Contents

Part 1: About the Code of Practice

1. This Code explains how the permissive powers contained in Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill should be used for the sharing of information by officials within specified public authorities for specific purposes set out in the legislation or, where appropriate, accompanying regulations. It also makes reference to requirements under the wider UK legislative framework, where appropriate. In addition, it provides details of the procedures that need to be followed when considering the disclosure, receipt or use of information under the powers. This Code should be read alongside the Information Commissioner's data sharing code of practice ('the ICO Code') which provides guidance on how to ensure personal data is shared in a way that is lawful, proportionate and compatible with the Data Protection Act 1998 (DPA) and other relevant legislation such as the Human Rights Act 1998.

2. This Code defines 'data sharing' in the same terms as the ICO Code[1], namely the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. The ICO Code states 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; and
    - several organisations pooling information and making it available to each other.

3. The relevant chapters of Part 5 of the Digital Economy Bill (i.e. pertaining to public service delivery, debt and fraud) define personal information as information which relates to and identifies a particular person (or body corporate)[2]. For these purposes, information 'identifies' a particular person if the identity of that person is (a) specified in the information; (b) can be deduced from the information, or (c) can be deduced from the information taken together with any other available information. The Data Protection Act 1998 ('DPA') defines personal data rather than personal information. Personal data for the purposes of the DPA is defined as data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller. The definition for the purposes of the DPA also includes the expressions of opinions about an individual and the indication of intentions around that individual.

[1] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf
[2] the definition of personal information does not include information about the internal administrative arrangements of the specified body permitted to disclose or receive data under these permissive powers.

4. The definitions of ‘personal information’ contained in the Bill are intended to ensure that the information shared through these powers is handled carefully. Though the definition of ‘personal information’ for the purposes of the Bill may differ from the definition of ‘personal data’ in the DPA, all information shared and used under the public service delivery, debt and fraud provisions must be handled in accordance with the framework of rules set out in the DPA, and in particular with the Data Protection Principles. There are also specific safeguards introduced in the Bill to ensure personal information is handled appropriately.

5. The public service delivery, debt and fraud provisions are subject to the DPA, including the criminal offences in relation to the unlawful obtaining or disclosing of personal data set out at section 55. New criminal offences have also been created to prevent the unlawful disclosure of personal information. Individuals convicted under those offences could face a maximum penalty of up to two years in prison, an unlimited fine, or both. These maximum penalties mirror those applying to existing offences contained in legislation governing the use of data held by HMRC and DWP, and are designed to underline the Government’s commitment to protecting citizens’ data.

6. In the past data sharing has commonly involved bulk data transfers within and between public authorities. New technology and methods have had a significant impact on data sharing. Application Programming Interfaces (APIs) are standards that allow software components to interact and exchange data. APIs allow applications and their datasets to interact with each other across organisational and geographical boundaries. This allows public authorities to identify or verify eligibility for services and other objectives for which data needs to be shared through less intrusive methods, such as running binary checks against one or more datasets. Though the method is generally safer (large amounts of data are not being transferred either physically or electronically and, in instances when eligibility is being checked, the need to share underlying data is removed completely) and less intrusive (binary checks can be run against very specific relevant data fields) information is still being shared and as such those sharing data in these ways require the legal powers, to do so.

7. In light of the fact that we are in transition between old and new approaches to data sharing, the legislation is intended to support the range of different approaches to data sharing and as such does not specify the use of a particular technology or a specific approach to be used in terms of the practicalities of transfer. Furthermore, we recognise the need to allow the opportunity to keep apace of and adopt better technologies and more efficient or effective approaches as they emerge.

8. The Government Digital Service (GDS), which is a team within the Cabinet Office leading the digital transformation of government, continues to work on how best to transition public authorities from outmoded legacy systems to the technologies required for a modern public sector. Future revisions to the Code

may reference or include guidance and best practice in relation to technical processes.

9. This Code does not provide guidance on individual organisations and their obligations on data sharing or data handling. Instead, in making use of these powers, you will need to satisfy yourself that you are complying with the DPA. It is advisable for those making use of the powers to seek your own legal advice regarding data sharing following any agreements to share information.

The Code's status

[This is indicative text to be added in the final version following formal consultation]

10. The Minister for the Constitution, Cabinet Office, has prepared and published this Code under section 35 of Chapter 1 (public service delivery), section 44 of Chapter 3 (debt owed to the public sector) and section 52 of Chapter 4 (fraud against the public sector) of Part 5 of the Digital Economy Bill. It has been developed in consultation with the Information Commissioner's Office, Ministers within the Devolved Administrations, as well as other relevant persons and has been laid before the UK Parliament and the devolved legislatures in Scotland, Wales and Northern Ireland, in accordance with the duties set out in the Act.

11. The contents of this Code are not legally binding, though the provisions of the Bill require that you have regard to the Code when making use of these powers. 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 recommends good practice to follow when exercising the powers set out in the Bill. Government departments will expect public authorities wishing to participate in a data sharing arrangement to agree to adhere to the code before data is shared. Failure to have regard to the Code may result in your public authority or organisation being removed from the relevant regulations and losing the ability to disclose, receive and use information under the powers.

Who should use the Code?

12. All persons responsible for or working in a capacity where they have to consider sharing information under chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill must have regard to this Code and should include a statement of compliance within any data sharing agreement produced under the powers.

13. Public authorities able to make use of these powers are set out in regulations which can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535311/2016-07-05_Digital_Government__Disclosure_of_Information__draft_regs.pdf

Part 2: Understanding the public service delivery, debt and fraud powers

Purpose of the public service delivery power

14. 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 sharing of data. This is presently hampered by a lack of clear and robust legal gateways which public authorities are confident will enable them to share relevant data on the individuals and families they are working with in compliance with the DPA. The primary purpose of the power is to support the well-being of individuals and households. Data sharing arrangements cannot be established for purposes which are to the detriment of the individual or household.

15. Three specific objectives for which information can be disclosed under the power will be set out in regulations. Further objectives can be added through regulations by an appropriate Minister in HM Government or in the Devolved Administrations. The objectives that have been drafted in regulations so far are:

- Identifying and supporting 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';
- Identifying, making contact with and establishing the entitlement of individuals and households who might need assistance in dealing with changes to use of any part of the electromagnetic spectrum between 470-790 MHz following the 700Mhz band being cleared for mobile broadband use;
- Reducing the energy costs, improving efficiency in use of energy or improving the health or financial well-being of, people living in fuel poverty.

16. The first objective around supporting individuals or households who face multiple disadvantages is designed to support those programmes and initiatives where different public authorities and other bodies need to work together to support vulnerable individuals and families, such as delivery of the Government's Troubled Families programme. Multiple disadvantages can be interpreted broadly as social and economic factors, which includes education, health and financial problems.

17. The second objective that is drafted in regulations allows data to be shared by DWP and other public authorities in order to identify vulnerable people who might need help from the authorities in re-tuning televisions in 2018/19 after the 700Mhz band will be used for mobile broadband rather than to transmit digital TV. Whilst it is expected that many of those affected can be identified through a consent-based approach, some individuals may be reluctant to identify themselves as being in need of support. This power will help to identify those who are most in need of support. Details of how the scheme will operate are being developed, but secure management of data will be a key requirement for all those who process it.

18. The third objective that is drafted in regulations allows data to be shared by specified public authorities for the purposes of reducing the energy costs, improving efficiency in use of energy or improving the health or financial well-being of people living in fuel poverty.

19. For the purposes of this legislation, a person is to be regarded as ″living in fuel poverty″ if they are a member of a household living on a lower income in a home which cannot be kept warm at reasonable cost. Schemes for providing assistance to persons living in fuel poverty may be run by public authorities, such as local authority or government run grant schemes, or they may take the form of supplier obligations, like the Energy Company Obligation (which was made under various provisions of the Gas Act 1986 and the Electricity Act 1989) and the Warm Home Discount (which was made under Part 2 of the Energy Act 2010), where the assistance is delivered or promoted by energy suppliers.

20. The best way to guarantee that this assistance reaches those who need it is to provide it automatically, although automatic rebates can only happen if the state can inform energy companies which of their customers should receive it. Pensioner households already receive rebates in this way, because a specific data sharing gateway has been created in section 142 of the Pensions Act 2008 to enable it to happen. This has been used to enable electricity suppliers to automatically provide rebates to customers on state pension credit under the Warm Home Discount scheme, without the need for the customers to identify themselves by applying for support. The data sharing gateway provided by this Bill is intended to be used in a similar way for other vulnerable persons.

21. A number of different public authorities hold data about incomes and dwelling characteristics, which would enable better targeting of fuel poverty support schemes at those in greatest need and more efficient delivery of the assistance to people living in fuel poverty.

22. The regulations will describe the objective as:
    - assisting people living in fuel poverty by reducing their energy costs,
    - assisting people living in fuel poverty by improving efficiency in their use of energy, or

- assisting people living in fuel poverty by improving their health or financial well-being.

23. Any disclosure of information to gas and electricity suppliers must also be for the purpose of reducing the energy costs, improving energy efficiency or the health or financial well-being of people living in fuel poverty and it must be disclosed for use in connection with an energy supplier obligation scheme. These schemes are the Warm Home Discount and the Energy Company Obligation. This enables other datasets to be used for the purpose of providing support under the Warm Home Discount and Energy Company Obligation schemes to people living in fuel poverty. Amendments can be made by affirmative regulations to the list of support schemes for which the information may be disclosed and to the list of permitted recipients of the information.

24. The purpose of the disclosure must always be to assist people living in fuel poverty.

25. In general, information disclosed under the power can only be used for the purposes for which it was disclosed. There are very limited instances where you can use information for another purpose. These circumstances are specifically:

- If the information has already been lawfully placed into the public domain;
- If the data subject has consented to the information being used for another purpose;
- For the purpose of a criminal investigation;
- For the purpose of legal proceedings;
- For the purposes of preventing serious physical harm to a person and loss of human life, safeguarding vulnerable adults or children, responding to an emergency or protecting national security.

26. These provisions do not apply to personal information disclosed by HMRC, which includes the Valuation Office Agency (VOA). Personal information which is disclosed by HMRC is subject to special protections, which reflect the confidentiality of HMRC information and the trust and confidence in which HMRC holds information, and so personal information disclosed by HMRC may not be used for other purposes, unless with HMRC consent. The criminal offence for wrongful disclosure of HMRC information continues to apply to HMRC information in the hands of the recipient.

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

25. The public service delivery power has been designed to give you the ability to respond more efficiently and effectively to the data you need to address emerging social and economic problems. The power allows Ministers in the UK

Government and Devolved Administrations (for devolved matters) to add new objectives via regulations. New objectives must meet the following two conditions set out in primary legislation:

- The objective has as its purpose -
    - 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.

- The objective has as its purpose the improvement of the well-being of individuals or households. The well-being of individuals or households includes their physical and mental health and emotional well-being, the contribution made by them to society, and their social and economic well-being.

26. The intended interpretation of 'benefit' in the first condition is the offer or delivery of a service or intervention or type of financial assistance that is for the good or advantage for the individual and their family. Although an individual may not recognise that there are issues that need to be addressed, for example in some cases of alcohol or drugs dependency, the defining of benefit should be consistent with Government social policy and ensuring the well-being of the individual.

27. "Well-being" is a broad concept, and for the purposes of these provisions relates to areas such as social and economic well-being, the individual's contribution to society, or their participation in work, education, training or recreation, suitability of living accommodation, physical and mental health and emotional well-being, protection from abuse and neglect, control of the individual over their day-to-day life, and positive domestic, family and personal relationships.

28. If you wish to propose to add a new objective you will first need to determine what types of data are required, which bodies hold the data and how the ability to share personal data will support achieving your policy objectives. Objectives should be drafted to ensure that they are aligned to conditions in primary legislation and specific enough to constrain the use of the power to a clear purpose. Where an objective has been developed by a devolved administration for a specific devolved matter, the objective should specify that it relates to a specific devolved territory.

29. Objectives must be sufficiently specific that they identify a section of the population and *what the intended benefit to some individuals* from that target population is. This can be identified in the form of one or more outcomes, all of which fit into the field of social policy.

Example objectives

Example of potentially suitable objectives are:

1. Reducing the number of people sleeping on the street for more than one night;
2. Improving employment outcomes for ex-offenders; and
3. Supporting gang members to safely exit gang culture.

Examples of objectives which would not meet the criteria because the objective is punitive are:

1. Identifying individuals operating in the grey economy; and
2. Identifying welfare claimants erroneously receiving welfare benefits.

Examples of objectives which would not meet the criteria because they are too 'General' in terms of targeting communities or broad public benefit rather than individuals or households or so broad that almost any data sharing arrangements could be enabled under it include:

1. Improving levels of safety in a neighbourhood;
2. Helping people into work; and
3. Preventing people going to prison.

30. You should discuss your proposal for a new objective with the relevant central government body with oversight responsibility for the respective policy area to seek their views. Either your organisation or the responsible central government departments can write to the Minister for the Cabinet Office and request for the new objective to be added via regulations. Once the Minister has agreed to the creation of a new objective, consultation must take place with the Information Commissioner's Office, relevant Ministers from the devolved administrations, Commissioners for HM Revenue and Customs and other persons as the Minister considers appropriate.

31. Public authorities within a devolved territory proposing to create a new objective limited to a devolved function involving devolved bodies within that territory should contact the relevant Ministerial body in the devolved administration (e.g. the Department of Finance in Northern Ireland). Ministers within the devolved administration have the powers to make regulations to create objectives within the legislative competence of the devolved administration. The Minister must consult the Minister for the Cabinet Office, relevant Ministers from the other devolved administrations, Commissioners for HM Revenue and Customs, HM Treasury and other persons as the Minister considers appropriate. Devolved administrations may wish to work together to develop an objective

which applies across devolved territories. In such instances Ministers in the relevant devolved administrations will need to agree the drafting of the objective and make the regulations as appropriate.

32. Any proposal by a public authority within a devolved territory for the creation of a UK-wide objective should be discussed with the relevant Ministerial body in the devolved administration before it is formally proposed to the Minister for the Cabinet Office for consideration. Legislation only allows the Minister for the Cabinet Office to make regulations for the creation of UK-wide objectives under the power.

Purpose of the debt and fraud powers

33. It is estimated that losses to Government through fraud are in the region of £29bn to £40bn. 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. The 2014 NAO report on Managing Debt Owed to Central Government estimated that around £22bn of debt was owed to Government in March 2013. At March 2016 it is estimated that the like for like debt balance rose to around £24.5bn.

34. Only debt owed to government that is legally collectable will be covered by these powers. Fairness is a key consideration in the exercise of the power to share data for the purposes of taking action in connection with debt owed to government. Any public authority(or private body fulfilling a public function on behalf of a public authority), who want to make use of this permissive power to share identified debt data to enable better debt management, including debt recovery, will need to consider fairness in their debt data sharing arrangements. The Fairness Principles are set out in Annex A.

35. The powers introduced by the Digital Economy Bill provide for the first time a simple and agile route for agreeing and establishing data shares between specified persons in order to protect them against fraud or to support them in the management of outstanding debt. These permissive powers are intended to ease the burden of establishing individual gateways or producing new legislation to ensure public authorities have the required legal powers each time or in each circumstance where they may wish to share data.

36. Steps have to be taken to ensure that data 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 gateway. Data sharing arrangements under these powers must comply with data protection legislation.

37. Parties wishing to share data under the fraud or debt power must put together a business case setting out the nature of the sharing required to fulfil their desired purposes, and must go through a pilot process to ensure that the sharing is effective.

38. Data sharing arrangements should be defined through a business case detailing the data sharing pilot to be undertaken. These data sharing pilot business cases will be scrutinised by a review group, which will include engagement with ICO, and recommendations made to a relevant Minister for approval. The process will be transparent, with all key information and privacy impact assessments made available to the general public for scrutiny

39. Information disclosed under the power can only be used for the purposes for which it was disclosed. There are very limited instances where information can be used by a public authority for another purpose. These circumstances 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 purpose of a criminal investigation;
- For the purpose of legal proceedings; and
- For the purposes of safeguarding vulnerable adults or children, or protecting national security.

40. As with the public service delivery power, these provisions do not apply to personal information disclosed by HMRC, which includes the Valuation Office Agency (VOA). Personal information which is disclosed by HMRC cannot be used for a purposes other than the purpose for which it was disclosed unless with HMRC consent.

Which organisations can use the powers?

41. Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill provide permissive powers enabling specified public authorities or a person providing services to a specified public authority to disclose information for specific purposes. Bodies able to disclose information under the respective powers will be listed in regulations. Draft regulations can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535311/2016-07-05_Digital_Government__Disclosure_of_Information__draft_regs.pdf

42. A public authority is defined for these purposes as a person or body who exercises functions of a public nature in the United Kingdom, a person or body entirely or substantially funded from public money, an office-holder appointed by a person or body falling within a body exercising functions of a public nature in

the United Kingdom, or a body more than half of whose governing body or members are appointed by a person or body exercising functions of a public nature in the United Kingdom.

43. The public service delivery, debt and fraud powers allow a person providing services to a public authority to share information. A person providing services to a public authority can be any legal entity such as a charity or company providing a defined service(s) to a public authority. This in effect could be a frontline service, which has been outsourced to a body outside the public sector to deliver. The key factor to consider is whether access to information held by such an organisation is critical to achieving the desired objective and similarly whether the delivery of better services could be improved by disclosing public sector information to them. An assessment must be made whether the persons providing services to a public authority have the systems and processes in place to securely handle data. The public authority receiving the services from the persons should make the assessment of the systems and processes the other party has in place, and should include details of the checks carried out within the privacy impact assessment.

44. A person providing services to a public authority sharing information under the powers can only disclose or use information for the functions/services it provides and for the specified purposes set out in the relevant provisions for its inclusion within the data sharing arrangement. For example, a data sharing arrangement relating to a Troubled Families programme may need to share information with a charity providing a service to a local authority within the region. The charity could only share information under these powers in relation to the service it provides to the local authority and not any other information it may hold, for example in respect of other services it provides in that region or other regions.

45. It is important that all public authorities and persons providing services to a public authority involved within a data sharing arrangement understand their roles and responsibilities in relation to information that they seek to use in the exercise of these powers, and are clear on what they may and may not access and share for these purposes. You must therefore adhere to and keep up to date with any guidance issued by the Information Commissioner in all instances where you are considering sharing information. This will ensure that consistent approaches and policies are being applied when considering requests to share information.

46. Prior to sharing information, you must first be satisfied that the sharing of information is in accordance with the purposes set out in legislation. You will need to strictly adhere to the DPA and ensure information is not disclosed where it is prohibited to do so under Part 1 of the Regulation of Investigatory Powers Act 2000.

Amending the list of bodies able to use the power

47. The public service delivery, debt and fraud powers will, by regulations, specify which public authorities can use the powers. The Minister for the Cabinet Office or relevant Minister from a Devolved Administration can make regulations to add, modify or remove a reference to a public authority or description of public authority allowed to share information under each of the powers.

48. If your public authority is not listed in regulations and you wish it to be in scope of the powers, your organisation will need to contact the relevant Minister with oversight for your work providing a case for its inclusion via regulations. The case should set out the systems and procedures in place for securely handling personal data as well as the reasons why they should be able to disclose and/or access data under the power. Where public authorities are based in England, the appropriate Minister, once satisfied with the case for inclusion should then write to the Minister for the Cabinet Office who will coordinate and lead the making of regulations. Devolved bodies should contact the relevant Minister in their devolved administration to make the necessary regulations.

Part 3: Data sharing and the law

How the powers work with other key legislation relating to data

49. To use the public service delivery, debt or fraud powers you will need to strictly adhere to the DPA and ensure no disclosures are made which are prohibited under section 1 of the Regulation of Investigatory Powers Act 2000. You will also need to ensure you are compliant with the Human Rights Act 1998. In addition, criminal sanctions for unlawful disclosure set out in section 19 of the Commissioners for Revenue and Customs Act 2005 will apply to personal information disclosed by HM Revenue and Customs.

Data Protection Act 1998

50. The DPA 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. It should be noted that it is possible that some data disclosed under these powers will not constitute personal data, for example where data relating to deceased persons, businesses or information comprising only statistics that cannot identify anyone are being shared. Those making use of the powers, however, must be aware of their obligations under the DPA and must ensure that no disclosures are made under the power in contravention of those rules.

51. The Information Commissioner's data sharing code of practice recommends that where information is shared, it is shared in a way that is line with the reasonable expectations of the individual whose data it is. This approach applies to routine data sharing as well as to a single one-off data disclosure.

52. Public authorities will need to demonstrate that they are complying with the provisions contained in the DPA, and in particular must ensure they are handling personal data in accordance with the data protection principles, details of which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/

Part 1 of the Regulation of Investigatory Powers Act 2000

53. The Regulation of Investigatory Powers Act 2000 provides a framework for lawful interception of communications, access to communications data, surveillance and the use of covert human intelligence sources. Part 1, Chapter 1 deals with interception. Section 1 of part 1 Chapter 1 makes it an offence, subject to exceptions, to intercept intentionally and without lawful authority any

communication in the course of its transmission by means of public postal service or public or private telecommunication system.

Human Rights Act 1998

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

55. Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal information. Whilst sharing data relating to deceased individuals is not treated as personal data under the DPA as outlined above, Human Rights Act considerations should be taken into account with regards to whether sharing information could impinge on the rights to a private life for the relatives of deceased individuals.

56. The Information Commissioner's data sharing code of practice advises that if information is being shared in ways that comply with the DPA, it is also considered likely that the sharing would comply with the Human Rights Act.

Commissioners for Revenue and Customs Act 2005

57. HMRC's unlawful disclosure provision is governed by section 19 of the Commissioners for Revenue and Customs Act 2005, which makes wrongful disclosure of information relating to an identifiable person a criminal offence carrying a maximum penalty of imprisonment for up to 2 years and an unlimited fine. Section 19(1) makes it an offence for any person to contravene section 18(1), or of section 20(9), by disclosing "revenue and customs information relating to a person" whose identity is revealed by the disclosure. The term "person" includes both natural and legal persons, and, for example, the tax affairs of a limited company are also protected by section 19(1).

Part 4: Deciding to share information under the powers

58. The powers under Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill are permissive. Your public authority has the discretion to decide whether to use the power to disclose information and participate in a data sharing arrangement. You should consider which, if any, powers are already available to your organisation to achieve your desired policy, operational or analytical objective and determine whether these existing powers would adequately fulfil your objectives. This is to avoid the creation of unnecessary new express legal gateways where pre-existing powers already fulfil that function.

59. The main criterion for sharing information with specified recipients under these powers is that the sharing of information is consistent with and aligned to the purposes set out in primary legislation for each of the respective powers. You should place the same importance on the benefits that citizens can derive from better and more timely services as a result of information sharing as you do on protecting the privacy of citizens' data. This approach to sharing information is consistent with the National Data Guardian's 7th principle which relates to health and adult social care data in England that 'the duty to share information can be as important as the duty to protect patient confidentiality'.

60. You should factor the ethical considerations around the use of data to achieve the objective. The first iteration of the data science ethics framework is available at www.gov.uk/government/publications/data-science-ethical-framework and provides guidance on ethical considerations which are applicable to the sharing and use of data beyond data science. You should consider running a public consultation where you feel the general public may have concerns about the proposal. You should set out the details of the public consultation or the reasons for not carrying out one in the business case for the data sharing proposal.

61. When developing a data sharing proposal you should look to use the minimum amount of personal data possible. Consideration should be given to data matching which utilises binary checks against details of individuals to restrict the amount of personal information shared. The sharing of large data sets should only be considered where it would otherwise be inefficient or difficult to achieve the objective.

62. Before you establish a data sharing arrangement, you must be satisfied that:

- all parties are clear on the tangible benefits that are expected from the information sharing, who will receive them, how they will be

measured and where information about the data sharing arrangement will be made available online for public scrutiny;
- the purpose of the information sharing falls within the purposes outlined in legislation (or regulations for defined objectives for the public service delivery power);
- there is clear governance of, and accountability for, making the decision to share data;
- information sharing will be physically and/or technically possible and be compliant with the DPA and other relevant legislation;
- strict compliance with government and departmental security guidelines to safeguard against any misuse or loss of data, including having secure methods in place for transferring data;
- as the data controller, it is appropriate and sensible to take part in the arrangements - for example are there any perceived conflicts of interest with sharing information?; and
- The minimum required information will be disclosed, ideally to binary eligibility checks to mitigate against any risks around disclosure (for example risk of fraud or any other harm).

The Data Protection Principles and the powers to disclose data

63. Schedule 1 to the DPA sets out 8 Data Protection Principles governing the way personal data is to be collected, held and managed. These include the requirements that personal data should be processed lawfully and fairly, and for a specified purpose. Further, information should be shared securely, with appropriate protective measures in place (such as encryption and other methods). The disclosure of information under Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill may only be made for the purpose of enabling the recipient to fulfil objectives consistent with the purposes of the powers.

64. What constitutes fair processing will vary from case to case, but a key consideration will be the reasonable expectation of the individual whose data it is as to how their data would be handled or whether it would be disclosed. A further key indicator of fairness will be around transparency as to how the data is being processed.

65. You are required to ensure that your data sharing practices are fair and transparent and consider the effect the disclosure would have on the interests of the people whose data is involved. You will also be required to have fair and transparent processes in place for disclosing and receiving data. You must be satisfied that your processes are suitable for the types of data proposed to be disclosed before any data is shared. Before disclosing data you should discuss with the proposed recipients their arrangements for securely receiving, handling and managing the data and make an assessment of the suitability of the systems

and processes (which should be described in the data sharing agreement). In considering whether to share information, you must also consider whether conditions need to be imposed on the future use and retention of the data by way of data sharing agreements. Any conditions will need to be clearly specified prior to sharing information.

66. When sharing information under the powers you should look to operate as transparently as possible. Succinct and clear descriptions of why information is being shared, what information is being shared and the bodies with which they are being shared should be published online and easy for people to find alongside the relevant data sharing agreements, privacy impact assessments and other relevant documents. You should also provide and keep up to date contact details so that people know who to direct any concerns or queries to.

67. In some instances, such as where information is used to match data concerning a large number of individuals, it may be impracticable to send notices to individuals affected by the data sharing. You will however need to comply with requirements of the DPA in ensuring that data has been shared fairly and lawfully. It will also be necessary to make records of data shared, detailing the circumstances, what information was shared and an explanation as to why the disclosure took place. Business cases and data sharing agreements will be important documents in recording these decisions and the reasoning behind them.

68. In addition, the first data protection principle requires that organisations must be able to satisfy one or more "conditions for processing" in relation to their processing of personal data. The conditions for processing are set out in Schedules 2 and 3 to the DPA. Many (but not all) of these conditions relate to the purpose or purposes for which information is intended to be used, or the reason for the processing. Organisations processing data need to meet one or more of the conditions in either Schedule 2 or Schedule 2 and 3 depending on the data being shared. When sharing sensitive personal data the more exacting requirement to meet at least one condition in each schedule applies (and indeed the conditions are themselves more stringent). For a definition of what constitutes sensitive personal data see section 2 of the DPA. In some instances, you may consider additional data fields as sensitive in the context of a data sharing arrangement. In such circumstances you should discuss, agree and set out any restrictions or specific conditions for the processing of that data in the relevant data sharing agreement with other organisations involved.

69. Fulfilling a Schedule 2 (and where necessary, Schedule 3) condition will not, on its own, guarantee that the processing is fair and lawful – fairness and lawfulness must still be looked at separately. Part II of Schedule 1 of the DPA provides guidance on the interpretation of this principle. To assess whether or not personal data is processed fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually.

Best practice considerations

70. In addition to applying the principles of the DPA, you should consider what best practices and guidance are in place in your organisation and ensure you adhere to and keep up to date with them so that consistent approaches are being applied when sharing information. For the purposes of public service delivery power, it would be common practice to develop data sharing arrangements between organisations.

Fairness Principles for establishing pilots under the debt power

Fairness is a key consideration for the debt data sharing power in particular. If you wish to use the permissive power to share identified debt data to enable better debt management, including debt recovery, you will need to consider fairness in your debt data sharing pilot.

A set of fairness principles specifically for use with the debt powers can be found at Annex A. Your organisation will continue to have its own fairness policies and practice. These principles align with departmental practices, and aim to create a more 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 this new power, and only in accordance with the legal obligations public authorities have a statutory duty to abide by.

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

Non-public authority duties

71. Where a data sharing arrangement proposes that information be disclosed to a body which is not a public authority, but fulfils a public function, an assessment should be made of any conflicts of interest that the non-public authority may have and identify whether there are any unintended risks involved with disclosing data to the organisation. Non-public authorities can only participate in a data sharing arrangement once their sponsoring public authority has assessed their systems and procedures to be appropriate for secure handling data. Details will need to be set out in the privacy impact assessment along with a statement of compliance with the Code of Practice in the data sharing agreement.

Data standards and rights of redress

72. Public authorities hold vast amounts of data in a number of different formats. When considering sharing information it is essential that every effort is made to ensure that the format of the data conforms to any appropriate standards defined in the Government Standards Hub and the API standard. This will help ensure that individuals are not adversely impacted by any exchanges – e.g. prevented from accessing a service where there are issues with data held by a recipient as a consequence of the data exchange.

73. It is also important that checks are made on the accuracy of data prior to transferring it, in line with the DPA's Privacy Principles. In instances where issues arise following the transfer of data, procedures need to be in place to allow for inaccurate data to be corrected by all bodies holding the information. Organisations involved in a data sharing arrangement should agree procedures, the process of recording and capturing corrections for auditing purposes and contacting the data subject where appropriate and set the details out in the Data Sharing Agreement. You will need to be aware of the correct procedures to follow in relation to correcting inaccurate data held on your own systems, including alerting officials responsible for data protection within your organisation and other identified teams to ensure data is corrected where held on other systems.

Checklist - points to consider
Why share

- For what purpose and public function is the information being requested?
- Are there any other benefits of the data exchange for the receiving party or any other public body?
- What are the implications of not sharing information? – e.g.
    - 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; and
  - Risk of wasting taxpayers' money by jeopardising public finances or commercial projects.

What to share

- What exact data items are required and why?
- Are there any express legal restrictions in place on the disclosure and use of the data involved and 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 e.g. using aggregate data, derived data or the use of a look-up process, in preference to bulk data sharing
- 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?
- Information handling responsibilities, including details of any data processors, contractors or subcontractors;
- Security considerations, e.g. the use of secure transfer mechanism, and encryption;
- 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?; and
- Periodic reviews of effectiveness and necessity of data sharing arrangement.

Part 5 - Fairness and transparency

74. You are required to ensure that your data sharing practices are fair and transparent. You should only share data once you are satisfied that the processes are fair and transparent. Under the debt and fraud powers, the secretariat to the Review Group will centrally maintain and make available online a list of pilots under the power, setting out the title, reason and potential benefits to be gained from the data sharing arrangement.

75. All organisations wishing to establish a data sharing arrangement under the power must adhere to the Information Commissioner's data sharing code of practice on Data Sharing. The process of establishing a data sharing arrangement under the public service delivery, fraud and debt powers vary in the following ways:

- The fraud and debt powers require a formal application process to allow the strategic management of data sharing arrangements under the powers during its three year review period;
- The public service delivery power operates as a more conventional legal gateway permitting specified persons to share information for defined purposes.

76. If you are looking to share information under any of the three powers you need to carefully consider why a data sharing arrangement should be established and maintain an audit trail of decisions to ensure that informed decisions on data sharing are made by public authorities at the right level in the organisation. Conducting a privacy impact assessment of the proposal should be one of the first steps you take. It will help you assess the potential benefits against the risk or potential negative effects, such as an en erosion of personal privacy.

77. The public service delivery, debt and fraud powers require a number of documents to be produced. These documents are:

- A business case for the data sharing arrangement (this can be co-developed by all the organisations involved);
- data sharing agreement(s); and
- security plan

78. You should operate as transparently as possible. Business cases, data sharing agreements and privacy impact assessments should be made available to the general public. You may wish to redact some sensitive information from your business case to establish a fraud pilot if you feel placing that information in the public domain could undermine achieving the objective of the data sharing arrangement. You should include a high level summary of the security plan in the

business case and avoid publishing the full security plan to reduce the risk of hacking.

Business Cases

79. If you wish to establish a data sharing arrangement under the public service delivery, debt and 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 data sharing arrangement. A data sharing arrangement can cover multiple transactions. Your business case must contain:

- the objective of the data sharing arrangement;
- a list of which bodies will be involved in the arrangement, and specifically which bodies would disclose or receive data, what type of data is involved, and what restrictions are in place on the data;
- an explanation of how the data will be used and what the conditions for processing are;
- the information sharing agreements that will be used in practice;
- fair processing notices that are relevant and appropriate;
- an explanation of how retention periods will be complied with and how they will continue to meet business needs;
- an assessment of the ethical considerations on the proposed data sharing arrangement;
- a statement of adherence to this code of practice;
- an outline of what the activities, delivery plan, costs and potential benefits are;
- an explanation of what steps will be taken to address any data quality issues identified;
- an outline of the data security arrangements to be put in place and the checks that will be run to ensure that all bodies involved are compliant (a separate security plan will need to be produced but public authorities may not wish to make this document available to the general public); and
- an outline of the accountability process for the data sharing arrangement including senior responsible owners and record of data sharing that has taken place for audit purposes.

80. As data sharing under the debt and fraud powers must be piloted, your business case for a pilot must also contain:

- high level details of the effective anti-fraud measure, or debt management measure;
- a period of duration;
- a statement of success criteria; and
- details of the methodology for measuring success.

81. Business cases provided under the fraud power need not go as far as detailing the counter fraud operation of partners. The intention of the business case is to justify the pilot and ensure that data is being protected.

Privacy Impact Assessments

82. A privacy impact assessment is a process which helps identify and reduce the privacy risks of a data 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[1] 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).

83. A privacy notice describes all the privacy information you make available or provide to individuals about what you do with their personal information. 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 fairness and transparency principles in the Information Commissioner's privacy notices code of practice[2] and data sharing code of practice. The Information Commissioner's privacy notices code of practice provides guidance on the content of these notices, as well as where and when to make them publicly available.

Data Sharing Agreements

84. You should follow the Information Commissioner's data sharing code of practice with regards to data sharing agreements. Before entering into data 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:

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

85. The data sharing agreements will not be legally binding. You will be expected to include details of:

a. the purpose of the data sharing arrangement;
b. the respective roles, responsibilities and liabilities of each party involved in the data share;

c. the legal basis for exchanging information;
d. the accuracy of the data – ensuring that the recipient is aware that data is only as accurate as at the time it is captured and will be treated as such;
e. precise details of what exact data is required to enable them to perform the function for which it is requested;
f. restrictions on sharing certain categories of data;
g. restrictions on any onward disclosure of information - if applicable;
h. information handling responsibilities, including details of any data processors or subcontractors;
i. conditions for data processing, including whether data subjects are aware of how their data is being shared, including the methods of sharing and whether they are likely to object to it;
j. process and methods of exchange;
k. standards and levels of expected operational service;
l. reporting arrangements, including any reporting in the event of any data loss and handling arrangements;
m. termination arrangements;
n. issues, disputes and resolution procedures;
o. information on data security, data retention and data deletion;
p. review periods;
q. individuals' rights – procedures for dealing with access requests, queries and complaints;
r. any costs associated with sharing data; and
s. sanctions for failure to comply with the agreement or breaches by individual staff.

86. The above list is not exhaustive. For more detail on data sharing agreements you should refer to the ICO data sharing code of practice.

87. Data 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 Bill. 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 Information Commissioner's Office;
- Public authority officials determining whether any misuse of public office offences have been committed, and if so, to take any necessary action; and
- 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 a data

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.

88. A register of data sharing arrangements under the debt and fraud powers will be maintained centrally and by the secretariat to the Review Group in the Cabinet Office for audit purposes. The Review Group is an oversight panel which will be constructed of representatives from across the government and privacy interest groups. It will include representation from the ICO. Its role is to check that data sharing arrangements adhere to this code of practice and that the arrangement can operate under the legislation. All public authorities sharing information under the public service delivery, fraud and debt powers are required to maintain records of their individual data sharing arrangements for audit purposes.

89. You will need to comply with the DPA and where necessary seek legal advice regarding data sharing following any agreements to disclose or access information.

The process for establishing data sharing arrangements under the debt and fraud powers

90. All data sharing proposals under the debt and fraud powers must be piloted to determine whether there is value in sharing personal information for the purposes set out in the relevant parts of the bill, namely to take action in connection with debt owed to government, or to combat fraud against the public sector.

91. Strong central governance is required to oversee the running of pilots to ensure there is consistent and appropriate use of the powers. A Review Group will be established by the UK Government to oversee any UK-wide and England only data sharing under the debt and fraud powers. The review group will also be responsible for collating the evidence which will inform the Minister's review of the operation of these powers, as required under the Bill after three years. This evidence will be gathered from the UK-wide and England only data sharing arrangements as well as those implemented in the devolved territories. The devolved administrations will establish their own governance structure for oversight of data sharing arrangement within their respective devolved territories. Data pertaining to the operation of pilots in the devolved territories should be periodically submitted to the secretariat for the Review Group for the purpose of collating the evidence for the review of the debt and fraud power after three years.

92. The Review Group and secretariat will be established to take responsibility for the strategic management of pilots established under the power to ensure bodies carrying out pilot data shares under these provisions operate with regard to the Code, and to gather and analyse evidence on the effectiveness of pilots to enable the review of the power after three years. The Review Group will also consider complaints and take account of the views of the Information Commissioner's Office. All proposals for pilots must be submitted to the Review Group through the secretariat. It is envisaged that the Review Group will sit monthly and that requests and clearance through the Minister should take around 6 weeks once an application has been submitted.

93. The Review Group will consist of appropriately qualified subject matters experts gathered from across government and will be attended by representatives from the ICO and members from public representative bodies. The secretariat will keep a record of pilots in operation and how those work, and will gather from the bodies operating the pilot the appropriate performance data for the recording and evaluation of the pilot.

94. If you wish to establish a pilot you must submit a business case to the secretariat to the Review Group. A single business case will need to be submitted which is agreed by all the participating bodies.

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

96. The Review Group will review the business case and advise you whether the proposal meets the requirement to use the power, and whether the request should be declined, amended or be recommended to the Minister for the Cabinet Office to be implemented.

97. Business cases may be declined for a range of reasons, for example the proposal may require modification to align it to best practice, or to more clearly define success criteria and methodology for measuring them, or the recommendation that alternative routes may be more appropriate. Pilots will become active upon confirmation from the Minister that the recommendation has been approved.

98. 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, either as a request to Review Group, or as a deviation and breach of the code; and
- closure of the pilot and final reporting.

Data Security

99. All persons and bodies involved in any data sharing arrangements under these powers will be subject to the data protection principles set out in the DPA.

100. Additional requirements include:

- Public authorities and receiving parties must satisfy themselves that all departmental or local authority standards and protocols are followed when providing or receiving information.
- Each party involved in the data share must ensure effective measures are in place to manage potential or actual incidents relating to the potential loss of information.
- In the event of a potential or actual data incident, public authorities and data processors, together with any other additional third parties must be fully engaged in the resolution of the data incident. The responsibilities of each party in the event of a potential or actual loss of information must be clearly defined in the data sharing agreement and or security plan.

101. You will need to agree a security plan as part of any formal data sharing agreements with public authorities who are granted access to information. Security plans should include:

- storage arrangements that ensure information is secured in a robust, proportional and rigorously tested manner;
- assurance that only people who have a genuine business need to see personal information involved in a data sharing arrangement will have access to it;
- confirmation as to who to notify in the event of any security breaches; and
- procedures in place to investigate the causes of any security breaches.

Data retention and disposal

102. It is a requirement of the DPA that personal information should be kept only for as long as necessary. How long it is “necessary” to hold such information will depend on the purpose for which the public authority holds the information, and its own policies and practices.

103. You will need to agree with recipients of data shared under these powers how long the data is expected to be held for and the period agreed should be documented in any data sharing agreements between both parties.

104. You should ensure that data no longer required is destroyed promptly and rendered irrecoverable. The same will apply to data derived or produced from the

original data, except where section 33 of the DPA applies (in relation to data processed for research purposes). You should refer to the ICO guidance on Deleting Personal Data[3].

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

Part 6: Governance

Implementing a data sharing arrangement

105. Data sharing under the power must adhere to the Information Commissioner's data sharing code of practice and other existing guidelines on data security. 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.

106. Where data quality issues are identified during a data sharing arrangement, the governance structure supporting the data sharing arrangement should take immediate steps to identify and manage the risks associated with the use of that data and any remedial action required.

107. 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 take criminal proceedings where necessary and will report any concerns about a body's systems and procedures for handling data to the relevant Minister (MCO for England only and UK-wide data sharing initiatives and the relevant Minister in the devolved administration for a data sharing arrangement within a devolved territory only), which may result in regulations being laid to exclude that body from participating in a data share under the power.

108. You should make it easy for citizens to access data sharing arrangements and provide information so that the general public can understand what information is being shared and for what purposes. You should communicate key findings or the benefits to citizens derived from data sharing arrangements to the general public to support a better public dialogue on the use of public data.

Review of a pilot under the debt and fraud powers

109. A Review Group will be established by the UK Government to oversee any UK-wide and England only data sharing under the debt and fraud powers. The review group will also be responsible for collating the evidence which will inform the Minister's review of the operation of these powers, as required under the Bill after three years. The devolved administrations will establish their own

governance structure for oversight of data sharing arrangement within their respective devolved territories.

110. A request to initiate a pilot to be carried out under the debt and fraud powers must be sent to the appropriate review group for your territory accompanied by a business case. Your business case must detail: its operational period, the nature of the fraud or the debt recovery issue being addressed, the purpose of the data share and the way its effectiveness will be measured.

111. At the end of the pilot's operational period its outcome will be presented to the review group for consideration, with an accompanying: proposal, actions or recommendation. For pilots designed to test a proposed data share under these powers, successful execution of the pilot may result in agreement that the process can at that point run as a 'business as usual' process (i.e. an ongoing data sharing arrangement) without any requirement for further reporting or management.

112. If the pilot has proved to be unsuccessful in meeting the defined requirements, then the pilot must be stopped. Any design changes that have been recognised during its operation that would make it successful should be submitted as a request for a new pilot.

Compliance with the Code

113. Any serious security breaches need to be reported immediately to the ICO, the Review Group and where applicable, the governance group in your devolved territory.

114. You should also report immediately any breaches regarding adherence to the code or any sharing that contravenes the terms of the data sharing arrangement but does not constitute a DPA breach. Such breaches to the code or data sharing arrangement relating to data sharing under the public service delivery power should be reported to the relevant person within the governance structure as relevant to the particular data sharing arrangement, whilst breaches under the debt and fraud powers should be reported to the review group for your territory.

115. Under the debt and fraud powers, the review group will inform the relevant public authorities that a breach has been reported, and will investigate the breach. In doing so, it may make one of the following findings:

- There is deemed to be no breach and no action is required.
- A breach is found to have taken place but deemed to be of low impact: it will notify the public authority and ask it to introduce measures to remedy this.

- A breach is found to have taken place but is deemed to be 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 is found but deemed to be 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.

116. Where the Minister has been informed by the Review Group under the debt and fraud powers of a recommended course of action regarding a breach, the Minister will notify the public authority and the Review Group as to the course of action he wishes to pursue. The Minister may in addition notify the ICO. There will be a right to appeal at each stage.

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

Review of the debt and fraud powers

118. You are required to report on the progress of your pilot (including the success or failings) to the relevant Review Group for your territory. These reports will support the overall evaluation of the operation of the powers, and will be used to inform the Minister's review at the end of the three-year period, as required under the provisions. This evidence will inform the Minister's assessment of the provisions and will enable him to prepare his report setting out the findings of his review.

Annex A - The Fairness Principles for data sharing under the debt power

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. These Principles aim to align with existing public authority practices, and aim to encourage a more 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 this new power, and only in accordance with the legal obligations public authorities have a statutory duty to abide by.

Pilots operating under the new data sharing 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.

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.

Pilots must 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 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; and
    - Consideration of the need for breathing space to seek advice, or forbearance, in cases of vulnerability and hardship.
- Where a vulnerable customer is identified, they should be given appropriate support and advice, 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 pilot that uses a third party (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.

Annex B - Summary of the 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?
    - Familiarise yourself with the DPA and the Information Commissioner's data sharing code of practice on information sharing
- Does the proposal pose any ethical issue or will it lead to any handling risks?
    - Refer to the Data Science Ethical Framework
    - Consider running a public consultation
- How do you want to share data and will it be secure?
    - Assess the data you need and ensure you can justify why you need each data field
    - Speak to your organisation's information governance and security experts and discuss what the best methods for data transfer are available.

Step 2 - Develop the proposal

- Agree a proposal with the other organisations involved in the data sharing arrangement
    - If bodies outside the public sector are involved you should consider any conflicts of interest and reflect it in the business case
    - Ensure all bodies are willing 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 consistent with the DPA and Part 1 of RIPA
- Conduct a privacy impact assessment

    - Assess the potential benefits of the data sharing arrangement against the risks or potential negative effects, such as an erosion of personal privacy
- Develop and draft a Business Case, data sharing agreements, a privacy impact assessment and Security Plan.
    - Ensure you refer to ICO guidance on data sharing agreements and privacy impact assessments
    - Ensure the responsibilities for each body involved in the data sharing arrangement is made clear and articulated in the documentation
    - 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 data sharing arrangement
    - 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, data sharing agreement and privacy impact assessment are made available to the public and are easy for the general public to find
    - You should ensure that all bodies adhere to the data sharing agreement and security plan and report any data breaches as appropriate
- Assessment of the data sharing arrangement
    - At the conclusion of a data sharing arrangement you should assess and review that arrangement and consider communicating to the general public the findings including any 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 have been fully implemented.

Annex C - Summary of the process for using the fraud and debt powers

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

- Do you need to use personal information?
    - Familiarise yourself with the DPA and the ICO Code of Practice on information sharing
- Does the proposal pose any ethical issue or will it lead to any handling risks?
    - Refer to the Data Science Ethical Framework
    - Consider running a public consultation
- Can the data share be piloted and what would the method for measuring success/failure?
    - Contact the relevant central review group for your national territory for advice
    - Discuss with your analysts what would be suitable measures to evaluate the particular data sharing arrangement
- How do you want to share data and will it be secure?
    - Assess the data you need to share and ensure you can justify why you need each data field
    - 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 you should consider any conflicts of interest and reflect this in the business case
    - Ensure all bodies are willing 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 consistent with the DPA and Part 1 of RIPA

    - If your proposal relates to debt, consider how the fairness principles can be embedded into the proposal
- Conduct a privacy 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, data sharing agreements, a privacy impact assessment and security plan.
    - Ensure you refer to ICO guidance on Data Sharing Agreements and privacy impact assessments
    - Ensure the responsibilities of each body involved in the data sharing arrangement are made clear 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 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 - Submitting the proposal

- Submit your proposal to the relevant central review group for your territory
    - Contact your central review group [D.N. details to be provided] and submit the relevant documentation to them
    - You may receive an initial view from the central review group 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 group 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 group 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 data sharing agreement and report any breaches as appropriate to the central review group for your territory. Serious data security breaches should be reported to your central review group and the ICO
- Reporting to the central review group in England
    - Send appropriate metrics data about your pilot through at agreed intervals to the secretariat to the Review Group
    - 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 Group
- Assessment of the Pilot
    - The central review group 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 proceed or not. The review group 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.