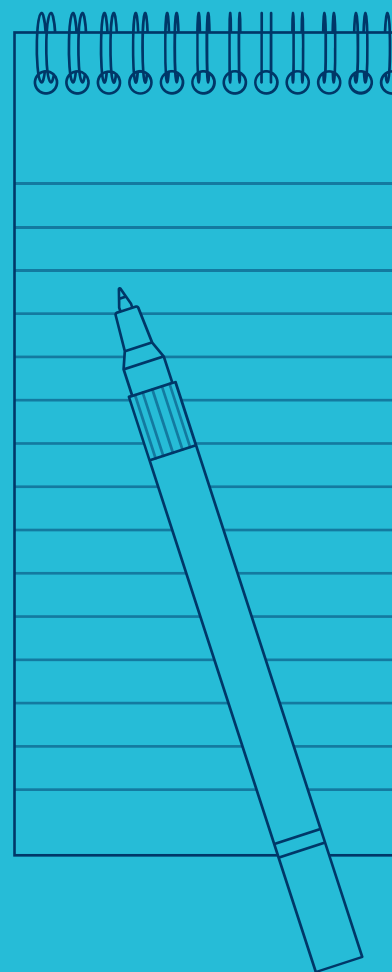
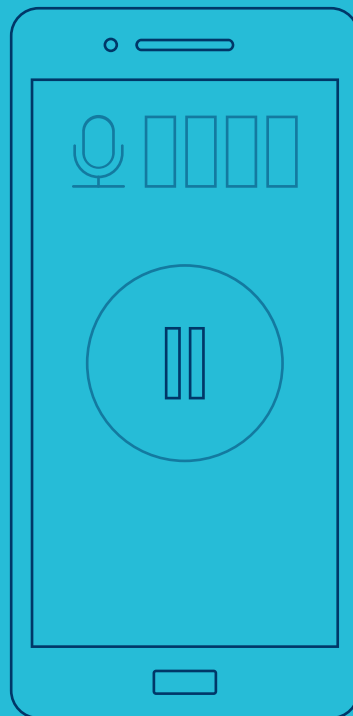
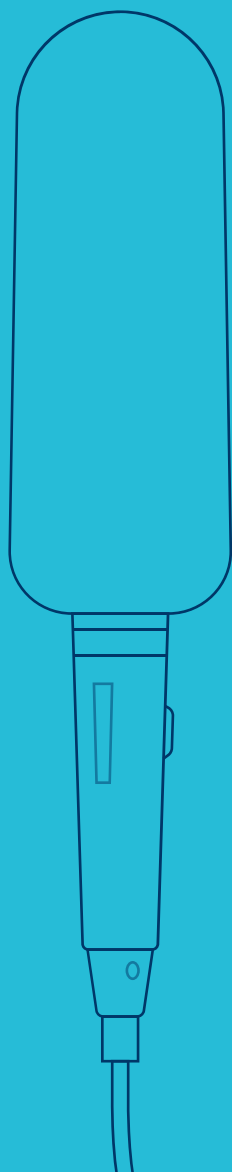
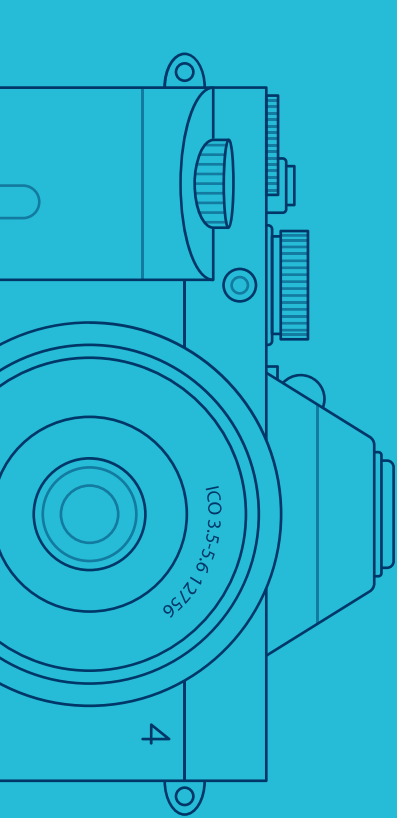


Draft journalism code impact assessment



Contents

1. Executive summary	3
2. Background	6
2.1. Problem under consideration and rationale for intervention.....	6
2.2. Approach to the code	12
2.3. Scope of the code	13
2.4. Affected groups	13
2.5. Approach to the impact assessment	15
2.6. Regulatory constraints.....	17
3. Costs and benefits of the code.....	18
3.1. Direct costs and benefits of the code	18
3.2. Indirect costs and benefits of the code	24
3.3. Overall assessment of direct and indirect impacts	25

1. Executive summary

Data protection law protects the importance of both the right to privacy and the public interest in freedom of expression and information. This is done mainly through the special purposes exemption for journalism academia, arts and literature. This exemption protects those processing personal data for the purposes of journalism.

Background

The Data Protection Act 2018 (DPA 2018) requires the Information Commissioner's Office (ICO) to prepare a statutory code of practice to help those processing personal data for the purposes of journalism to understand their legal obligations and to comply effectively.

In preparing the code, the ICO must specifically consider the special public interest in protecting freedom of expression and information.

The code aims to provide practical guidance, updating existing ICO guidance for the media published in 2014. In particular, the code's key purpose is to protect freedom of expression, while also protecting people's right to privacy and data protection.

This impact assessment sets out the benefits and costs associated with the code. It draws on evidence including desk-based research, responses to the initial call for evidence, and previous analysis of related issues.

As part of the ongoing consultation exercise, we are seeking views on both the code and the findings of the impact assessment.

The impact assessment finds that the code is well-aligned with specific areas of relevant policy that the Government and industry bodies are pursuing. The policy reviewed includes The Leveson Inquiry; the Draft Online Safety Bill; the National Data Strategy and relevant industry codes.

Although most journalism on a day-to-day basis does not raise data protection concerns, there are some occasions when it does. When this does occur, the power and influence of the press means that processing personal data for journalism may cause substantial harm to individuals.

In addition, an overarching societal harm that may occur is harm to the important public interest that journalism serves. Journalism has a special role to support the free flow of communication and hold the powerful to account. This may be undermined by a lack of public trust arising from, for example, inaccurate news.

This impact assessment identifies instances of harm caused by personal data being processed for journalism. This includes physical harm, material harm (such as financial harm) and non-material harm (such as distress).¹

The rationale for the code is provided by the statutory duty to produce it under s124 DPA 2018. Looking beyond this, the potential to reduce the risk of data protection harms and alignment with industry and government policy objectives provide further evidence for its need.

Impact assessment

The assessment focuses on the incremental impacts of the code (direct or indirect impacts attributable to the code). Impacts that necessarily arise because of the statutory requirement to comply with legislation and for the ICO to produce this code are not considered as incremental impacts.

Generally, it is not possible to quantify the affected groups or provide quantifiable evidence about the code's costs and benefits. The affected groups are broad, the incremental costs vary considerably depending on the circumstances, and the benefits are often intangible.

The code's scope is appropriately broad, although the primary focus is on media organisations and professional journalists. Other affected groups are individuals whose data is processed for journalism and organisations involved in processing personal data for journalism where this is not their main purpose.

The code will also affect the ICO, as the regulator of data protection, and the justice system. Both have statutory responsibilities to take the code into account, where relevant.

The code may also affect individuals and organisations indirectly. For example, through the code's impacts on society-wide harms.

Direct impacts

The direct incremental costs of the code (costs deemed attributable to the code) are limited. The key direct impacts assessed are the costs and benefits of reading through the relevant materials (familiarisation). Although not possible to calculate with certainty, we have estimated an indicative range of £350,000 to £700,000.

The benefits are in helping controllers to comply with existing legislation and providing regulatory certainty. We consider these impacts to be an inevitable consequence of DPA 2018 and the UK GDPR and are therefore not attributable to the code itself.

¹ More Information on Data Protection Harms can be found in the [ICO's Regulatory Policy Methodology Framework](#)

We also assessed specific elements of the code which cover a range of issues such as the code's scope; the special purposes exemption; accountability; and individual's rights.

The assessment finds that impacts of these specific elements are a result of the statutory obligation placed on the Commissioner by s124 of DPA 2018 and are therefore not attributable to the code.

Indirect impacts

Indirect impacts are caused by a change in behaviour or later stage impacts following implementation of the code.² The assessment does not find any significant indirect costs and although it is not possible to rule these out, they are considered to be outweighed by indirect benefits.

The benefits of the code are linked to the objectives and rationale for it in providing:

- additional regulatory certainty;
- building public trust; and
- reducing the risk of harm in the context of data protection and journalism.

The code is only one of the elements necessary to meet these objectives. However, it is not possible to robustly estimate the benefits that could be attributed to the code. Even a minor contribution could bring about significant impacts for both those processing personal data for the purposes of journalism and wider society.

Overall assessment

The code has a strong rationale and aligns well with relevant policy. We generally judge that direct impacts of the code are not incremental. However, there is potential for the code to produce significant beneficial incremental impacts indirectly. We judge that any potential incremental costs are limited and outweighed by these benefits.

² Further discussion on direct and indirect impacts can be found in: Regulatory Policy Committee, RPC case histories – direct and indirect impacts (2019)

2. Background

This document sets out the findings of our initial impact assessment. As part of the ongoing consultation exercise, we are seeking views on both the code and the findings of the assessment. Therefore, we have posed a set of questions to help us develop the impact assessment. You should read these alongside this report.

2.1. Problem under consideration and rationale for intervention

This section provides an overview of the context of the code, the harms to be addressed and the rationale for developing it.

2.1.1. The data protection and journalism code

The data protection and journalism code is a statutory code of practice prepared under section 124 of the DPA 2018. The Information Commissioner was required to prepare the code:

- to provide practical guidance in relation to the processing of personal data for the purposes of journalism in accordance with the requirements of the data protection legislation; and
- such other guidance as considered appropriate to promote good practice in the processing of personal data for the purposes of journalism.

The code does not impose any legal requirements beyond those already in the legislation. It will help controllers to understand their legal obligations under the UK GDPR³ and the DPA 2018 and to comply effectively.

High level objectives of the code

Bearing in mind the requirements set out above, the key objectives of the code are to:

- provide practical guidance to help controllers to comply with data protection legal requirements and good practice when processing personal data for the purposes of journalism;
- build on and update the guidance for the media we published in 2014 to reflect changes to legislation, case law and other developments;

³ The GDPR is retained in domestic law now the transition period has ended, but the UK has the independence to keep the framework under review. The UK GDPR sits alongside an amended version of the DPA 2018. See here for more information: <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/>

- make sure we protect freedom of expression and information, while also protecting privacy, when applying data protection law. This is particularly so regarding the main provision (the special purposes exemption for journalism);
- promote accountability in line with the accountability principle under the UK GDPR, particularly concerning justifying publication in the public interest and accuracy; and
- help build and sustain public trust in the processing of personal data for the purposes of journalism. Ultimately, this supports the crucial public interest role journalism plays in contributing to the free flow of communication and acting as the 'public's watch dog'.

Policy alignment

An important part of the context for the code and its objectives is its alignment with specific areas of policy that the Government is pursuing. The most relevant are described below and demonstrate strong alignment:

The Leveson inquiry

The [Leveson inquiry](#) was a judicial public inquiry into the culture and ethics of the UK press following evidence of phone hacking by News International and other media organisations. It ran from 2011-2012 and was chaired by Lord Justice Leveson.

The inquiry considered the harm caused by the press to ordinary members of the public, people with a public profile and victims of crime, amongst others.

The inquiry found evidence of unethical cultural practices in parts of the UK press. In particular, it found inaccuracy in press reporting and a lack of respect for individual privacy in circumstances where there was no or insufficient public interest justification.

In January 2013, we published [our response to the inquiry](#) and in September 2014, we published [Data protection and journalism: a guide for the media](#). The guidance was produced in response to a formal recommendation to the inquiry.

Part II of the inquiry did not proceed as Government judged that the terms of the second part have largely been met through changes made in response to Part I, both by journalists and through measures such as the Crime and Courts Act 2013⁴ and the creation of the Press Recognition Panel^{5,6}. However, a requirement for the ICO to produce a journalism code of practice was included under section 124 of the DPA 2018 to support future compliance.

⁴ [Crime and Courts Act 2013 - GOV.UK](#)

⁵ [The Royal Charter | Press Recognition Panel \(PRP\)](#)

⁶ [Leveson Consultation Response - GOV.UK](#)

Draft Online Safety Bill

The [Draft Online Safety Bill](#) aims to respond to the risks posed by harmful activity and content online, particularly the increased risks to children.

The bill aims to increase the accountability of technology companies, in line with the significant role they play in people's lives, by introducing a new duty of care.

Managing online harms needs to be balanced against the contribution to economic growth made by digital technology and the importance of protecting freedom of expression. The bill therefore proposes protections for journalism.

We are actively engaging with the Department for Digital, Culture, Media and Sport (DCMS) and Ofcom to ensure consistency.

National Data Strategy

The National Data Strategy is the Government's pro-growth strategy for data. It focuses on the UK building a world-leading data economy, whilst making sure that the public trust how data is used.

The code particularly complements pillar 4 of the strategy 'Responsible data'. This involves making sure that data is used responsibly, in a way that is lawful, secure, fair, ethical, sustainable and accountable. These are key considerations in data protection law, which are discussed in the context of journalism in this code.

One of the code's key objectives is to build and sustain public trust in the processing of personal data for the purposes of journalism, which makes an extremely valuable contribution to democracy and society.

The Cairncross review

In February 2019, the Government published an independent report, [The Cairncross Review](#), about securing a sustainable future for journalism. This acknowledged the economic pressures on journalism operating in a competitive and evolving digital environment.

We have updated the code to reflect the realities of the digital world and the special public interest in freedom of expression and information, whilst being aware of the economic context of the industry. It will support responsible data use and help people to understand the application of data protection law in the digital age. We will continue to engage with industry stakeholders about the practicalities of the code in this context.

Industry codes on press standards

Press standards more generally are dealt with by a number of industry codes of practice and guidelines, including:

- [Independent Press Standards Organisation \(IPSO\) Editors' Code of Practice](#);
- [IMPRESS Standards Code](#);
- [BBC Editorial Guidelines](#); and
- [Ofcom Broadcasting Code](#).

These should be distinguished from the ICO code, which does not concern general press standards. Rather it is limited to journalism in the context of data protection law, as explained above.

The industry codes include considerations about data protection. For example, IPSO's Editor's code covers accuracy and the public interest generally. The ICO code expands on these areas to provide more detailed guidance to the industry in the specific context of data protection.

We consider the industry codes and the ICO's code to be well-aligned and expect them to complement one another. We have spoken to the organisations responsible for industry codes, and we will continue to engage proactively as the code develops.

2.1.2. Data protection harms related to the processing of personal data for the purposes of journalism

As stated in the code, a free press is a fundamental component of democracy and is associated with strong and important public benefits. It is important to balance the benefits of a free press with other rights, such as the right to privacy, which is also fundamental to democracy.

Although most journalism, especially on a day-to-day level, does not raise data protection concerns, there are occasions when it does. When this does occur, the power and influence of the press means that processing personal data for the purposes of journalism may cause substantial harm to individuals. This is due in part to their access to large audiences.

The Leveson inquiry found evidence of unethical cultural practices in parts of the press that caused harm (see above).

The harm to individuals' rights and freedoms can vary in degree and type. In line with damages, as described in Article 82 of the UK GDPR, harms can include:

- **physical harm:** physical injury or other harms to physical health;
- **material harm:** harms that are more easily monetised such as financial harm; or
- **non-material harm:** less tangible harms such as distress.

This means that harm can arise from actual damage and more intangible harm, including any significant economic or social disadvantage. Of course, harms may also fall into more than one of these categories.

There may be a harmful impact on wider society. For example, unfair or unlawful processing of personal data for the purposes of journalism may lead to a loss of public trust. Ultimately, this undermines the important public interest role that journalism serves in our democracy.

The recent [Digital News Report](#) by the Reuters Institute for the Study of Journalism says that only 36% of people trust most news most of the time (the previous figure was just 28%). The UK is 33rd out of the 46 countries involved in the rankings based on a sample size of about 2,000 with surveys conducted by You Gov.⁷

While the specific causes of this general lack of trust are unclear, and there is disparity between trust in different news brands, the report's author says that:

"...in almost all countries we see audiences placing a greater premium on accurate and reliable news sources".

We have identified some relevant examples of harm to individuals when personal data is processed for the purposes of journalism using desk-based research. These examples are illustrative only and should not be viewed as an exhaustive or hierarchical list.

Bodily or emotional harm

In some cases, processing personal data for the purposes of journalism poses risks to people's physical or emotional health or both. For public figures or people with a public role, the harm may accumulate over time because of persistent or frequent invasions of privacy. This may put people's mental health under significant strain, and in extreme cases may cause or contribute to suicidal thoughts.

Financial loss and damage to reputation

This includes loss of employment or income. This material harm is commonly linked to reputational harm. Financial loss may also occur because of steps taken to mitigate harm, such as pursuing legal action, which is expensive.

Example: Sir Cliff Richard

Sir Cliff Richard was awarded damages following the BBC's decision to name him as a suspect in an ongoing police investigation and to broadcast a search of his home. His evidence included reference to a planned album being put on hold, cancelled public appearances, shelved book deals, retailers refusing to stock merchandise, as well as significant legal costs. Sir Cliff Richard's evidence also

⁷ <https://pressgazette.co.uk/trust-in-uk-news-reuters-institute-digital-news-report/>

made it clear that these events seriously affected him physically and mentally.⁸

Stereotyping, racism, and discrimination

The inclusion of specific types of personal data in stories may contribute to stereotyping, racism and discrimination.

A key principle under the UK GDPR is that processing of personal data is minimised. This includes not processing irrelevant or excessive personal data. Personal data must also be accurate.

Processing of personal data must be fair and lawful. Special category data includes personal data revealing or concerning information about racial or ethnic origin, or religious or philosophical beliefs. This type of data needs more protection because it is particularly sensitive.

Unlawful privacy intrusion

Unlawful privacy intrusion occurs when personal data is processed in a way that is not in line with the key data protection principles. Such harms may vary significantly in severity and the impact may be material or non-material.

Unlawful privacy intrusion in the context of journalism, especially investigative journalism, may take the form of covert surveillance, subterfuge or similarly intrusive methods. Some activities of this nature are criminal offences. Legal actions concerning phone hacking of public figures by parts of the press in the past are still ongoing.⁹

Unlawful privacy intrusion violates the right to privacy that is a protected human right. It may cause an individual to feel a loss of control over their personal data and interfere with their right to autonomy, integrity, dignity and respect. There are likely to be other harmful consequences as well, such as distress or reputational damage.

Fear of the harmful consequences of unlawful privacy intrusion may itself lead to harm because it may prevent individuals from acting as they normally would. In other words, there may be a 'chilling effect' on people's behaviour.

Example: Naomi Campbell

In [Naomi Campbell v MGN Ltd. \[2004\] UKHL 22](#), photographs were taken of Miss Campbell in a public street leaving a Narcotics Anonymous meeting.

The judge said that the mere fact of covert photography is not sufficient to make information private but he found that the newspaper had misused private

⁸ Sir Cliff Richard OBE v the BBC [2018] EWHC 1837 (Ch)

⁹ <https://www.theguardian.com/media/2020/may/20/kris-marshall-settles-claim-over-news-of-the-world-phone-hacking>

information in this case. He said that in context, the picture added to the information conveyed by the story and the potential harm by making Miss Campbell think she was being followed or betrayed, and deterring her from going back to the same place for treatment.

Prejudice to the course of justice

There is a strong public interest in ensuring that the process of justice is fair. As a general starting point, suspects in investigations have a reasonable expectation of privacy. A breach of privacy may cause a variety of the types of harm we have described, including reputational damage. There may also be a risk of prejudice to the course of justice. For example, people may be deterred from reporting crimes or there may be a prejudicial impact on legal proceedings.

Example: Sand Van Roy

Associated Newspapers paid substantial damages to actor Sand Van Roy for revealing her identity as a complainant in a rape case against the French film director Luc Besson following unlawful coverage in the French press. Sand Van Roy said that she hoped victims of crime would not be deterred by fear of their identity being publicised.¹⁰

2.1.3. Summary of rationale for intervention

We have a statutory duty to produce the code under section 124 of the DPA 2018. However, beyond this, the code is likely to reduce the risk and severity of data protection harms. It is also well-aligned with government policy and industry codes. Taken together, there are strong reasons for this policy intervention.

2.2. Approach to the code

The development of the code has been informed by responses to an [initial call for views](#) published in 2019, to which 39 organisations responded including media organisations, trade associations and individuals. We have also engaged in more detail with the most relevant organisations. We have published a [summary of the call for views responses](#) alongside individual responses as appropriate. We are also [publicly consulting on the draft code](#) for 12 weeks. Additionally, we are consulting a variety of stakeholders on an ongoing basis.

¹⁰ <https://www.theguardian.com/media/2021/may/21/associated-newspapers-pays-damages-for-revealing-sand-van-roy-as-luc-besson-accuser>

2.3. Scope of the code

The code contains guidance for those processing personal data for journalism who must comply with the UK GDPR and DPA 2018.

The code defines journalism broadly in line with key case law. It is flexible in its approach to the definition of journalism allowing it to be assessed on a case-by-case basis, drawing on multiple factors to decide if activities constitute journalism.

As acknowledged in the code, it is often straightforward to determine whether personal data is being processed for the purposes of journalism by newspapers, magazines or broadcasters, for example. Closer consideration of the specific circumstances may be needed in the case of non-professional journalism, such as citizen journalism, and other online services (eg on-demand services, search engines, content aggregation services and services that host third party contributions).

2.4. Affected groups

Groups affected by the code are wide and varied, reflecting the broad definition of journalism above.

The code is primarily focused on controllers whose primary purpose for processing personal data is journalism, including newspapers, magazines and broadcasters. However, it is also relevant to non-professionals and other controllers that may sometimes process personal data for journalism.

The code affects individuals whose personal data is processed for journalism, the ICO as the regulator of the data protection legislation, and courts and tribunals, that are required to take account of the code, where relevant.

The code may also impact individuals and organisations indirectly. This includes the impact of society-wide harms and benefits as well as impacts on organisations that supply or interact with journalists.

Professional journalists and media organisations

It is estimated that there are around 96,000 professional journalists in the UK.¹¹ It is not possible to estimate the total number of media organisations as their structures and activities are often complex. The ICO data protection register has 1,040 individuals or organisations registered under 'Journalism' as well as 1,321 under 'Television and radio' which could provide a conservative lower-end estimate.¹² This affected group has been under significant economic pressures¹³

¹¹ National Council for the Training of Journalists, Diversity in Journalism, May 2021

¹² ICO, Analysis of the Data Protection Register as at February 2021

¹³ [THE CAIRNCROSS REVIEW A sustainable future for journalism \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/90444/the-cairncross-review-a-sustainable-future-for-journalism.pdf)

and the assessment recognises that the sector is particularly sensitive to additional costs or burdens.

Other organisations or individuals involved in the processing of personal data for the purposes of journalism

It is not possible to quantify the size of this group given how wide and varied these individuals and organisations are, and that journalism is not necessarily their only or main purpose. This group includes some online services and citizen journalists, for example.

Individuals whose data is processed for the purposes of journalism

It is not possible to quantify the size of this group of individuals given the very broad scope of journalism. We have no way of estimating how many individuals' data has been processed for the purposes of journalism or will be processed in the future.

The Information Commissioner's Office

The ICO will be affected, as the regulator of data protection legislation. In accordance with section 127(4), the Commissioner must take the provisions of this code into account in determining a question arising in legal proceedings where relevant.

The ICO will also need to provide advice, promote good practice and assess compliance with the code. There are some limited enforcement provisions for journalism under the DPA 2018. However, in recognition of the special public interest in freedom of expression, the ICO's powers are significantly restricted in this respect.

The DPA 2018 includes a statutory requirement for a review of processing of personal data for the purposes of journalism under section 178. The code sets out the standards against which we will review processing for journalism in practice once it comes into force. The ICO must report to the Secretary of State about this.

Justice system

The justice system will be affected because, in accordance with section 127(3) of the DPA 2018, a court or tribunal must take the provisions of the code into account in legal proceedings, where relevant.

Wider society

It is not possible to quantify this affected group.

2.5. Approach to the impact assessment

We have assessed the impacts using cost-benefit analysis, which aims to identify the full range of impacts of the code. However it should be noted that it is not practical nor necessary for the purpose of this impact assessment to undertake a forensic analysis of all of the code's implications.

In identifying the potential impacts of the code it is important to distinguish between:

- incremental impacts – these are impacts that can be attributed to the code itself;
- impacts of the requirements of section 124 of the DPA 2018 – these are not incremental to the code; and
- impacts of requirements of the UK GDPR and the DPA 2018 – these are not incremental to the code because controllers are expected to be compliant with these requirements already.

It is not always possible to categorise impacts distinctly, but our assessment focuses on the incremental impacts of the code. These incremental impacts may be direct or indirect:¹⁴

- **Direct impacts:** these are 'first round' impacts that are generally immediate and unavoidable with relatively few steps in the chain of logic between the introduction of the measure and the impact taking place.
- **Indirect impacts:** these are 'second round' impacts that are often the result of changes in behaviour or reallocations of resources following the immediate impact of the introduction of the measure.

Accordingly, our assessment is split into two main parts considering the code's direct and indirect incremental impacts.

To assess direct impacts, we have focus on key parts of the code that may impact any of the affected groups. We present each element in turn and consider, overall, how likely it is that there would be an incremental impact. We then consider the potential indirect impacts as a whole and how likely it is there would be an incremental impact.

The evidence base primarily constitutes desk-based research, responses to the call for evidence, and previous analysis of related issues. We adopted a similarly

¹⁴ Further discussion of direct and indirect impacts can be found in section 1 or in: Regulatory Policy Committee, RPC case histories – direct and indirect impacts (2019).

proportionate approach to complete the impact assessments for the Data sharing code of practice¹⁵ and the Age-appropriate design code of practice.¹⁶

Since the code was mandated by Parliament in s124 DPA 2018, the Commissioner did not have an option to consider alternative action or regulatory intervention. For this reason, this assessment does not consider alternative options to drafting a statutory code of practice. It is simply an evaluation of the introduction of the code against the counterfactual explained below.

Counterfactual

The counterfactual in an impact assessment is the baseline against which you can estimate the incremental impacts of introducing a policy. If the code was not introduced then the underlying data protection legislation would continue to apply and form the counterfactual for the purposes of this assessment.

In line with impact assessment guidance¹⁷, the assessment assumes compliance both with existing legislation and guidance within the code in the absence of specific evidence to suggest otherwise. This simplifies the assessment, but it is not intended to suggest that there is total compliance. If we did identify any specific lack of compliance, the code would help controllers to improve.

The code does not impose any additional legal requirements, which limits the code's incremental impacts over and above that of the counterfactual. This is discussed further in section 3.

Quantification

Quantified analysis of the impacts is particularly challenging for the code because of its wide ranging scope and the difficulty in quantifying the affected groups, as explained above.

Calculating the incremental cost to controllers is also complex because the nature of these costs varies considerably depending on the different factors, for example:

- how sophisticated and mature the controller's existing data protection systems and processes are;
- the nature of the activities;
- the processing associated with those activities; and
- the level of risk to individuals.

It is similarly challenging to quantify many of the code's benefits, such as:

- reductions in harm;
- increased controller understanding; or

¹⁵ ICO, Data sharing code of practice – Impact assessment (2021).

¹⁶ ICO, Age Appropriate Design: a code of practice for online services – Impact assessment (2020).

¹⁷ BEIS, Business Impact Target: appraisal of guidance (2017).

- increased trust amongst the public because of their intangible nature.

Our analysis therefore focuses primarily on non-monetised impacts. However, where possible, we have provided high level quantitative analysis to indicate scale.

2.6. Regulatory constraints

The Commissioner has drafted the code within the following regulatory constraints:

- her remit, powers and duties as set out in the UK GDPR and the DPA 2018; and
- the obligations placed upon her by section 124 of the DPA 2018.

3. Costs and benefits of the code

In this section, we consider the code's potential costs and benefits. Our aim is to understand whether there are likely to be significant impacts on affected groups (both positive and negative) and to judge the code's overall impact on society.

We draw on a mixture of quantitative and qualitative evidence but, as noted above, our analysis is limited by the evidence available.

The analysis of effects is split into direct and indirect impacts as set out in section [2.5](#).¹⁸

Direct impacts are given the same weight as indirect impacts. The only distinction is that the indirect impacts are considered collectively because these are not sufficiently distinct to justify individual analysis.

The impacts are assessed under the following headings which then feed into our conclusion on the code's overall impact on society:

- **Cost** - a discussion of the related costs that could bring about significant impacts to affected groups.
- **Benefits** - as with costs.
- **Categorisation of impact** - our assessment of whether there is likely to be a significant net cost or benefit as well as the categorisation of the impact (ie are the impacts incremental?).

3.1. Direct costs and benefits of the code

We identified and analysed direct impacts of the code in the form of familiarisation with the code itself and the specific elements that it contains below.

3.1.1. Familiarisation

Controllers are expected to familiarise themselves with the code, although the extent to which this is required will vary between controllers (as discussed in section [2.5](#)).

Cost-benefit analysis

Costs

Controllers will incur a direct cost as a result of the introduction of the code because of the time taken to read and become familiar with the code. These are

¹⁸Further discussion on direct and indirect impacts can be found in: Regulatory Policy Committee, RPC case histories – direct and indirect impacts (2019)

referred to as familiarisation costs.¹⁹ The code contains guidance for all controllers processing personal data for the purposes of journalism. However, it may not be necessary for all controllers to familiarise themselves with the whole code. For example, this may be the case for smaller organisations that undertake lower risk processing.

The indicative familiarisation costs are estimated to be between £350,000 to £700,000, using the information available on the media industry and the likely time taken to read it. However, this is only to indicate the scale of this impact. It is not possible to accurately estimate the number of organisations or individuals that would need to familiarise themselves with the code.

It should be noted that further work is ongoing into the development of supplementary guidance to lessen the load on organisations in terms of familiarisation costs. This could include shorter guidance that is specifically targeted at smaller organisations. This means any estimates of the costs could be an overstatement at this point. There are further details of the method used to estimate familiarisation costs in [Annex A](#).

Benefits

The direct benefits to controllers of becoming familiar with the code are that it:

- helps them to understand their existing legal obligations under data protection law;
- helps them to comply with these obligations effectively;
- reduces the potential harm to individuals; and
- increases confidence to process data responsibly (discussed further under indirect costs and benefits in section [3.2](#)).

Categorisation of impact

The impact on controllers of needing to become familiar with the code is the natural consequence of the requirement to produce a statutory code of practice under section 124 of the DPA 2018.

Section 124 is not explicit about the precise content and length of the code and enables some judgement on what the Commissioner considers appropriate. However, this discretion does not necessarily imply that there is an incremental impact. A similar assessment was also made for the impacts of familiarisation of the data sharing code and age-appropriate design code.²⁰

Our assessment acknowledges that the issue of attribution here is complex. However, we have assumed that even if elements of the code could be perceived

¹⁹ For guidance on familiarisation costs, see: BEIS, BIT Appraisal of Guidance: Assessments for Regulator-Issued Guidance (2017)

²⁰ ICO, Age Appropriate Design: a code of practice for online services – Impact assessment (2020) see section 3.1.

to be incremental, these are limited and likely to be at least balanced by the benefits to controllers.

3.1.2. Specific elements of the code

We have identified below the key parts of the code which may cause direct impacts. We then assessed the potential for incremental costs or benefits to controllers and other affected groups.

Code's scope

Although the primary focus on the code is media organisations and professional journalists whose main purpose is to publish journalistic material, it does apply more broadly. The 'Who is this code for?' section acknowledges that we may require further consideration in this broader area to understand the code's application. This is particularly the case for online services.

This part of the code aims to help people understand the code's application in the context of the digital age. This is increasingly important for journalism (see policy alignment above). It includes factors that may be relevant and illustrative examples to provide more certainty.

The code also includes a section on the broad definition of journalism (see What is journalism? section of the code). This refers to key case law and indicates what factors may be relevant to deciding whether personal data is being processed for journalism.

Special purposes exemption

The code provides guidance on the application of the special purposes exemption for journalism (see What is the special purposes exemption? section of the code).

We include guidance on the meaning of "with a view to publication". This builds on our earlier media guidance to clarify the circumstances in which processing of personal data post-publication can be covered by this exemption, especially regarding complaints about journalism.

Drawing on relevant privacy case law, the code also provides greater clarity about the meaning of "reasonable belief" in the context of this exemption.

Accountability

The code is clear that controllers must be able to demonstrate their compliance, known as the accountability principle (see the section of the code "Be able to demonstrate compliance")

The code refers to the ICO's separate tool known as the Accountability Framework. This is to help controllers to assess whether they have appropriate data protection measures in place and whether they would be able to

demonstrate compliance. The 'About this code' section is clear that any links to other guidance are there to be helpful and do not form part of the code itself.

We recognise the challenging environment in which journalists operate. Although the concept of accountability is itself risk-based and proportionate, we have specifically considered its impact on the special public interest in freedom of expression. For example, we include guidance to help journalists to manage the impacts of data protection impact assessments (DPIAs). We highlight that although compulsory, it is not necessary to do a DPIA for every story. We provide guidance to help make this requirement for high-risk processing feasible and proportionate in this special context, recognising the need to be flexible.

In the section 'Demonstrating your decision-making' about the special purposes exemption, we also include further guidance recognising the special context. For example, this section discusses using risk as a basic guide to support proportionate record-keeping. It does not impose a prescriptive approach which would not be appropriate.

Justifying the use of personal data

Guidance on the principle of processing personal data lawfully, fairly and transparently is included in the code. This draws on various aspects of broader privacy case law that is relevant to data protection. The potential overlap and the benefits to be derived from appreciating these is explained in the section of the code 'How does this code relate to other laws affecting the media?'.

Accuracy principle

The code includes guidance on the key data protection principle that controllers must take reasonable steps to make sure that personal data is accurate.

This section of the code includes guidance about some practical measures that controllers could consider. As mentioned above, the accountability principle that underpins these considerations is a flexible and adaptable principle. These are not prescriptive requirements but are indicative of what may be reasonable steps to take depending on the circumstances.

This part of the guidance again recognises the special context and that in some circumstances it may be difficult to undertake normal accuracy checks. The guide refers to industry guidance to support controller's considerations in such circumstances. Accuracy is obviously key to wider industry guidance, and we believe this section is well aligned (see Policy alignment). Industry guidance is flagged specifically for further reading, showing the complementary nature of this code.

Storage limitation

The code contains guidance on the data protection principle that personal data must not be kept for longer than necessary.

There is guidance about dealing with research and background materials. This is in keeping with the requirement to consider the special public interest in freedom of expression and the specific context in which journalists operate. It specifically acknowledges that it may be difficult in the context of journalism to know when, or if, a piece of information will become useful in the future. The code is clear that this should be considered and justifiable to a proportionate extent where possible.

Third party roles and responsibilities

The code includes guidance to help controllers to assess the data protection responsibilities that they and third parties have when processing personal data.

The code clarifies that private investigators, who may be used by journalists for information, are often likely to be acting as controllers in their own right. This is because of the level of independence they are likely to have to determine the means and purposes of the processing.

Guidance in the code about data sharing is aligned with the separate ICO Data sharing code of practice²¹ produced under the DPA 2018. For example, this includes that it is good practice to use data sharing agreements in certain circumstances. It is also clear, in line with the Data sharing code, that it is generally appropriate to make enquiries and checks about personal data that is received from third parties when this is used for journalism.

Individuals' rights

The code contains practical guidance to help support individual rights. This is in line with ICO's existing guidance. For example, good practice recommendations that also appear in the Guide to the UK GDPR²² include:

- personal data should be restricted while accuracy is in dispute;
- a note should be put on the system to explain that the individual disputes the accuracy of the data; and
- records of mistakes should be kept providing that those records are themselves accurate.

Regarding the latter, we add to this that in the specific context of journalism, these are often called corrections, which may take a variety of forms. We acknowledge that where these are very minor, a record is not likely to be proportionate. We also acknowledge that the practical realities of correcting inaccurate personal data online may pose more challenges.

The code includes guidance about the limitations of the right to erasure, particularly in the context of news archives which are very important in our

²¹ <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/>

²² [Guide to the UK General Data Protection Regulation \(UK GDPR\) | ICO](#)

democracy. This is in line with stakeholder feedback from the code's call for views.

Cost benefit analysis

Costs

The key elements of the code set out above are not additional obligations or impositions over and above existing legislation and what would be required generally to comply effectively with the legislation. The code is not overly prescriptive and it is clear where there are steps or considerations that may be helpful. We have also considered the special public interest in protecting freedom of expression.

Where controllers perceive that there are additional obligations or burdens, it is likely that there were existing issues with compliance. In these limited instances, controllers may need to implement additional measures or restrict activities. However, the costs of these will be significantly outweighed by the benefits of improved compliance both to the controllers themselves and also to wider society. This impact is to some extent an implicit and inevitable aspect of the code's function because it exists to improve compliance.

Benefits

The greater clarity provided by the code is likely to benefit controllers through increased regulatory certainty and efficiency. This in turn is likely to reduce some of the costs associated with compliance or non-compliance. For example, better compliance may reduce costs incurred through legal challenges.

We are required to reflect the special public interest in protecting freedom of expression and information when producing the code. Where there is scope for some discretion, we have considered the context in which journalists need to operate. The code will help journalists to understand the flexibility permitted within the law in this special area, and to act proportionately to comply with data protection.

The specific parts of the code we have highlighted should also help the ICO to review compliance and investigate where necessary. For example, a good quality accuracy checklist or other relevant documentation could mean we are able to assess compliance more quickly and efficiently.

Categorisation of impacts

The impacts described above are a direct result of the statutory requirement within section 124 of DPA 2018. We are required to develop a code that supports the understanding of the legislation and good practice when personal data is processed for journalism. Therefore, the potential for incremental impacts is limited and the direct impacts of the code are assessed as neutral.

3.2. Indirect costs and benefits of the code

3.2.1. Costs

Although it is not possible to rule out indirect costs, it is difficult to identify any that are likely to bring about significant indirect impacts that are incremental to the code.²³

Additional restrictions or burdens (perceived or actual) could place pressure on the freedom of the press. However, we do not consider that the code places any significant restrictions (or indeed freedoms) that go over and above existing legislation and what would generally be reasonable to comply effectively. As such, there is no substantive evidence of indirect costs.

3.2.2. Benefits

The indirect benefits of the code are primarily that it is likely to increase confidence and regulatory certainty. In turn, increased compliance is likely to lead to a reduction in the risk of harm to individuals when personal data is used for journalism.

Increased confidence

There is a high degree of uncertainty around impacts related to increased confidence. It is not possible to make a robust estimate of how incremental these impacts are.

The code will provide greater regulatory certainty and clarity because it is tailored specifically to the context of journalism. It is therefore likely to increase confidence within the industry generally. This will support the freedom of the press, particularly in circumstances where there may be more uncertainty about how to balance freedom of expression and privacy rights. This may increase efficiency, which is particularly important in the context of journalism given its competitive nature and the increased challenges of digital publication.

Increased accountability may result in higher public trust levels, which are reported to be comparatively low.²⁴ This may increase public engagement with journalism. This indirectly improves the public interest benefits that journalism aims to serve that are fundamental to our democracy. For example, the free flow of communications and public accountability of people in powerful positions.

Increased regulatory certainty and confidence may result in more consistent understanding and application of the law across organisations. The code is a free to use resource by the data protection regulator that is tailored specifically to the needs of this sector. There will also be complementary resources such as a Quick

²³ Additional information may be provided through the consultation exercise

²⁴ <https://pressgazette.co.uk/trust-in-uk-news-reuters-institute-digital-news-report/>

guide. This may increase competition and may also support smaller organisations particularly to participate more fully. Additional confidence may also result in innovation and economic growth.

Where organisations are not aware that they are processing personal data for the purposes of journalism, they may benefit from the code's guidance and knowledge of data protection provisions which protect freedom of expression.

Reduction of data protection harms related to the processing of personal data for journalism

As illustrated in section [2.1.2](#), data protection harms may occur when personal data is processed for the purposes of journalism. Although the harms presented do not necessarily point to specific areas of non-compliance, the examples provided do correlate to key principles of data protection law. The code also includes guidance on key areas such as considering the public interest and making sure that personal data is accurate.

The guidance is likely to contribute to reducing the risk and severity of the types of harms we have identified in this assessment. Even a small contribution to minimising harms would be helpful in view of the potentially very damaging consequences for individuals.

The code encourages controllers to demonstrate accountability throughout which is a key data protection principle introduced by the UK GDPR. There are benefits to putting in place appropriate, risk-based data protection measures and being able to demonstrate this. These are that controllers manage risks and harms associated with the processing of personal data. In turn, this increases confidence, both within and outside the industry.

3.2.3. Categorisation of impact

The code is likely to offer significant indirect benefits to society. This is because it is likely to provide greater regulatory certainty, increase confidence, and reduce harms. These beneficial impacts are judged to be incremental to the code.

However, it is difficult to draw firm conclusions about the likelihood and scale of the code's indirect benefits. This is because the indirect impacts are often intangible, vary according to the circumstances and depend on behaviour change.

3.3. Overall assessment of direct and indirect impacts

The direct and indirect costs identified in this assessment are generally judged not to be incremental. This is primarily because of the terms of the statutory requirement to produce the code and the need for controllers to comply with the legislation.

Where there may be some discretion, we have considered:

- responses to the call for views;
- the special public interest in freedom of expression and information; and
- the circumstances in which journalists often operate.

We welcome input and evidence on these issues in response to the ongoing consultation.

It is difficult to quantify evidence on costs. However, there is limited potential for incremental costs, in view of the legislative background to the code and the steps taken by the ICO to produce it.

We consider that the code is likely to have some significant indirect incremental beneficial impacts. This is due to increased regulatory certainty, confidence, and reducing the risk and severity of harms in the context of data protection and journalism. However, it is difficult to draw firm conclusions about the likelihood and scale of these benefits, which largely depend on behaviour change.

Overall, any costs associated with the code are considered to be significantly outweighed by the incremental societal benefits that the code may produce. These benefits align strongly with specific policies and complement existing industry codes.

Annex A: Estimating familiarisation costs

This annex sets out the approach taken to estimating familiarisation costs for the code, which follows a standard approach.

Organisations or individuals in scope

As with identifying affected groups in section 2.4, it is not possible to produce a robust estimate of the organisations that would be expected to familiarise themselves with the code. However, we can provide an indicative range to demonstrate the type of costs related to familiarisation.

As a starting point we have used the total number of organisations or individuals on the data protection register related to journalism and television and radio broadcasting. As of February 2021, this was 2,361. Some organisations or individuals may not appear on the data protection register, either due to exemptions or a poor understanding of their obligations. It is therefore reasonable to view this as a lower-end estimate.

Given the lack of information to make a robust estimate, we have doubled this number to provide an indicative upper-end, resulting in a range of **2,361 to 4,722**. This appears reasonable, particularly as not all organisations read guidance materials, although this may be less likely in the case of codes of practice with statutory effect.²⁵

Familiarisation costs

Drawing on impact assessment guidance²⁶, we have estimated the total time for reading the code at five hours and 33 minutes. This is based on a word count of around 25,000 words and a Fleisch reading ease score of 42.

For the purposes of this assessment, we have made the simplifying and conservative assumption that each organisation or individual will read the code, in its entirety, once. It should be noted that this is not a recommendation on how organisations or individuals should familiarise themselves with the code, as this will differ on a case-by-case basis. Some will need to read significantly less, and a small subset may need multiple people to read it. It is only intended to provide an indicative average for the assessment of familiarisation costs.

The impact of familiarisation on organisations can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings (ASHE).²⁷ Assuming that the relevant occupational group is 'Managers, Directors and Senior Officials', the 2019 median hourly earnings (excluding overtime) for this group is £21.90.

²⁵ See BEIS, BIT Appraisal of guidance: assessments of regulator-issues guidance (2017) sections 2.3 and 2.4

²⁶ BEIS, BIT Appraisal of Guidance: Assessments for Regulator-Issued Guidance (2017)

²⁷ See https://ec.europa.eu/eurostat/statistics-explained/index.php/Hourly_labour_costs and <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/bulletins/annualsurveyofhoursandearnings/2020>

This hourly cost is up-rated for non-wage costs using the latest figures from Eurostat and in line with Regulatory Policy Committee guidance,²⁸ resulting in an uplift of 22% and an hourly cost of £26.71. Using this hourly cost, and making the simplifying assumption of one individual being responsible for familiarisation for each of the relevant organisations²⁹, the total estimated familiarisation costs for the code ranges from £350,000 to £700,000.

²⁸ See guidance in https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/RPC_short_guidance_note_-_Implementation_costs_August_2019.pdf

²⁹ In reality there may be one individual responsible for understanding the code for multiple organisations or multiple individuals in one organisation but in the absence of data to make a precise estimate, the simplifying assumption is deemed appropriate