Department for Digital, Culture Media & Sport

Cabinet Office

# Draft Information Sharing Code of Practice

Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017

Presented in draft to Parliament pursuant to sections 43(7), 52(7) and 60(7) of the Digital Economy Act 2017 for approval by resolution of each House

May 2018

Produced by the Department for Digital, Culture, Media and Sport and the Cabinet Office

permission from the copyright holders concerned.

# Contents


| | |
|---|---|
| **1. Overview (this applies to the public service delivery, debt and fraud chapters)** | 5 |
| | 5 |
| 1.1 - About the Code of Practice | 8 |
| 1.2 - Data sharing principles | 10 |
| 1.3 - Information sharing and the law | 15 |
| 1.4 - Understanding the public service delivery, debt and fraud powers | |
| **2. Public Service Delivery** | 20 |
| 2.1 - Understanding the purpose of the public service delivery power | 20 |
| 2.2 - Understanding the purpose of the fuel and water poverty powers | 21 |
| 2.3 - Using the public service delivery power | 23 |
| 2.4 - The process for establishing a new objective under the public service delivery power | 24 |
| 2.5 - Process for using the public service delivery power | 27 |
| **3. Debt** | 31 |
| 3.1 - Understanding the purpose of the debt power | 31 |
| 3.2 - Using the debt power | 32 |
| 3.3 - Process for using the debt power | 35 |
| 3.4 - The Fairness Principles for data sharing under the debt power | 39 |
| **4. Fraud** | 41 |
| 4.1 - Understanding the purpose of the fraud power | 41 |
| 4.2 - Using the fraud power | 42 |
| 4.3 - Process for using the fraud power | 44 |
| **5. Fairness and transparency** | 49 |
| 5.1 - Register of information sharing activity | 49 |

| | |
|---|---|
| 5.2 - Other documentation | 51 |
| **6. Governance**<br><br>6.1 - Implementing a data sharing arrangement<br>6.2 - Compliance with the Code | 55<br><br>55<br>55 |
| **Annex A - conflicts of interest** | 57 |

# 1. Overview (this applies to the public service delivery, debt and fraud chapters)

1. Part 1 of the Code of Practice sets out its purpose and status and gives other important information about requirements that all persons who are involved in disclosing or using information under the public service delivery, debt and fraud powers will need to understand if they wish to make use of these powers in Chapters 1, 3 and 4 respectively of Part 5 of the Digital Economy Act 2017.

# 1.1. About the Code of Practice

2. Part 5 of the Digital Economy Act 2017 introduces a number of new powers to share information to help make the digital delivery of government services more efficient and effective. Sections 35 to 39 are collectively considered to benefit the delivery of public services. Section 35 allows for information sharing between public authorities for public service delivery objectives that have been specified in regulations. Sections 36 to 39 differ in that they provide specific powers for energy suppliers and water and sewerage undertakers to allow for the more efficient delivery of public authority schemes intended to help people living in fuel and water poverty. References to public service delivery in this Code refer to all information sharing arrangements under sections 35-39, unless otherwise specified. Sections 48 and 56 create specific gateways to share information for the purpose of managing debt and fraud against the public sector respectively. While the Digital Economy Act 2017 provides a legislative gateway to share information, public authorities will also need to have robust safeguards in place to ensure that people's information is processed in a secure and appropriate way in line with the requirements of “the data protection legislation”.[1]

3. The purpose of this Code is to provide a set of principles and guidance for the use and disclosure of information under these powers. It also refers to other requirements when sharing information, and explains what these requirements are likely to mean in practice in the context of an information sharing arrangement under the Digital Economy Act 2017.

[1] In this Code, “the data protection legislation” means the full, applicable data protection framework as set out in the Data Protection Act 2018. This encompasses general processing (including the General Data Protection Regulation and the applied GDPR), law enforcement processing, and intelligence services processing. References to “the Data Protection Act 1998” in the Digital Economy Act 2017 are amended to “the data protection legislation” by the Data Protection Act 2018.

## The Code's status

4. This Code is issued by the Secretary of State under section 43 of the Digital Economy Act 2017 and by the Minister for the Cabinet Office under sections 52 and 60 of that Act. It has been developed in consultation with the Information Commissioner's Office ("ICO"), the Commissioners for Her Majesty's Revenue and Customs, the devolved administrations, and other interested persons. It has been laid before Parliament and the devolved legislatures in Scotland and Wales, in accordance with the Digital Economy Act 2017.

5. This Code will be reviewed periodically. Any changes resulting from the review will be made in consultation with the parties named above, and revised copies laid before Parliament and the devolved legislatures in Scotland, Wales and Northern Ireland in accordance with sections 43, 52 and 60 of the Digital Economy Act 2017.

6. The Code does not itself impose additional legal obligations on parties seeking to make use of the powers, nor is it an authoritative statement of the law. It sets out principles and good practice to follow when exercising the powers set out in the Digital Economy Act 2017. Anyone sharing information under Chapters 1, 3 and 4 of Part 5 of the Digital Economy Act 2017 is required to have regard to this Code when doing so. Government departments will expect public authorities and other participants in an information sharing arrangement to agree to have regard to the Code before any information is shared. Failure to have regard to the Code may result in your public authority or organisation losing the ability to disclose, receive and use information under the powers. In addition, there are criminal sanctions for disclosing personal information in ways that are not permitted by the Digital Economy Act 2017 including onward disclosure of information other than for the limited exceptions set out in Part 1.4.

7. This Code is required to be consistent with the Information Commissioner's data sharing code of practice ("the ICO data sharing code"), as altered or replaced from time to time, and should be read alongside it.

## Definition of "information sharing"

8. This Code uses essentially the same definition of "information sharing" as the ICO data sharing code: the disclosure of information from one or more organisations to a third-party organisation or organisations, or the sharing of information between different parts of an organisation. The ICO data sharing code says that data sharing can take different forms including:

    - a reciprocal exchange of data;
    - one or more organisations providing data to a third party or parties; or

- several organisations pooling information and making it available to each other.

9. While we consider the terms 'information' and 'data' to have the same meaning, "personal information" in the Digital Economy Act 2017 has a slightly different meaning to "personal data" in the data protection legislation. In this Code, personal information is information which relates to and identifies a particular person or body corporate (but which does not relate to the internal administrative arrangements of a person who may disclose or receive information under the Digital Economy Act 2017).[2] The data protection legislation, which replaces the Data Protection Act 1998 and applies the General Data Protection Regulation, has an expanded definition of "personal data" from the one used in the Data Protection Act 1998. This includes information relating to location, online identifiers and pseudonymised data (de-identified data which needs additional information to be fully attributed to a data subject). You need to apply both definitions when you use these powers because you must both observe the requirements for "personal information" under the Digital Economy Act 2017 and make sure that you have also complied with the requirements for "personal data" under the data protection legislation.

10. This Code provides a framework to help organisations understand their obligations on information sharing and data handling. If you follow the best practice and recommendations set out in the Code, this will help you to be compliant with the data protection legislation and other relevant legislation.

    However, you should seek your own legal advice to support specific information sharing arrangements.

## Who should use the Code

11. All persons who are involved in disclosing or using information under the public service delivery, debt and fraud powers must have regard to this Code. A requirement to comply with the Code where it applies and a statement that due regard has been had to the Code should be included in any information sharing agreement produced for such sharing.

12. Public authorities and specified persons providing a service to public authorities who are able to make use of these powers are set out in in Schedules 4-8 to the Digital Economy Act 2017.[3] Health and adult social care bodies are not

[2] In practice authorities are likely to want to apply the Data Protection Principles to all processing of information under this Act, where they are relevant, to ensure that best practice is followed in processing such information.

[3] These Schedules will be amended and kept up to date by regulations made by Parliament and the devolved legislatures - http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted

included in the list of specified persons permitted to use the new powers in England or for UK-wide activities. Arrangements for information sharing under this Code of Practice therefore should not include health and adult social care bodies in England or for activities that are not devolved. Until the recommendations made by the National Data Guardian's Review of Data Security, Consent and Opt-outs have been implemented and there has been public consultation, including with appropriate representative health bodies, adult health and social care bodies in England and for activities which are not devolved will not be added to the Schedules. For further information, please refer to Part 1.4 of this Code.

# 1.2. Data sharing principles

13. It is of vital importance that data is handled in a way that inspires the trust and confidence of citizens. The following principles support the security of data and privacy of citizens whilst enabling the delivery of better services and outcomes for citizens and government.

| Stages of the Data Sharing Lifecycle | Principles |
|---|---|
| Agreeing to Share | 1. In deciding whether to include persons in information sharing activity, consider if the sharing is necessary and proportionate to achieve the desired objective.<br><br>2. Privacy impact assessments (or data protection impact assessments[4]) are carried out before any data sharing takes place and reviewed at critical milestones throughout the lifecycle. They should be made available to citizens in line with ICO guidance.[5]<br><br>3. Information about information sharing agreements[6] under the public service delivery, debt and fraud powers is made available to citizens in a searchable electronic list, unless there are particular national security issues or other sensitivities which would outweigh the public interest in doing so.<br><br>4. Steps should be taken to minimise the amount of data shared, and ensure this is the minimum required for the |

[4] Under the data protection legislation, privacy impact assessments are known as "data protection impact assessments". However, it is important to note that the data protection legislation (unlike the Data Protection Act 1998) sets out certain circumstances in which a data protection impact assessment must be carried out, and what the assessment must contain.
[5] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[6] Information sharing agreements are a common set of rules binding on the organisations involved in the information share. The agreement should identify all the organisations that will be involved in the information share. It should be initiated by the controller. The controller will also be responsible for submitting the required information about an information share to relevant registers (see Part 5.1).

| | |
|---|---|
| | purpose of achieving the specified objective, using methods which avoid unnecessarily sharing or copying of large amounts of personal information. |
| Hold | 5. Data is always held securely, to the appropriate security standards.<br><br>6. Data held is maintained to the appropriate quality and where appropriate citizens can view, correct and delete data held about them. |
| Use | 7. Data held can only be used for specified purposes.<br><br>8. The ethical issues around the use of data are factored into the decision-making process and any new data analysis techniques are assessed against the Data Science Ethical Framework.[7]<br><br>9. Relevant codes of practice (e.g. Technology Code of Practice[8] and Code of Practice for Official Statistics[9]) are adhered to when accessing and analysing data. |
| Delete | 10. Data is only kept as long as necessary and is then securely deleted. |

14. All persons using the public service delivery, fraud and debt powers are required to apply these principles when they do so. These are separate to the Data Protection Principles referenced in Part 1.3 of this Code which should also be adhered to. Further guidance on data standards, security, retention and disposal are provided in Part 1.3 below.

15. These principles are underpinned by four key requirements:

- Before using the powers you must carefully assess whether disclosure is

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf

[8] https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice#the-technology-code-of-practice

[9] https://www.statisticsauthority.gov.uk/wp-content/uploads/2015/12/images-codeofpracticeforofficialstatisticsjanuary2009_tcm97-25306.pdf

consistent with both the Digital Economy Act 2017 and the requirements of the data protection legislation. You should also have regard to the relevant Codes of Practice issued by the Information Commissioner.

- You must only share the minimum data required to fulfil the stated purpose for sharing. Limit the amount of data copied or shared as far as you are able and where possible, develop and use application programming interfaces[10] (APIs) to run binary checks ('yes' or 'no' answers) or exchange attributes.

- Information sharing agreements should, subject to limited exceptions, ensure that where datasets are linked, it should be for the specified purpose and should not lead to the creation of new identity registers.[11] Information sharing agreements must include details of retention and destruction policies that prevent the retention or use of data for longer than it is needed or its use for any purposes other than those for which it was disclosed/received (subject to limited exceptions provided for in law).

- You must be transparent about your use of the powers so citizens can understand what data is being shared, the bodies that are disclosing or receiving data, and why. Unless there are particular national security or other sensitivities which would outweigh the public interest in disclosure, information about information sharing agreements should be published in a searchable electronic public register. You must also have regard to the ICO's codes of practice such as the one on privacy notices.[12]

# 1.3. Information sharing and the law

## How the powers work with other legislation

16. For information to be disclosed lawfully under the public service delivery, debt and fraud powers, you need to operate according to the Digital Economy Act 2017 and comply with other relevant legal requirements which are either overarching under UK law or which are expressly preserved by the Digital Economy Act 2017. These are:

[10] API means a set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service. When used in the way proposed, an API check restricts the amount of data which is processed or transferred to the minimum necessary and so helps provide user privacy and security.
[11] A limited exception would be for example where a dataset is held, for national security purposes, further to a warrant approved by a Judicial Commissioner under Part 7 of the Investigatory Powers Act 2016.
[12] https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf

- the data protection legislation;
- Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016 (and, until that Act comes fully into force, Part 1 of the Regulation of Investigatory Powers Act 2000);
- obligations in European law which are binding in UK law; and
- the Human Rights Act 1998.

17. The data sharing powers under the Digital Economy Act 2017 are not, in general, suitable for the sharing of information which is sensitive on national security grounds, and in particular any information which was provided directly or indirectly by an intelligence service (MI5, MI6 or GCHQ) and was subject to express restrictions on disclosure. You must therefore always consider at the outset whether it is permissible to share information on security grounds. You must also adhere to the Security Policy Framework[13] and observe handling controls in relation to protective markings. If in doubt, seek advice from your organisation's security officer and, in all cases of national security sensitivity, ensure that authorisation is sought from those who have provided the information in question.

18. You should seek your own legal advice if you are unsure whether a proposed use of the public service delivery, fraud or debt powers is lawful.

19. Unlawful disclosure of personal information by HM Revenue and Customs is subject to criminal sanctions set out in section 19 of the Commissioners for Revenue and Customs Act 2005. The Digital Economy Act 2017 extends that sanctions regime to offences under the Digital Economy Act 2017 which involve the unlawful disclosure of information received contrary to section 41 of the Digital Economy Act 2017 or received from HM Revenue and Customs (see section 42).

## Data Protection Legislation

20. The data protection legislation requires that personal data is processed fairly and lawfully and that individuals are aware of which organisations are sharing their "personal data" and what it is being used for (the "lawfulness, fairness and transparency" principle). Some information disclosed under these powers will not constitute personal data: for example, data relating to deceased persons, businesses, or information comprising only statistics that cannot identify anyone. The data protection legislation will not apply in these instances, although its principles will often still be relevant and it may be practical to treat all information in the same way. Disclosures will still need to comply with the Human Rights Act

[13] https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

1998 (see below).

21. Public authorities will need to demonstrate that they are complying with the provisions contained in the data protection legislation including adhering to the Data Protection Principles.

22. The Data Protection Act 1998 set out eight principles which had to be complied with when personal data was collected, held or otherwise processed. These principles are largely carried over to the data protection legislation (although some are strengthened or clarified).

## Data Protection Principles

23. Article 5 of the General Data Protection Regulation sets out six principles relating to processing of personal data. Personal data shall be:

(a) "processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage

limitation");

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")".

In addition, controllers (known as "data controllers" in the Data Protection Act 1998) must be able to demonstrate that they are in compliance with the these principles. This is known as the "accountability" principle

24. The above principles apply to general data processing. However, please note that there are slightly different principles, as set out in the data protection legislation, which apply in respect of law enforcement data processing and intelligence services data processing which should be referred to when considering those types of processing.

25. For more detail on these six principles read the ICO's guide to data protection[14] or contact your local data protection adviser.

## The Data Protection Act 2018

26. The Data Protection Act 2018 will replace the Data Protection Act 1998, apply the General Data Protection Regulation standards (which will take effect from 25 May 2018) and implement the Law Enforcement Directive.[15] The Data Protection Act 2018 will cover general data processing, as well as law enforcement data processing and intelligence services data processing.

27. It is important for practitioners to be aware of the requirements and obligations contained in the data protection legislation. Although many aspects of the regime will be familiar from the Data Protection Act 1998, there are some new requirements and processes. For example, some of the changes made by the General Data Protection Regulation include:

- Changes to some of the definitions that set the scope of data protection law. For example, the definition of "personal data" is more detailed and makes

[14] https://ico.org.uk/for-organisations/guide-to-data-protection/

[15] The Law Enforcement Directive (EU 2016/680) concerns the processing of personal data by competent authorities for law enforcement purposes. The Data Protection Act 2018 transposes the provisions of the Law Enforcement Directive into UK law.

explicit provision for a wider range of personal identifiers to constitute personal data.
- The new concept of "special categories of personal data". This includes genetic data and biometric data.
- Additional rights for individuals - such as the right to be informed or the right to have personal data rectified or erased in specific circumstances.
- Processing of data which falls into a 'special category' due to its sensitivity is prohibited unless certain conditions are met.
- The Information Commissioner's powers are extended - in the most serious cases, the Commissioner can issue a maximum penalty of £18 million (€20 million) or 4% of turnover. The data protection legislation ensures the Commissioner's powers to issue fines are subject to certain safeguards, including the form of notice given and a right of appeal. The data protection legislation also includes information about how to exercise appeal rights.

28. Although when the Digital Economy Act 2017 was first passed it referred to the data protection obligations under the Data Protection Act 1998, these references have been amended by the Data Protection Act 2018 so that they now refer to "the data protection legislation".

## The Investigatory Powers Act 2016

29. The Investigatory Powers Act 2016[16] provides a framework for lawful interception of communications, equipment interference, the obtaining and retention of communications data and the retention and examination of bulk personal datasets. Where relevant, any potential disclosure under the public service delivery, debt or fraud powers which would be prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016 would be unlawful and must not be made. Until that Act is fully in force, Part 1 of the Regulation of Investigatory Powers Act 2000 continues to apply.

## Human Rights Act 1998

30. Public authorities must always ensure that data sharing is compliant with the Human Rights Act 1998 and must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

31. Article 8 of the Convention, which gives everyone the right to respect for their private and family life, home and correspondence, is especially relevant to sharing personal information. Whilst sharing data relating to deceased individuals is not personal data under the data protection legislation as outlined above, you

[16] http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

should consider whether sharing this information could affect the right to private life of the relatives of deceased individuals.

## Commissioners for Revenue and Customs Act 2005

32. Although the unlawful disclosure of information received from HM Revenue and Customs under the Digital Economy Act 2017 is governed by offences in that Act, those offences have been framed so that they are consistent with the protection for information under the Commissioners for Revenue and Customs Act 2005. Elements of section 19 of the Commissioners for Revenue and Customs Act 2005, which deal with the penalties for and prosecution of unlawful disclosure of Revenue and Customs information, also apply to relevant Digital Economy Act 2017 offences.

# 1.4 Understanding the public service delivery, debt and fraud powers

33. This part sets out the elements of the Digital Economy Act 2017 which apply across the public service delivery, debt and fraud chapters. It also provides further guidance on data standards, security, retention and disposal of data referred to in the data sharing principles (Part 1.2 of this Code).

## Onward disclosure of information under the public service delivery, debt and fraud powers

34. Normally, information disclosed under these powers can only be used for the purposes for which it was disclosed. However there are very limited instances where information can be used by a public authority for another purpose. These circumstances vary between the powers but include:

- if the information has already been lawfully placed into the public domain;
- if the data subject has consented to the information being used for the other purpose;
- for the prevention or detection of crime or the prevention of anti-social behaviour;
- for the purposes of a criminal investigation;
- for the purposes of legal proceedings;
- for the purposes of safeguarding vulnerable adults or children; or
- for the purposes of protecting national security.

35. A different regime applies to personal information disclosed by HM Revenue and Customs, which would include information disclosed by the Valuation Office Agency. Personal information disclosed by the Revenue and Customs can only be used for purposes other than the purpose for which it was originally disclosed with the Revenue and Customs' consent.

## Which organisations can use the powers?

36. The public service delivery, debt and fraud powers are permissive powers, which means the persons who are potentially able to share information under them can choose whether or not to do so. Those persons are "specified" public authorities and persons who provide services to specified public authorities who have themselves been specified. Only those persons listed in Schedules to the Digital Economy Act 2017 and the persons listed in sections 36 to 39 of the Digital Economy Act 2017 are able to disclose information under the respective

powers.

37. It may be helpful to consider the public service delivery power to be separated into three distinct parts: section 35 (general public service delivery), sections 36-37 (fuel poverty) and sections 38-39 (water poverty). Section 35 is the general public service delivery power, which allows for sharing between public authorities (or persons providing services to public authorities) for specified objectives that meet the criteria in section 35. These objectives must be set out in regulations. A list of specified persons able to use the section 35 power is set out in Schedule 4. Sections 36 to 39 of the Digital Economy Act 2017 provide powers to assist persons in fuel and water poverty; these sections enable information to be shared by and to licensed gas and electricity suppliers or water and sewerage undertakers for those purposes. Accordingly, there are separate schedules (5 and 6) that set out the specified persons and specific restrictions that apply to sharing under sections 36 to 39. Additionally, the specified persons for debt are set out in Schedule 7 and those for fraud in Schedule 8.

38. There is a definition of "public authority" for each power. The powers allow a person providing services to a public authority to share information as well as the public authority itself, on the condition that the service provider has also been specified. The Schedules contain generic descriptions of such persons. For example, the public service delivery power includes in its Schedule of specified persons "a person providing services in connection with a specified objective (within the meaning of section 35) to a specified person who is a public authority".

39. A person providing services to a public authority can potentially be any person or body, such as a charity or company providing a defined service(s) to a public authority. For example, this could be a frontline service outsourced to a body outside the public sector to deliver. In addition to the conditions set out in the Digital Economy Act 2017 (including information security) the initial consideration in deciding whether to include such persons in a proposed information share is whether enabling the sharing of the relevant information with that organisation and other public authorities is necessary to achieve the desired objective.

## Amending the list of persons able to use the power

40. The public service delivery, debt and fraud powers specify in Schedules 4-8 of the Digital Economy Act 2017 the public authorities that can use the powers. The Secretary of State, the Minister for the Cabinet Office, or the relevant authority from a devolved administration can make regulations to add, modify or remove a reference to a public authority or description of a public authority. Applications to amend the Schedules should be made through the secretariats for the relevant review board (as set out in sections 2, 3 and 4 of this Code).

41. Health and adult social care bodies are not included in the list of specified persons permitted to use the new powers in England and for activities that are not devolved. Arrangements for information sharing under this Code of Practice therefore should not include health and adult social care bodies in England or for any non-devolved activities. Until the recommendations made by the National Data Guardian's Review of Data Security, Consent and Opt-outs have been implemented and there has been public consultation, including with appropriate representative health bodies, adult health and social care bodies in England and for non-devolved activities will not be added to the Schedules.

## Non-public authority duties

42. Where an information sharing arrangement proposes that information be disclosed to or received from a body which is not a public authority,[17] the body should be asked to declare all potential conflicts of interest (see Annex A), for example from other work it does for public authorities or its own commercial interests. An assessment should be made of any conflicts of interest that the non-public authority may have, to identify whether there are any legal or reputational risks involved in sharing data with the organisation. If such risks are identified, appropriate steps should be taken to help reduce the risks to acceptable levels. If that cannot be done, information should not be shared with the body.

43. Non-public authorities can only participate in an information sharing arrangement once their sponsoring public authority has assessed their systems and procedures to be appropriate for secure data handling. Details will need to be set out in the privacy impact assessment (data protection impact assessment), along with a statement of compliance with this Code of Practice (where it applies) in the information sharing agreement.

## Data standards

44. Public authorities hold data in a number of different formats. When planning to share data, make sure that the data's format and sharing protocol follow all the relevant standards set out in the Open standards for government data and technology[18] and the API standards[19] if at all possible, unless it would be disproportionate to do so.

[17] Non-public authorities includes bodies covered by paragraph 28 of Schedule 4, paragraph 18 of Schedule 5, paragraph 12 of Schedule 6, paragraph 17 of Schedule 7 and paragraph 41 of Schedule 8 to the Digital Economy Act 2017. This also includes licensed gas and electricity suppliers and water and sewerage undertakers to which information may be shared with under sections 36 - 39.
[18] https://www.gov.uk/government/collections/open-standards-for-government-data-and-technology
[19] https://www.gov.uk/service-manual/technology/application-programming-interfaces-apis

45. You should check the accuracy of data prior to transferring it, in line with the Data Protection Principles. Organisations involved in an information sharing arrangement should also agree procedures and processes for:

- correcting inaccurate data and making sure all bodies that the data has been transferred to correct it too;
- recording and capturing corrections for auditing purposes;
- deleting data, where there is a right to erasure;
- contacting the data subject where appropriate;
- how information and access to data is to be provided to data subjects;
- how data subjects can exercise their rights to restrict and object to processing.

46. These requirements must be set out in the information sharing agreement. You will also need to apply your organisation's procedure for correcting inaccurate data and deleting data held on your own systems, including alerting officials responsible for data protection and any other teams that hold the relevant data on their systems.

47. Public authorities making their data available must make sure that they share the minimum amount of personal information required to properly fulfil the purpose for which it is being processed. This is referred to in the data protection legislation as the "data minimisation" principle. Organisations must design and structure information sharing processes to avoid oversharing: i.e. disclosing more information about individuals, or about more individuals, than is strictly required. Organisations should format as much of their output as possible into standardised minimal confirmations of specific questions (for example a yes/no answer in response to an eligibility check) or using data matching techniques. Organisations must work with data recipients to understand their specific needs and how data sharing can be minimised.

## Data security

48. Everyone who is involved in information sharing arrangements under these powers is required to comply with the security requirements in the Digital Economy Act 2017 and the data protection legislation, and have regard to the specific security standards outlined below.

49. There are three specific requirements in this Code:

- public authorities and receiving parties should factor the standards and protocols that apply to their organisation when providing or receiving information before agreeing appropriate standards and protocols. All parties should be satisfied that they provide a level of security that is both

appropriate and meets or exceeds their own standards and protocols;
- each party involved in the data share must make sure effective measures are in place to manage potential or actual incidents relating to the potential loss of information; and
- public authorities and data processors, together with any other additional third parties, must be fully engaged in the resolution of a potential or actual data incident. The responsibilities of each party in the event of a potential or actual loss of information must be clearly defined in the information sharing agreement or security plan. The controller has a responsibility to inform the ICO of a breach where the relevant thresholds are met.

50. You will need to agree a security plan as part of any formal information sharing agreement with public authorities and third parties who are party to the data share. Security plans should include:

- storage arrangements that make sure information is secured in a robust, proportional and rigorously tested manner, including how to comply with protective marking handling requirements where applicable;
- assurance that only people who have a genuine business need to see personal information will have access to it;
- who to notify in the event of a security breach;
- procedures to investigate the causes of any security breach.

## Data retention and disposal

51. It is a requirement of the data protection legislation that personal information should be kept only for as long as necessary. How long it is necessary to hold personal information depends on the purpose for which the public authority holds the information. This is referred to in the data protection legislation as the "storage limitation" principle.

52. You will need to agree with recipients of data shared under these powers how long the data is expected to be held for. The period agreed should be documented in the information sharing agreements between both parties and you should continuously review the need to continue to hold information.

53. You should put procedures in place to ensure that data no longer required is destroyed promptly and securely and rendered irrecoverable. The same will apply to data derived or produced from the original data, (subject to the specific rules on data processed for research purposes). You should refer to the ICO guidance on Deleting Personal Data.[20]

[20] https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

# 2. Public Service Delivery

54. This part of the Code is for organisations wishing to make use of the public service delivery power. It sets out the purpose of the general public service delivery provisions, current objectives, how the powers are to be used, and the process you will need to follow to set up a new objective. Guidance is also provided in section 2.2 which specifically relates to the fuel and water poverty provisions.

# 2.1 Understanding the purpose of the public service delivery power

55. Public service delivery is changing, due to increasing acknowledgement that services are more efficient and effective when they are joined up. Joining up services requires the sharing of information. The Digital Economy Act 2017 creates a mechanism for establishing clear and robust legal gateways which will enable public authorities to share relevant information on the individuals and families they are working with in compliance with the data protection legislation. The primary purpose of this power is to support the well-being of individuals and households.

56. The public service delivery power gives you the ability to gain access to the data you need to respond more efficiently and effectively to current and emerging social and economic problems. The power allows ministers in the UK government and, for devolved matters, the devolved administrations to set objectives in regulations. All objectives must meet all of the following conditions which are set out in section 35 of the Digital Economy Act 2017:[21]

- condition 1: the purpose is the improvement or targeting of a public service provided to individuals or households, or the facilitation of the provision of a benefit (whether or not financial) to individuals or households;
- condition 2: the purpose is the improvement of the well-being of individuals or households; and
- condition 3: the purpose is the supporting of the delivery of a specified person's functions, or the administration, monitoring or enforcement of a specified person's functions.

57. For an explanation of terms in the above conditions — for example, "benefit" and "well-being" — please refer to the Digital Economy Act 2017 and its Explanatory Notes.

[21] http://www.legislation.gov.uk/ukpga/2017/30/section/35/enacted

58. Here is a summary of the initial objectives for which information may be disclosed by specified persons under section 35 of the 2017 Act. For full details of the objectives, see the Schedule to the Digital Government (Disclosure of Information) Regulations 2018.

- Identifying individuals or households who face multiple disadvantages and enabling the improvement or targeting of public services to such individuals or households and providing for the monitoring and evaluation of programmes and initiatives;
- Assisting people living in fuel poverty by reducing their energy costs, improving efficiency in their use of energy or improving their health or financial well-being;
- Reducing water or sewerage costs, improving efficiency in use of water or improving the health or financial well-being of people living in water poverty; and
- Identifying and making contact with vulnerable people who might need help from the authorities in re-tuning televisions in 2018 to 2019 after the 700Mhz band will be used for mobile broadband rather than to transmit digital TV.

Additional objectives can be set by further regulations under section 35 of the Digital Economy Act 2017.

# 2.2 Understanding the purpose of the fuel and water poverty powers

59. There are powers to assist persons living in fuel poverty or water poverty both in the initial regulations made under section 35 and in sections 36 to 39 of the Digital Economy Act 2017. These powers can work together but have different purposes. Under section 35, the two “public service delivery” objectives which relate to fuel and water poverty allow specified public authorities to share information with each other to assist persons living in fuel and water poverty. The powers in sections 36 to 39 allow public authorities to share information with energy, water and sewerage companies for the same purpose, but only in connection with specific fuel poverty measures listed in or added to those sections.

## Section 35 and fuel and water poverty

60. The initial regulations identify the public authorities, including local authorities and their service providers, which are able to share information between themselves in connection with the aim of alleviating fuel or water poverty.

61. They will enable better targeting of support from local and national schemes, by enabling, for example, DWP and HMRC to disclose social security information, and enabling the Valuation Office Agency (VOA) to share property characteristics information with other specified public authorities to help identify customers who are more at risk of fuel or water poverty - for example, those who live on a low income or live in inefficient properties.

## Sections 36 and 37: Fuel poverty

62. Section 36 of the Digital Economy Act 2017 allows the public authorities which are specified in Schedule 5 to disclose information to licensed gas and electricity suppliers. The disclosure must be for the purpose of assisting people living in fuel poverty by reducing their energy costs, or improving efficiency in their use of energy or improving their health or financial well-being. The disclosure must be in connection with a fuel poverty measure listed in section 36(3) of the Digital Economy Act 2017 (i.e. a scheme, an arrangement or a function). Currently the Digital Economy Act 2017 lists the Warm Home Discount (WHD), the Energy Company Obligation (ECO) and devolved grant schemes. The relevant Minister can add, remove or amend the list of fuel poverty measures, the list of public bodies allowed to share information, and the list of persons permitted to receive information through regulations.

63. Subject to some very limited exceptions, the Digital Economy Act 2017 prohibits the use of the information shared under section 36 for any purposes other than the fuel poverty measures listed in that section. The information shared must be the minimum amount required for the purpose of the specified fuel poverty measure, and shared in line with the data protection legislation and the requirements of this Code.

64. Therefore, we would normally expect the only government data to be shared with suppliers under those arrangements would be a “yes/no” or unknown answer to whether their customer is eligible or suitable for support. The provision of more detailed information would need particular justification, for example, if it was necessary in order to provide additional support to certain groups of customers under the scheme.

65. Section 37 of the Digital Economy Act 2017 allows gas and electricity suppliers to share certain customer data with specified public authorities. This enables the matching of suppliers’ customer data with Government-held data to provide the “yes/no” or unknown answers indicating which of the suppliers’ customers would be eligible or suitable for assistance under a fuel poverty scheme.

66. Under sections 36 and 37 of the Digital Economy Act 2017, misuse of information is likely to breach the data protection legislation and attract the sanctions available under the data protection regime, including criminal sanctions under the Digital Economy Act 2017. It could also be a breach of the information sharing agreement with possible contractual remedies, and/or a breach of the Code with possible sanctions that include removal from the list of specified persons able to take part in information sharing for the fuel poverty objective.

## Sections 38 and 39: Water poverty

67. Section 38 of the Digital Economy Act 2017 allows specified public authorities listed in Schedule 6 to disclose information to water and sewerage undertakers, for the purpose of assisting people living in water poverty by reducing their water or sewerage costs, improving efficiency in their use of water, or improving their health or financial well-being. The disclosure must be in connection with a water poverty measure listed in section 38(3) of the Digital Economy Act 2017 (i.e. a scheme, an arrangement or a function).

68. Currently the schemes listed in the Digital Economy Act 2017 include social tariffs as provided for under section 44 of the Flood and Water Management Act 2010 and the WaterSure Scheme under regulation 2 of the Water Industry (Charges) (Vulnerable Groups) (Consolidation) Regulations 2015.

69. Subject to some very limited exceptions, the Digital Economy Act 2017 prohibits the use of the information shared under section 38 for any purposes other than the water poverty measures listed in that section. The information shared must be the minimum amount required for the purpose of the specified water poverty measure, and shared in line with the data protection legislation and the requirements of this Code.

70. Section 39 allows water and sewerage undertakers to share details of their customers with specified public authorities.

71. The relevant Minister can add, remove or amend the list of water poverty measures, the list of public bodies allowed to share information and the list of persons permitted to receive information through regulations.

72. Information sharing arrangements between undertakers and specified public authorities are expected to operate on the same basis as those between energy suppliers and public authorities.

73. Under sections 38 and 39 of the Digital Economy Act 2017, misuse of information is likely to breach the data protection legislation and attract the sanctions available under the data protection regime, including criminal sanctions

under the Digital Economy Act 2017. It could also be a breach of the information sharing agreement with possible contractual remedies, and/or a breach of the Code with possible sanctions that include removal from the list of specified persons able to take part in information sharing for the water poverty objective

## 2.3 Using the public service delivery power

73. If your organisation has identified that the sharing of personal data is necessary to achieving a social or economic policy you should check whether the policy aims fall within one of the existing objectives set out in regulations. If it doesn't you should consider whether your purpose for information sharing falls within the criteria in section 35 and should be added as a new objective via regulations (see section 2.3). You should identify which public authority holds the information you wish to access and check whether they are listed on Schedule 4. If the public authority is not listed, it is possible to add them to the Schedule via regulations (see section 2.3). If the public authority is listed you need to carefully consider whether your policy aims are consistent with the objectives described in regulations. Seek legal advice where appropriate. The public service delivery provisions and all chapters in Part 5 of the Digital Economy Act require that processing of information must be carried out in accordance with the data protection legislation.

An illustrative example of an appropriate use of the PSD power:

- A local authority wishes to access data held by the local police force and local school to identify whether there are individuals or households who meet the criteria for support under the troubled families programme.
- The local authority considers the multiple disadvantages objective and assesses that the objective is consistent with the purpose of the proposed information share. The bodies that the local authority wishes to share data with are also present on Schedule 4.
- The local authority has a lawful basis to share data. As the powers are permissive, the local authority will still need to agree with the other bodies to share information for this purpose and draw up an appropriate data sharing agreement.

74. The disclosure of data to achieve a public service delivery objective must only be used for the purpose for which it was disclosed, unless one of the

exceptions in section 40(2) of the Digital Economy Act 2017 is engaged - for example, preventing serious physical harm to a person or loss of life. In such instances section 40 permits the specified person(s) to use that information to take action in accordance with the identified exception, using the minimum information required to fulfil that purpose. The exceptions in section 40(2) do not apply to information disclosed by Her Majesty's Revenue and Customs (unless the Commissioners for Her Majesty's Revenue and Customs have provided consent).

## 2.4 The process for establishing a new objective under the public service delivery power

75. The public service delivery provisions provide public authorities with the power to create new objectives for which information can be shared. If your public authority identifies a long-term or time-limited objective for information sharing that meets the conditions in section 35(9), (10) and (12), it is possible to create a new objective via regulations. To propose a new objective, you need to determine what types of data are required, which bodies hold the data and how the ability to share personal data will support the achievement of your policy objectives.

**Example objectives**

Examples of potentially suitable topics for objectives which would deliver an improvement in a service or benefit are:

- reducing the number of people sleeping on the street for more than one night;
- improving employment outcomes for ex-offenders;
- supporting gang members to safely exit gang culture.

Examples of objectives which would not meet the conditions because the objective is punitive instead of providing a benefit and improving well-being are:

- identifying individuals operating in the grey economy;
- identifying welfare claimants erroneously receiving welfare benefits.

Examples of objectives which would not be acceptable because they are too 'general' in terms of targeting communities or conferring a broad public benefit rather than one targeted at individuals or households, or which are insufficiently specific for an information sharing arrangement include:

- improving levels of safety in a neighbourhood;
- helping people into work;
- preventing people going to prison.

76. A review board will be established by the UK government to advise the relevant Ministers on proposals for new non-devolved or England-only objectives and to ensure a consistent strategic approach to the use of the public service delivery powers. All proposals for objectives must be submitted to the review board. The review board will be supported by a secretariat based in the Government Digital Service and will sit on a quarterly basis.

77. The review board will consist of senior officials from relevant information governance or social policy areas from across government and will be attended by representatives from the ICO and invited members from appropriate public representative bodies. The secretariat will work with public authorities to ensure relevant information about the proposed objective is prepared and submitted to the review board for consideration.

78. If you wish to establish a new objective you should first consider what policy objectives you are trying to achieve and the data necessary to achieve them. You should also speak to your legal advisers to understand whether new data sharing powers are necessary to access the data required. You should speak to contacts from the relevant departments that either hold or will need to process the data identified to understand any issues that may impact the proposed data sharing. You should be clear about which specified persons in Schedule 4 to the Digital Economy Act 2017 Act will be able to disclose or use data for the proposed purpose. Once you have established the outline details of a proposal for a new objective you should contact the secretariat for the review board. The secretariat will provide advice on how to develop the proposal and the material required for submission to the review board.

79. On receipt of a proposal for a new objective, the secretariat will assess the proposal and will confirm with you whether it is suitable for submission and, if so, the date by which the proposal will be considered by the review board. The board will review the proposed new objective and consider whether it is suitable. It will make recommendations to the relevant Minister on whether the proposal should be taken forward, accepted subject to amendments, or declined. You will be informed of the outcome by the secretariat. Proposals may be declined for

reasons such as:

- The proposed objective does not fully meet the criteria set out in the public service delivery power;[22]
- The proposed objective is drafted too broadly; or
- There is insufficient or unclear justification for sharing information under the proposed objective.

80. All new objectives will be set in regulations which will need to be approved by both Houses of Parliament. Regulations for new objectives must be subject to consultation, as set out in the Digital Economy Act 2017. This will help ensure the government considers views on the proposed objective from those likely to be affected, and that the drafting is appropriately constrained to stand up to parliamentary scrutiny. The secretariat will work with departments to bring together proposals to reduce the pressures on Parliamentary time and ensure consistent approaches to consultation and drafting are adopted.

81. The review board will also be responsible for strategic oversight of the public service delivery power including the searchable electronic register of data sharing. The board will advise Ministers on information sharing under the power and consider complaints and act as a point of contact with the ICO. The board will also consider and coordinate any revisions to the code of practice as necessary.

82. The devolved administrations will establish their own governance structures for oversight of information sharing arrangements within their areas. The UK review board will work closely with governance bodies within the devolved administrations.

# 2.5 Process for using the public service delivery power

## Step 1: Identify the policy objective and the data needed to support it

- Do you need to use personal information? If you don't need it, don't use it:
    - Familiarise yourself with the data protection legislation, the Data

[22] Any proposed specified objective for public service delivery must meet the three conditions set out in section 35(9) - (12) of the Digital Economy Act 2017.

Protection Principles and the ICO data sharing code. Does the proposal pose any ethical issue or will it lead to any data handling risks?
    - Refer to the Data Science Ethical Framework;[23]
    - Consider running a public consultation.
- How do you want to share information and will it be secure?
    - Assess the data you need and ensure you can justify why you need each data item. Build in data protection by design and default, as required by the data protection legislation;
    - Speak to your organisation's information governance and security experts (e.g. the data protection officer) and discuss what the best methods are for data transfer.

## Step 2: Develop the proposal

- Agree a proposal with the other organisations involved in the information sharing arrangement:
    - If bodies outside the public sector[24] are involved you should consider any conflicts of interest (see Annex A) and reflect it in the business case;
    - Ensure all bodies undertake to comply with this Code of Practice;
    - Seek advice from your legal advisers that your proposal is suitable for use under the public service delivery power and is compliant with the data protection legislation or applicable investigatory powers legislation.
- Conduct a privacy impact assessment (or data protection impact assessment):
    - Assess the potential benefits of the information sharing arrangement against the risks or potential negative effects, such as an erosion of personal privacy.
- Develop and draft a business case, information sharing agreements, a privacy impact assessment and security plan:
    - Ensure you have regard to ICO guidance on data sharing agreements and privacy impact assessments and review this assessment at critical milestones;
    - Ensure the responsibilities for each body involved in the information sharing arrangement are understood and articulated in the documentation;

[23] https://www.gov.uk/government/publications/data-science-ethical-framework

[24] This includes bodies covered by paragraph 28 of Schedule 4, paragraph 18 of Schedule 5, paragraph 12 of Schedule 6, paragraph 17 of Schedule 7 and paragraph 41 of Schedule 8 to the Digital Economy Act 2017. This also includes licensed gas and electricity suppliers and water and sewerage undertakers to which information may be shared with under sections 36 - 39.

    - The outcomes of any public consultation or, if a decision was taken not to undertake public consultation, the reasons for that decision, should be articulated in the business case;
    - Ensure each organisation involved in the data sharing arrangement has the appropriate systems and procedures in place to handle data securely and that a security plan has been agreed which sets out how data security will be managed.

## Step 3: Operating the data sharing arrangement

- Managing the information sharing arrangement:
    - You should ensure you comply with the data protection legislation, including the Data Protection Principles;
    - You should ensure you apply fairness and transparency principles as set out in the ICO Code of Practice on Data Sharing;
    - You should ensure the business case, information sharing agreement and privacy impact assessment are made available to the public and reviewed at critical milestones (and be ready to justify any redactions);
    - You should ensure that all bodies adhere to the information sharing agreement and security plan and report any data breaches to the ICO in accordance with the data protection legislation;
    - You should notify the secretariat for the Public Service Delivery review board in the Department for Digital, Culture, Media and Sport (DCMS) of your information sharing arrangement, to be maintained in a searchable electronic register available to the general public.
- Assessment of the information sharing arrangement:
    - At the conclusion of a data sharing arrangement you should assess and review that arrangement and consider publishing the findings including an assessment of benefits derived. This will help improve understanding of data sharing and also help share best practice and lessons learned with other public authorities. Finally, you should ensure that arrangements for the destruction of data which does not need to be retained have been fully implemented.

In considering whether to use the public service delivery powers, the following checklist may also be helpful:

**Checklist: points to consider**

Why share:

- For what purpose and public function is the information being requested?
- What are the benefits of the data exchange for the receiving party or any other public body?
- What are the implications of not sharing information? For example:
    - increased risk that people do not receive the support or the services they require in a timely manner;
    - risk that burdens will be placed on people to repeatedly supply information to access the services they require;
    - risk of wasting taxpayers' money by jeopardising public finances or commercial projects.

What to share:

- What specific data items are required and why?
- Are there reasons why the data should not be shared (consider the Data Protection Principles and any legal restrictions that may apply)?
- Are there any legal obligations on the recipient of the data to provide it to any other bodies?
- How regularly and in what volume is it proposed to share the data?
- Are there any ethical issues with the proposed data sharing arrangement?

How to share:

- What methods or technology can be used to minimise the amount of information shared and risk of data loss for example using aggregate data, derived data or the use of a lookup process, in preference to sharing large amounts of data;
- What procedures will be in place to correct any inaccurate data identified during the data sharing process and the process for capturing the changes made for auditing purposes?
- What are the conditions for processing information? Will data subjects be aware that their data is being processed and will procedures for dealing with access requests, queries and complaints

be in place? How will information be provided to data subjects, in accordance with the requirements of the data protection legislation?

- Information handling responsibilities, including details of any data processors, contractors or subcontractors;
- Security considerations, like the use of secure transfer mechanism, encryption, etc;
- For audit purposes document the process and methods of exchange, how exchanges are logged, what information is stored and who has access to it;
- Standards and levels of expected operational service;
- Termination arrangements;
- Minimising cost of providing/transferring the data;
- Issues, disputes and resolution procedures;
- Sanctions for failure to comply with the agreement or breaches by individual staff;
- Is there a time limit suggested for using the data and, if so, how will the data be deleted?
- Periodic reviews of effectiveness and necessity of data sharing arrangement.

# 3. Debt

83. This part of the Code is for organisations wishing to make use of the debt power in Chapter 3 of Part 5 of the Digital Economy Act 2017. Initially all information sharing under the debt power will be run as pilots. This part of the Code sets out the purpose of the debt provisions and guidance on the process you will need to follow to establish a new pilot.

# 3.1 Understanding the purpose of the debt power

84. As at March 2017, it was estimated that £22.5bn of debt was owed to government.

85. The debt power in section 48 of the Digital Economy Act 2017 creates a permissive gateway that enables information to be shared between specified persons (bodies listed in Schedule 7) in order to take action in connection with debt owed to a public authority or to the Crown. Information sharing between public authorities under the debt power will help to improve their ability to identify, manage and recover debt owed to them.

86. A debt is owed to a public authority for the purposes of the Digital Economy Act 2017 if (a) a person is required to pay a sum of money to a public authority or to the Crown, and (b) all or part of that sum remains unpaid after the date on which (or after the end of the period within which) it is required to be paid. Taking action in context of this power includes: identifying and collecting debt, bringing civil proceedings, and taking administrative action as a result of that debt.

87. Fairness is a key consideration in the exercise of the power. All users of the power will be required to consider fairness in their debt information sharing arrangements. The applicable Fairness Principles are set out in Part 3.4 below.

88. These permissive powers are intended to ease the burden of establishing individual gateways and remove the need to seek new legislation to ensure public authorities have the required legal powers where they wish to share data. It is important to note that the powers are intended to be operated initially through pilots, established to explore the benefit of the data share.

89. Steps have to be taken to ensure that information sharing proposals are

balanced and proportionate and come under an appropriate level of scrutiny, similar to that which would be applied to the development of a new legal gateway.

# 3.2 Using the debt power

## The debt power

90. In order to lawfully use the debt power, you must identify a debt owed to a public authority or to the Crown, and any public authority who wishes to share information to take action against that debt must be listed as a "specified person" in Schedule 7. Furthermore, any additional bodies who may be involved in the proposed information share must also be listed in Schedule 7 in order to disclose or receive information under this power. Any information sharing must also comply with the requirements of the Digital Economy Act 2017 and the data protection legislation, and you should consider the Fairness Principles set out in Part 3.4.

An illustrative example of an appropriate use of the debt power:

- Customer A owes a debt to Public Authority A. Public Authority A is unable to collect this debt after Customer A fails to notify it of a change of address. Public Authority B collects address information in the course of its operations. Public Authority A would like to share information with Public Authority B for the purposes of taking action to recover the debt owed to it.

- Public Authority A considers the debt powers and assesses that the purpose of the proposed information share meets these requirements. Both public authorities are listed as specified persons in Schedule 7.

- Public Authority A has a lawful basis to share data. As the powers are permissive, Public Authority A will still need to agree with Public Authority B to share information for this purpose and draw up an appropriate information sharing agreement.

91. Specified persons exercising this information sharing power must ensure that all of the relevant conditions are met, that they are listed on Schedule 7, and that the information sharing is a lawful exercise of this power. Where a specified person is a person providing services to a public authority, any disclosure under

the debt power is limited to functions that person exercises for that public authority.

92. If a public authority wishes to use the debt power but is not in Schedule 7, it may be added through regulations — provided it meets the conditions in section 48(6) to (8).[25] Applications to amend the Schedules should be made through the secretariats for the relevant review board (as set out in sections 2, 3 and 4 of this Code).

93. Personal information shared under section 48 can only be used for the purpose for which it was disclosed, unless one of the limited exceptions in section 49(1) applies. For example, information received under section 48 may be disclosed further if it is to be used for protecting vulnerable adults or children. These exceptions do not apply to information disclosed by Her Majesty's Revenue and Customs unless the Commissioners for Her Majesty's Revenue and Customs have provided consent.

## Pilots and review board

94. The policy is that all information sharing proposals under the debt powers should be piloted to determine whether there is value in sharing personal information for the purposes set out in the relevant parts of the Digital Economy Act 2017, namely to take action in connection with debt owed to the public sector.

95. A review board will be established by the UK Government to oversee any non-devolved and England-only information sharing under the debt powers, and to monitor the pilots. This will help ensure bodies carrying out pilot data shares under these provisions operate having had regard to the Code. It will support any decision made on the basis of the outcome of the pilots, such as implementing the data share on a wider scale, and will gather and analyse evidence on the effectiveness of pilots to assist the review of the power after three years.

96. The review board will also consider issues about the use of the power and act as a point of contact with the ICO. All proposals for pilots should be submitted to the review board through its secretariat. It is envisaged that the review board will sit monthly and that requests and clearance through the

[25] These conditions are: (a) the body must be a public authority or a person providing services to a public authority; (b) the body must require information from a public authority (or person providing services to a public authority) to improve its ability to identify, manage or recover debt owed to a public authority or the Crown, or hold information that, if shared, would improve a public authority or person providing services to a public authority's ability to do so. Alternatively to (b), the body must have functions relating to the recovery or management of such debt, the exercise of which may be improved by the disclosure of information to or by that body.

Minister should take around six weeks once an application has been submitted.

97. The review board will consist of appropriately qualified subject experts gathered from across government and will be attended by representatives from the ICO and invited members from appropriate public representative bodies. The secretariat will monitor and record the progress of pilots, and will gather performance data for the evaluation of pilots and the power itself.

98. If you wish to establish a pilot you will need to submit a business case and privacy impact assessment (data protection impact assessment) to the secretariat of the review board. A single business case will need to be submitted which is agreed by all the participating bodies.

99. On receipt of a given business case, the secretariat will assess the business case, and will confirm with you whether it is suitable for submission to the review board and will let you know the date by which the business case will be considered by the review board.

100. The review board will review the business case and consider whether the proposal meets the requirements to use the power. It will make recommendations to the Minister for the Cabinet Office on whether the request should be accepted for implementation, accepted subject to amendments, or declined. You will be informed of the outcome by the secretariat.

101. Business cases may be declined for a range of reasons: for example the proposal may require modification to align it to best practice (including the Fairness Principles in Part 3.4); to more clearly define success criteria and the methodology for measuring them; or because alternative delivery routes may be more appropriate. Pilots can only commence under this power upon confirmation from the Minister that the recommendation has been approved.

102. During the operation of the pilot, you are responsible for:
- adherence to the terms of the pilot;
- reporting on the performance of the pilot;
- reporting of any variation in the pilot as a request to the review board;
- reporting of any breach of the code; and
- closure of the pilot and final reporting.

103. After the pilot has concluded, and if it is considered to have been a success, you can put a recommendation to the review board to act upon the findings of the pilot. The review board may, at this point, approve the continuation of the pilot as “business as usual” or recommend further piloting activity.

104. The review board is responsible for collating the evidence which will inform

the Minister's review of the operation of the debt power, as required under the Digital Economy Act 2017 after three years. This evidence will be gathered from the non-devolved and England-only information sharing arrangements as well as those implemented in the devolved administrations.

105. The devolved administrations will establish their own governance structures for oversight of information sharing arrangements within their areas. Data pertaining to the operation of pilots in the devolved administrations should be periodically submitted to the secretariat for the review board for the purpose of collating the evidence for the review of the debt power after three years.

# 3.3 Process for using the debt power

## Step 1: Identify the policy objective and the data needed to support it

- Do you need to use personal information?
  - Familiarise yourself with the data protection legislation,[26] the Data Protection Principles and the ICO's data sharing code
- Does the proposal pose any ethical issue or will it lead to any handling risks?
  - Refer to the Data Science Ethical Framework.
- Can the information sharing be piloted and what would be the method for measuring success/failure?
  - Contact the relevant central review board for your national territory for advice;
  - Discuss with your analysts what would be suitable measures to evaluate the particular information sharing arrangement.
- How do you want to share information and will it be secure?
  - Assess the data you need to share and ensure you can justify why you need each data field. Build in data protection by design and default, as required by the data protection legislation;
  - Speak to your organisation's information governance and

[26] In this Code, "the data protection legislation" means the full, applicable data protection framework as set out in the Data Protection Act 2018. This encompasses general processing (including the General Data Protection Regulation and the applied GDPR), law enforcement processing, and intelligence services processing. References to the Data Protection Act 1998 in the Digital Economy Act 2017 will be amended to "the data protection legislation" by the Data Protection Act 2018.

security experts and discuss what the best available methods are for data transfer.

## Step 2: Develop the proposal

- Agree a proposal with the other organisations involved in the data pilot
    - If bodies outside the public sector are involved (i.e. a person providing services to a specified person who is a public authority) you should consider any conflicts of interest (see Annex A) and reflect this in the business case;
    - Ensure all bodies undertake to comply with this Code of Practice;
    - Agree success/failure criteria for the pilot;
    - Seek advice from your legal advisers that your proposal is suitable for use under the debt power and is compliant with the data protection legislation or applicable investigatory powers legislation;
    - Consider how the Fairness Principles can be embedded into the proposal.
- Conduct a privacy impact assessment (data protection impact assessment):
    - Assess the potential benefits against the risks or potential negative effects, such as an erosion of personal privacy and review this assessment at critical milestones.
- Develop and draft a business case, information sharing agreements, a privacy impact assessment and security plan:
    - Ensure you have regard to ICO guidance on Data Sharing Agreements and privacy impact assessments review this assessment at critical milestones;
    - Ensure the responsibilities of each body involved in the information sharing arrangement are understood and articulated in the documentation;
    - The outcomes of any public consultation or decision as to why a public consultation did not take place should be articulated in the business case;
    - Ensure each organisation involved in the information sharing arrangement has the appropriate systems and procedures in place to handle data securely and that a security plan has been agreed which sets out how data security will be managed.

## Step 3: Submitting the proposal

- Submit your proposal to the relevant central review board for your

territory:
    - Contact your central review board and submit the relevant documentation to them;
    - You may receive an initial view from the central review board with any recommendations they may have for strengthening the proposal, which you should respond to accordingly to enable the proposal to progress;
    - The central review board will contact you to let you know whether a) your proposal will be recommended to the relevant Minister; b) whether modifications are recommended; or c) the proposal has not met requirements and an alternative approach should be pursued;
    - Your central review board will contact you to let you know whether the Minister is content for the pilot to proceed and the updates that will be required so that they can monitor progress.

## Step 4: Running the pilot

- Managing the pilot:
    - Upon receiving confirmation that the pilot may proceed, you should ensure there is an appropriate governance structure in place for the pilot;
    - You should ensure that all bodies taking part in the relevant arrangement adhere to the information sharing agreement and report any breaches as appropriate to the central review board for your territory. Serious data security breaches should be reported to your central review board and in accordance with the requirements of the data protection legislation (including to the ICO if required).
- Reporting to the central review board in England:
    - Send appropriate metrics data about your pilot through at agreed intervals to the secretariat to the review board;
    - The secretariat will publish relevant information about the pilot online and update with metrics as appropriate;
    - At the end of the pilot period send a summary of the findings, and other relevant information to the review board.
- Assessment of the pilot:
    - The central review board for your territory will analyse the metrics and findings of the pilot and make a recommendation to the relevant Minister as to whether it has met its objectives and whether the data sharing should continue on a “business as usual” basis or not. The review board will contact you to inform you of the Minister’s decision;
    - If the decision is to stop the pilot, you must ensure that steps

are taken to destroy any data acquired under the power which do not need to be retained.

106. In considering whether to use the debt power, the following checklist may also be helpful:

**Checklist: points to consider**

Why share

- For what purpose and public function is the information being requested?
- What are the benefits of the data exchange for the receiving party or any other public body?
- What are the implications of not sharing information? For example:
    - increased risk that people do not receive the support or the services they require in a timely manner
    - risk that burdens will be placed on people to repeatedly supply information to access the services they require
    - risk of wasting taxpayers' money by jeopardising public finances or commercial projects

What to share

- What specific data items are required and why?
- Are there reasons why the data should not be shared (consider the Data Protection Principles and any legal restrictions that may apply)?
- Are there any legal obligations on the recipient of the data to provide it to any other bodies?
- How regularly and in what volume is it proposed to share the data?
- Are there any ethical issues with the proposed information sharing arrangement?

How to share

- What methods or technology can be used to minimise the amount of information shared and risk of data loss, for example using

aggregate data, derived data or the use of a lookup process, in preference to sharing large amounts of data;

- What procedures will be in place to correct any inaccurate data identified during the data sharing process and the process for capturing the changes made for auditing purposes?
- What are the conditions for processing information: will data subjects be aware that their data is being processed and will procedures for dealing with access requests, queries and complaints be in place? How will information be provided to data subjects, in accordance with the requirements of the data protection legislation?
- Information handling responsibilities, including details of any data processors, contractors or subcontractors;
- Security considerations, like the use of secure transfer mechanisms, encryption, etc;
- For audit purposes document the process and methods of exchange, how exchanges are logged, what information is stored and who has access to it;
- Standards and levels of expected operational service
- Termination arrangements;
- Minimising cost of providing/transferring the data;
- Issues, disputes and resolution procedures;
- Sanctions for failure to comply with the agreement or breaches by individual staff;
- Is there a time limit suggested for using the data and, if so, how will the data be deleted?
- Periodic reviews of effectiveness and necessity of data sharing arrangement.

# 3.4 The Fairness Principles for data sharing under the debt power

107. Fairness is a key consideration in respect of the operation of the debt data sharing power. Public authorities will continue to have their own fairness policies and practice in how they manage debt. These Fairness Principles provide a set of best practice guidelines to help ensure a common approach to fairness is considered when sharing information under the power. These Principles aim to align with existing public authority practices, and aim to encourage a consistent approach to fairness across the debt data sharing pilots. The Principles only apply to debt data sharing pilot activity to be carried out under the Digital Economy Act 2017, and only in accordance with any legal obligations to which public authorities are subject.

108. Pilots operating under the debt power should aim to use relevant data to help differentiate between:

- A customer who cannot pay their debt because of vulnerability or hardship - so that individuals can, for example, be offered advice and guidance about the debt owed (where appropriate), or be signposted to non-fee-paying debt advice and support, with the aim of minimising the build-up of further debt;
- A customer who is in a position to pay their debt - some of whom may need additional support; and
- A customer who has the means to pay their debt, but chooses not to pay - so public authorities, and private bodies acting on their behalf, can assess which interventions could best be used to recover the debt.

109. The use of wider data sharing for this purpose will help enhance cross-government debt management capability, and will help to enable a more informed view of a customer's individual circumstances and their ability to pay.

110. Pilots should be conscious of the impact debt collection practices have on vulnerable customers and customers in hardship. Statistical and anecdotal evidence from debt advice agencies shows that in a substantial amount of cases, a non-fee-paying customer who has an outstanding debt will owe money to more than one creditor. The aim is to ensure any repayment plans are affordable and sustainable. This should balance the need to maximise collections, while taking affordability into account. This may be achieved by:

- Using relevant sources of data and information to make informed decisions about a customer's individual circumstances and their ability to pay. This process could include:
    - An assessment of income versus expenditure to create a tailored and

    - affordable repayment plan based on in work and out of work considerations, including the ability to take irregular income into account;
    - Consideration of the need for a 'breathing space' to seek advice, or forbearance, in cases of vulnerability and hardship.
- Where a vulnerable customer is identified, they should be given appropriate advice and support, which may include signposting to non-fee-paying debt advice agencies;
- Government should liaise with non-fee-paying debt advice agencies who are helping customers in debt;
- Communication should clearly set out relevant information to enable the customer to take action, and encourage them to engage with the government;
- Any third party participating in a pilot (such as a Debt Collection Agency or Shared Services) must also treat people fairly, in line with these Principles and relevant regulatory rules;
- Pilots should undertake regular engagement with stakeholders to encourage regular feedback about how fairly the pilots are working in practice.

# Part 4. Fraud

111. This part of the Code is for organisations wishing to make use of the fraud power in Chapter 4 of Part 5 of the Digital Economy Act 2017. It sets out the purpose of the fraud provisions and guidance on the process you will need to follow to establish a new pilot.

# 4.1 Understanding the purpose of the fraud power

## Purpose of the fraud power

112. It is estimated that losses to Government through fraud are in the region of £31bn to £49bn per annum. It is in all our interests to prevent fraud, and public bodies have a particular responsibility to ensure that taxpayers' money is spent appropriately and is not taken out of the system fraudulently.

113. The fraud power in section 56 of the Digital Economy Act 2017 creates a permissive gateway that enables information to be shared between specified persons (bodies listed in Schedule 8) in order to share information to take action in connection with fraud against a public authority. Information sharing between public authorities will help to improve their ability to identify and reduce the risk of fraud against the public sector and recover public sector funds.

114. Fraud against a public authority for the purposes of the Digital Economy Act 2017 means a fraud offence which involves (a) loss to a public authority, or (b) the exposure of a public authority to a risk of loss. Taking action in the context of this power includes: preventing, detecting, investigating and prosecuting fraud, bringing civil proceedings, and taking administrative action as a result of fraud.

115. These permissive powers are intended to ease the burden of establishing individual gateways and remove the need to seek new legislation to ensure public authorities have the required legal powers where they may wish to share data. It is important to note that the powers are designed to be operated initially through pilots, established to explore the benefit of the information share.

116. Steps have to be taken to ensure that information sharing proposals are balanced and proportionate and come under an appropriate level of scrutiny, similar to that which would be applied to the development of a new legal gateway.

# 4.2. Using the fraud power

## The fraud power

117. In order to lawfully use the fraud power, you must identify a fraud offence against a public authority, and any public authority who wishes to disclose information to take action against that fraud offence must be listed as a "specified person" in Schedule 8. Furthermore, any additional bodies who may be involved in the proposed information share must also be listed in Schedule 8 in order to disclose or receive information under this power. Any information sharing must also comply with the requirements of the Digital Economy Act 2017 and the data protection legislation.

An illustrative example of an appropriate use of the fraud power:

- Public Authority A has identified a risk of loss in discretionary financial awards where Customer A has not reported all relevant personal circumstances. Public Authority B collects information about customers' personal circumstances in the the course of its operations. Public Authority A would like to share information with Public Authority B for the purposes of taking action against the risk of loss.

- Public Authority A considers the fraud powers and assesses that the purpose of the proposed information share meets these requirements. Both public authorities are listed as specified persons in Schedule 8.

- Public Authority A has a lawful basis to share data. As the powers are permissive, Public Authority A will still need agree with Public Authority B to share information for this purpose and draw up an appropriate information sharing agreement.

118. Specified persons exercising this information sharing power must ensure that the relevant conditions are met, that they are listed in Schedule 8, and that the proposed information sharing is a lawful exercise of this power. Where a specified person is a person providing services to a public authority, any disclosure under the fraud power is limited to the functions that person exercises for that public authority.

119. If a public authority wishes to use the fraud power but is not listed in Schedule 8, it may be added through regulations — provided it meets the

conditions in section 56(7) to (9).[27] Applications to amend the Schedules should be made through the secretariats for the relevant review board (as set out in sections 2, 3 and 4 of this Code).

120. Personal information shared under section 56 can only be used for the purpose for which it was disclosed, unless one of the limited exceptions in section 57(1) applies. For example, information received under section 48 may be disclosed further if it is to be used for protecting vulnerable adults or children. The exceptions do not apply to information disclosed by Her Majesty's Revenue and Customs unless the Commissioners for Her Majesty's Revenue and Customs have provided consent.

## Pilots and review board

121. The policy is that all information sharing proposals under the fraud power are piloted to determine whether and how there is value in sharing personal information for the purposes set out in the relevant parts of the Digital Economy Act 2017, namely to take action in connection with fraud against the public sector.

122. A review board will be established by the UK government to oversee any non-devolved and England-only data sharing under the fraud powers, and to monitor the pilots. This will help ensure bodies carrying out pilot data shares under these provisions operate with regard to the Code. It will support any decision made on the basis of the outcome of the pilots, such as implementing the data share on a wider scale, and gather and analyse evidence on the effectiveness of pilots to assist the review of the power after three years.

123. The review board will also consider issues about the use of the power and act as a point of contact with the ICO. All proposals for pilots should be submitted to the review board through the secretariat. It is envisaged that the review board will sit monthly and that requests and clearance through the Minister should take around six weeks once an application has been submitted.

124. The review board will consist of appropriately qualified subject experts gathered from across government and will be attended by representatives from the ICO and invited members from appropriate public representative bodies. The secretariat will monitor and record the progress of pilots, and will gather

[27] These conditions are: (a) the body must be a public authority or a person providing services to a public authority; (b) that body must require information from a public authority (or person providing services to a public authority) to improve its ability to identify or reduce fraud against it or a public authority to which it provides services, or holds information that would assist other public authorities to do so. Alternatively to (b), the body must have functions of taking action in connection with fraud against a public authority, which would be improved by it disclosing or receiving information.

performance data for the evaluation of the pilot and the power itself.

125. If you wish to establish a pilot the policy requirement is for you to submit a business case and privacy impact assessment (data protection impact assessment) to the secretariat of the review board. A single business case will need to be submitted which is agreed by all the participating bodies.

126. On receipt of a given business case, the secretariat will assess the business case, and will confirm with you whether it is suitable for submission to the review board and will let you know the date by which the business case will be considered by the review board.

127. The review board will review the business case and consider whether the proposal meets the requirements to use the power. It will make recommendations to the Minister for the Cabinet Office on whether the request should accepted for implementation; accepted subject to amendments; or declined. You will be informed of the outcome by the secretariat.

128. Business cases may be declined for a range of reasons, for example the proposal may require modification to align it to best practice, to more clearly define success criteria and the methodology for measuring them, or because alternative delivery routes may be more appropriate. Pilots can only commence under this power upon confirmation from the Minister that the recommendation has been approved.

129. During the operation of the pilot, you are responsible for:
- Adherence to the terms of the pilot;
- Reporting on the performance of the pilot;
- Reporting of any variation in the pilot as a request to the review board;
- Reporting of any breach of the code; and
- Closure of the pilot and final reporting.

130. After the pilot has concluded, and if it is considered to have been a success, you can put a recommendation to the review board to act upon the findings of the pilot. The review board may, at this point, approve the continuation of the pilot as “business as usual” or recommend further piloting activity.

131. The review board is responsible for collating the evidence which will inform the Minister’s review of the operation of the fraud power, as required under the Digital Economy Act 2017 after three years. This evidence will be gathered from the non-devolved and England-only data sharing arrangements as well as those implemented in the devolved administrations.

132. The devolved administrations will establish their own governance structures for oversight of information sharing arrangements within their areas. Data

pertaining to the operation of pilots in the devolved administrations should be periodically submitted to the secretariat for the review board for the purpose of collating the evidence for the review of the debt and fraud power after three years.

# 4.3 Process for using the fraud power

## Step 1: Identify the policy objective and the data needed to support it

- Do you need to use personal information?
  - Familiarise yourself with the data protection legislation,[28] the Data Protection Principles and the ICO data sharing code.
- Does the proposal pose any ethical issue or will it lead to any handling risks?
  - Refer to the Data Science Ethical Framework
- Can the information share be piloted and what would the method for measuring success/failure?
  - Contact the relevant central review board for your national territory for advice;
  - Discuss with your analysts what would be suitable measures to evaluate the particular information sharing arrangement.
- How do you want to share information and will it be secure?
  - Assess the data you need to share and ensure you can justify why you need each data field. Build in data protection by design and default, as required by the data protection legislation. Speak to your organisation's information governance and security experts and discuss what the best available methods are for data transfer.

## Step 2: Develop the proposal

- Agree a proposal with the other organisations involved in the data pilot:
  - If bodies outside the public sector are involved (i.e. a person providing services to a specified person who is a public authority) you should consider any conflicts of interest (see

[28] In this Code, "the data protection legislation" means the full, applicable data protection framework as set out in the Data Protection Act 2018. This encompasses general processing (including the General Data Protection Regulation and the applied GDPR), law enforcement processing, and intelligence services processing. References to the Data Protection Act 1998 in the Digital Economy Act 2017 will be amended to "the data protection legislation" by the Data Protection Act 2018.

Annex A) and reflect this in the business case;
    - Ensure all bodies undertake to comply with this Code of Practice;
    - Agree success/failure criteria for the pilot;
    - Seek advice from your legal advisers that your proposal is suitable for use under the relevant power (fraud or debt) and is compliant with the data protection legislation or applicable investigatory powers legislation.
- Conduct a privacy impact assessment (data protection impact assessment):
    - Assess the potential benefits against the risks or potential negative effects, such as an erosion of personal privacy.
- Develop and draft a business case, information sharing agreements, a privacy impact assessment and security plan.
    - Ensure you have regard to ICO guidance on Data Sharing Agreements and privacy impact assessments and review this assessment at critical milestones;
    - Ensure the responsibilities of each body involved in the information sharing arrangement are understood and articulated in the documentation;
    - The outcomes of any public consultation or decision as to why a public consultation did not take place should be articulated in the business case;
    - Ensure each organisation involved in the information sharing arrangement has the appropriate systems and procedures in place to handle data securely and that a security plan has been agreed which sets out how data security will be managed.

## Step 3: Submitting the proposal

- Submit your proposal to the relevant central review board for your territory:
    - Contact your central review board and submit the relevant documentation to them;
    - You may receive an initial view from the central review board with any recommendations they have for strengthening the proposal, which you should respond to accordingly to enable the proposal to progress;
    - The central review board will contact you to let you know whether a) your proposal will be recommended to the relevant Minister; b) whether modifications are recommended; or c) the proposal has not met requirements and an alternative approach should be pursued;
    - Your central review board will contact you to let you know

whether the Minister is content for the pilot to proceed and the updates that will be required so that they can monitor progress.

## Step 4: Running the pilot

- Managing the pilot:
  - Upon receiving confirmation that the pilot may proceed, you should ensure there is an appropriate governance structure in place for the pilot;
  - You should ensure that all bodies taking part in the relevant arrangement adhere to the information sharing agreement and report any breaches as appropriate to the central review board for your territory. Serious data security breaches should be reported to your central review board and in accordance with the requirements of the data protection legislation (including to the ICO if required).
- Reporting to the central review board in England:
  - Send appropriate metrics data about your pilot through at agreed intervals to the secretariat to the review board;
  - The secretariat will publish relevant information about the pilot online and update with metrics as appropriate;
  - At the end of the pilot period send a summary of the findings, and other relevant information to the review board.
- Assessment of the Pilot:
  - The central review board for your territory will analyse the metrics and findings of the pilot and make a recommendation to the relevant Minister as to whether it has met its objectives and whether the information sharing should proceed or not. The review board will contact you to inform you of the Minister's decision;
  - If the decision is to stop the pilot, you must ensure that steps are taken to destroy any copies of data acquired under the power which do not need to be retained.

133. In considering whether to use the fraud power, the following checklist may also be helpful:

**Checklist: points to consider**

Why share

- For what purpose and public function is the information being requested?

- What are the benefits of the data exchange for the receiving party or any other public body?
- What are the implications of not sharing information? For example:
    - risk of wasting taxpayers' money by jeopardising public finances or commercial projects

What to share

- What specific data items are required and why?
- Are there reasons why the data should not be shared (consider the Data Protection Principles and any legal restrictions that may apply)?
- Are there any legal obligations on the recipient of the data to provide it to any other bodies?
- How regularly and in what volume is it proposed to share the data?
- Are there any ethical issues with the proposed data sharing arrangement?

How to share

- What methods or technology can be used to minimise the amount of information shared and risk of data loss for example using aggregate data, derived data or the use of a lookup process, in preference to sharing large amounts of data;
- What procedures will be in place to correct any inaccurate data identified during the data sharing process and the process for capturing the changes made for auditing purposes?
- What are the conditions for processing information: will data subjects be aware that their data is being processed and will procedures for dealing with access requests, queries and complaints be in place? How will information be provided to data subjects, in accordance with the requirements of the data protection legislation?
- Information handling responsibilities, including details of any data processors, contractors or subcontractors;
- Security considerations, like the use of secure transfer mechanisms, encryption, etc;
- For audit purposes document the process and methods of exchange, how exchanges are logged, what information is stored and who has access to it;

- Standards and levels of expected operational service;
- Termination arrangements;
- Minimising cost of providing/transferring the data;
- Issues, disputes and resolution procedures;
- Sanctions for failure to comply with the agreement or breaches by individual staff;
- Is there a time-limit suggested for using the data and if so how will the data be deleted?
- Periodic reviews of effectiveness and necessity of information sharing arrangement.

# Part 5 - Fairness and transparency

134. When using the powers for public service delivery, fraud and debt, you are required to ensure that your information sharing practices are fair and transparent. You should only share information once you are satisfied that the processes are fair and transparent. This is necessary to comply with the "lawfulness, fairness and transparency" principle in the data protection legislation.[29] The "accountability" principle in the data protection legislation makes controllers responsible for demonstrating that the "lawfulness, fairness and transparency" principle, together with the other principles in the data protection legislation, have been complied with.

135. The data protection legislation may provide for an exemption from transparency requirements, for instance, on grounds of national security or defence sensitivities. This may be supported by a ministerial certificate. Where appropriate, it may be helpful simply to indicate to the relevant authority that information has been redacted on the basis that it is subject to a ministerial certificate issued in accordance with the data protection legislation.

136. This part of the Code sets out a number of specific obligations for reporting information sharing activities under these powers (building on or in addition to the requirements in the data protection legislation) and the documents you will need to prepare and make available.

## 5.1 Register of information sharing activity

137. Information about all information sharing agreements concerning England-only or non-devolved bodies for a disclosure or group of disclosures under the public service delivery, debt and fraud powers must be submitted to the Public Service Delivery secretariat in DCMS for public service delivery, or the Fraud and Debt secretariat in the in the Cabinet Office for debt and fraud. The secretariat in DCMS will maintain searchable electronic registers available to the general public.

138. It is important that citizens can understand what data is being shared, the specific purposes for which it is being shared, which bodies are disclosing and

[29] Please note that the 'transparency' requirement does not apply to data processing to which Part 3 of the Data Protection Act 2018 applies.

receiving that data, the potential benefits to be derived from the data sharing, and where appropriate how long that data will be held for. Furthermore, under the data protection legislation, controllers are required to keep records of their data processing activities.

139. The register will allow government, the ICO and the public to understand what information sharing is taking place under the provisions to assess the value of the provisions. This information could be used to run audits where appropriate to check compliance with legislation and the use of this Code and other security and data processing guidelines.

140. Responsibility for submitting the required information about an information sharing agreement for a disclosure or group of disclosures rests with the controller, or in the case of the fraud and debt provisions, with the secretariat. Where an agreement establishes several disclosures over a period of time such as a data feed, a single entry is sufficient. If there is more than one controller, they should work together to provide information for a single entry in the register.

141. The information to be submitted for inclusion in the register is as follows:

- Title of the information sharing agreement;
- Short description of the purpose of the information sharing agreement;
- Which chapter under Part 5 of the Digital Economy Act 2017 the information is being shared under (and the specific objective where the public service delivery provisions are used);
- Description of the information being disclosed and by which body (including bodies outside the public sector);
- Method by which data will be disclosed;
- Bodies receiving the data (including bodies outside the public sector);
- How long the information will be held;
- When the data sharing agreement will come into effect and when it will end;
- Anticipated benefits of the data sharing;
- Contact details for any subject access requests (for Public Service Delivery and debt).

142. Providing this information should not be burdensome as it will already have to be collated as part of the process of developing the business case and information sharing agreement as well as for the controller's records of its processing activities. Information should be submitted for inclusion in the register as early as possible before the data sharing comes into effect. There is a presumption that information sharing arrangements - whether preparing to go live, live, or closed - will be included on the register and available for citizens to scrutinise.

143. There may be instances where publication of information about an

information sharing agreement may in itself risk the objectives of the data share, such as where it pertains to national security, counter-fraud or criminal investigations. In such instances an entry should still be submitted to GDS and a description agreed for publication and audit purposes.

144. Documents may be redacted where appropriate to protect material which it would not be in the public interest to publish - for example where publication would damage national security. Such redactions will be the exception and will need to be justified. It is the responsibility of the authority or authorities who submit information to DCMS (for public service delivery) or the Cabinet Office (for debt and fraud) to redact material before they submit it and to mark clearly where redactions have been made. Where you are asking for material to be published with redactions, you should provide the DCMS (for public service delivery) or the Cabinet Office (for debt and fraud) with a separate list of the material that you propose for redaction and, in each case, an explanation of why you consider that redaction to be justified. This is subject to the need to protect this information appropriately.

# 5.2 Other documentation

145. If you are looking to share information under any of the public service delivery, debt or fraud powers you need to carefully consider why an information sharing arrangement should be established and maintain a full audit trail of decisions. Conducting a privacy impact assessment (data protection impact assessment) of the proposal should be one of the first steps you take. It will help you assess the potential benefits against the risks or potential negative effects, such as an erosion of personal privacy. It will also provide a platform for considering how to design the information sharing to help ensure the minimum amount of information is shared to achieve the desired objective. See below for further guidance on privacy impact assessments.

146. You should always seek to operate as transparently as possible. Business cases, information sharing agreements and privacy impact assessment reports should be published in line with ICO guidelines. You may wish to redact some sensitive information from these documents before making them available. You should keep a record of redactions in each case and the reasons for making them. For example, in a privacy impact assessment or business case for a fraud or debt pilot, if you consider that placing certain information about the pilot in the public domain could undermine the objectives of the information sharing arrangement, you should redact that information. You should include a high level summary of the security plan in the business case unless there are particular national security or other sensitivities which would outweigh public interest in disclosure, but you do not need to publish the full plan.

## Business cases

147. If you wish to establish an information sharing arrangement under the public service delivery, debt or fraud powers you must develop and agree a business case with the other bodies participating in the data share. A single business case will need to be developed for each information sharing arrangement. An information sharing arrangement could cover multiple transactions, and may cover the exploration of the benefit of sharing a single data asset, through to the trialling of a complete business process (for example under the debt and fraud powers).

148. Because all initial uses of the debt and fraud powers will be run as pilots, the initial purpose of the business case for debt and fraud arrangements is to justify the pilot by clarifying its objectives, how the pilot will be measured and the processes to ensure that data is being protected and used appropriately.

149. Your business case should contain the following information.

**An outline of the information share**. This should include:

- the objective of the information sharing arrangement;
- an overview of the activity under the arrangement (and how the data will be used);
- the period of duration for the arrangement, when the data share will be live and how retention periods will be managed; and
- an outline of what types of data will be shared and the data security arrangements to be put in place.

**Persons included in the information share**. This should include:

- a list of all persons and bodies that will be involved in the share – specifying which would disclose or receive data:
    - to note - a business case provided under the fraud power need not go as far as detailing the counter fraud operation of partners.

**How the benefits of the information share will be measured**. This should include:

- the potential benefits the information share could bring;
- the success criteria for the data share and the methodology you will use to measure success.

**A statement of adherence to the Code of Practice:**

- for a debt data share, you should also include a statement explaining how you will comply with the Fairness Principles (in Part 3.4).

## Privacy impact assessments and Privacy Notices

150. A privacy impact assessment (data protection impact assessment) is a process which helps identify and reduce the privacy risks of an information share. You must conduct a privacy impact assessment if you wish to share data under the public service delivery, debt and fraud powers. The ICO's Conducting Privacy Impact Assessments Code of Practice[30] provides guidance on a range of issues in respect of these assessments, including the benefits of conducting privacy impact assessments and practical guidance on the process required to carry one out. The privacy impact assessment should be reviewed at critical milestones and updated where necessary (for example when a pilot under the debt or fraud power has demonstrated benefit and is to be upscaled). The data protection legislation now requires "data protection impact assessments" to be conducted prior to the processing when the processing is likely to result in a high risk to the rights and freedoms of individuals.

151. A Privacy Notice is either provided directly to individuals or otherwise made easily accessible. It explains, among other matters, what you do with their personal information, which bodies are involved and so forth. In exercising these powers to share data, you must ensure that suitably worded privacy notices are published and made available to the public in line with the fairness and transparency principles in the ICO's Privacy notices, transparency and control code of practice[31] (which provides guidance on the contents of these notices, as well as where and when to make them publicly available) and the ICO data sharing code. The data protection legislation now requires privacy notices to contain more detailed and specific information than under the Data Protection Act 1998.[32]

152. The Digital Economy Act 2017 requires all persons who are involved in disclosing information under the public service delivery, debt and fraud powers to have regard to the codes issued by the Information Commissioner, in so far as they are relevant, when they disclose information under these powers.[33]

## Information Sharing Agreements

153. You should follow the ICO data sharing code with regard to information sharing agreements. Before entering into information sharing agreements, you will need to agree with the other organisations involved in the data share that they will take appropriate organisational, security and technical measures to:

[30] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[31] https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf
[32] See, for example, Articles 12, 13 and 14 of the General Data Protection Regulation.
[33] See sections 43(13), 52(13) and 60(13) respectively.

- ensure information will be retained securely and deleted once it has been used for the purpose for which it was provided;
- keep information accurate and up to date, and provide for its rectification or erasure where appropriate;
- prevent accidental loss, destruction or damage of information;
- ensure only people with a genuine business need have access to the information.

154. Information sharing agreements should contain details of sanctions that will apply to recipients of information who are found to be unlawfully or inappropriately processing data. These sanctions will include, but are not limited to:

- Public authorities ceasing to receive information from other public authorities under the relevant power in the Digital Economy Act 2017. Regulations may be made to remove the organisation from the list of bodies able to share information under the power;
- Public authorities considering whether a given incident and/or organisation needs to be reported to the ICO;
- Public authority officials determining whether any misuse of public office offences have been committed, and if so, to take any necessary action;
- Persons granted access to information following a previous data breach will be required to have their systems and procedures assessed by a sponsoring public authority. Such persons will only be able to participate in an information sharing arrangement once public authority officials are satisfied that any security or other issues have been resolved to reduce the risk of any further issues occurring again in the future. The data sharing agreement should capture details of the assessments and the steps that have been taken to address previous problems.

# 6. Governance

## 6.1 Implementing a data sharing arrangement

155. Information sharing under these powers must adhere to the ICO data sharing code and other existing guidelines on data security, and the requirements of the data protection legislation. You must respond swiftly and effectively to any complaints, objections or requests under the right of access to personal information. You should periodically run checks to ensure data security best practice is adhered to and publish details online of what checks were carried out and when.

156. Where data quality issues are identified during an information sharing arrangement, the governance structure supporting the arrangement should provide for immediate steps to be taken to identify and manage the risks associated with the use of that data and any remedial action required.

157. The ICO has a general power to conduct audits (including compulsory audits of government departments, designated public authorities and other categories of designated persons) of organisations to check that they are complying with law in relation to the handling of personal information. All bodies are required to comply with the ICO's request for assistance so that they can determine whether data has been processed lawfully within the data sharing arrangement. The ICO is able to initiate criminal proceedings where necessary.

158. Anyone with concerns about a person's systems and procedures for handling data, including the ICO, may raise those concerns with the responsible Minister. The responsible minister is the Secretary of State or the Minister for the Cabinet Office for England-only and non-devolved information sharing initiatives and the relevant Minister or authority in the devolved administration for an information sharing arrangement within a devolved territory only. Serious or persistent failure to handle data securely may result in regulations being laid to exclude a person from participating in any data share under the power.

## 6.2 Compliance with the Code

159. Any serious security breaches or serious breaches of the data protection legislation need to be reported immediately to the Public Service Delivery review board (for activities under the public service delivery powers) and the Debt and Fraud review board (for fraud and debt pilots) and, where applicable, the governance group in your devolved territory. Any breaches should be reported in accordance with the requirements of the data protection legislation (including to

the ICO if required).

160. You should also report immediately any breaches of the Code or any sharing that contravenes the terms of the information sharing arrangement even if it may not constitute a serious breach of the data protection legislation to the relevant review board or point of contact for your territory.

161. For debt and fraud, the review board will inform the other public authorities participating in the pilot that a breach has been reported. The Board will work with the controller to understand the results of any investigation and to evaluate the implications for the future of the pilot. In doing so, it may make one of the following findings:

- There has not been a breach and no action is required;
- A breach has taken place but is of low impact: it will notify the public authority and ask it to report on remedial measures;
- A breach has taken place and is of such seriousness that the pilot must be stopped: in this case, it will notify the public authority of the finding and inform the Minister of its recommendation;
- A breach has taken place and is so serious that the public body must be removed from the Schedule. In such cases, it will notify the public authority of the finding and inform the Minister of its recommendation.

162. Where the Minister has been informed by the review board under the debt and fraud powers of a recommended course of action following a breach, the Minister will notify the public authority and the review board as to the course of action he wishes to pursue. The Minister may in addition notify the ICO. Authorities will be kept informed of decisions and where possible invited to make representations or comments.

163. You should address any general questions and concerns about the debt and fraud powers to the secretariat in the first instance.

# Annex A - conflicts of interest

## Definition

165. The National Audit Office defines a conflict of interest as:

> *"a set of circumstances that creates a risk that an individual's ability to apply judgement or act in one role is, or could be, impaired or influenced by a secondary interest. The perception of competing interests, impaired judgement or undue influence can also be a conflict of interest."*[34]

166. A conflict of interest may arise in respect of a company and/or an individual.

167. There are two types of conflicts of interest:

- actual conflict of interest — for example, a material conflict between one or more interests; and
- potential conflict of interest — for example, the possibility of a material conflict.

## How to manage a conflict of interest

168. There are a variety of ways to manage conflicts of interest and we do not propose that this Code provides an in-depth 'how to'. However, we think it would be helpful to include some key principles for identifying and managing conflicts of interest:

- Non-public authorities should ensure they have adequate systems in place to identify and assess conflicts of interest. The rules should be clear and robust, but not overly prescriptive. Staff should also be adequately trained to identify and assess conflicts of interest;
- This process could be assisted by a conflicts of interest policy — for example one that requires all employees to regularly declare their interests when entering into new agreements. An internal or industry-wide code of ethics may also apply, where employees are required to confirm compliance;
- Conflicts of interest (actual and potential) should be identified as early as possible to avoid later issues. Information about the conflict should be adequately recorded, including any information about steps taken to manage it and any decisions made on the severity of the conflict;
- The system for managing conflicts should be audited to ensure compliance.

[34] https://www.nao.org.uk/wp-content/uploads/2015/01/Conflicts-of-interest.pdf

169. The appendices to the National Audit Office guidance on conflicts of interest are helpful: https://www.nao.org.uk/wp-content/uploads/2015/01/Conflicts-of-interest.pdf