU:
- 41. Persons responsible:

Information Commissioner's Office	NCSC
Director of Regulatory Cyber, Regulatory Supervision  Deputy Commissioner, Regulatory Supervision  	Deputy Director Incident Management  Deputy Director Critical National Infrastructure  

- 42. These 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.
- 43. The parties will monitor the operation of this MoU and will review it every two years.
- 44. Any minor changes to this MoU identified between reviews may be agreed in writing between the parties.
- 45. Any issues arising in relation to this memorandum will be notified to the point of contact for each organisation (as identified above).
- 46. The NCSC and ICO both agree to uphold and respect this MoU.

### Signatories

<b>John Edwards</b> <b>Information Commissioner</b>	<b>Lindy Cameron</b> <b>CEO</b>
--	------------------------------------

Information Commissioner's Office	NCSC
	
Date: 12/09/2023	Date: 12/09/2023

v1

Note: This document has been signed and signatures redacted for publication.