

<b>Title:</b> Data protection and journalism code impact assessment <b>Lead department or agency:</b> Information Commissioner's Office/DCMS	<b>Impact Assessment (IA)</b>
	<b>Date:</b> July 2022
	<b>Stage:</b> Draft
	<b>Source of intervention:</b> Legislative
	<b>Type of measure:</b> Statutory code of practice
<b>Summary: intervention and options</b>	

**What is the problem under consideration? Why is regulatory action or intervention necessary?**

The Information Commissioner was required to prepare the Data protection and journalism code under section 124 (s124) of the Data Protection Act 2018 (DPA 2018) to provide practical guidance about processing personal data for the purposes of journalism in accordance with the requirements of the data protection legislation; and other guidance, as considered appropriate to promote good practice when processing personal data for the purposes of journalism.

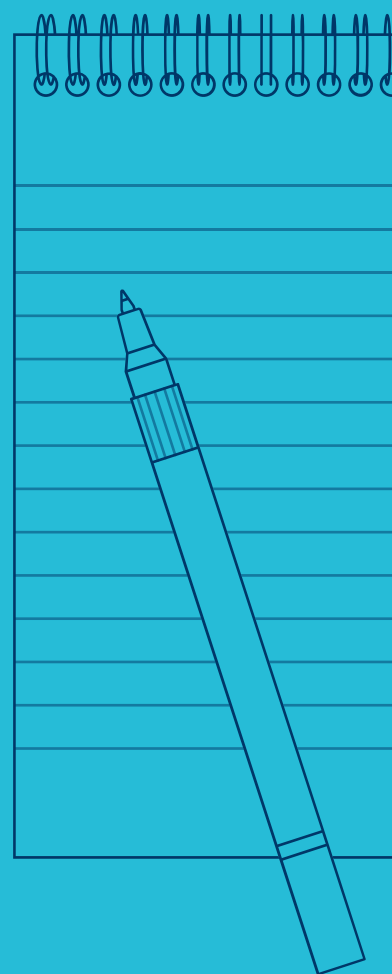
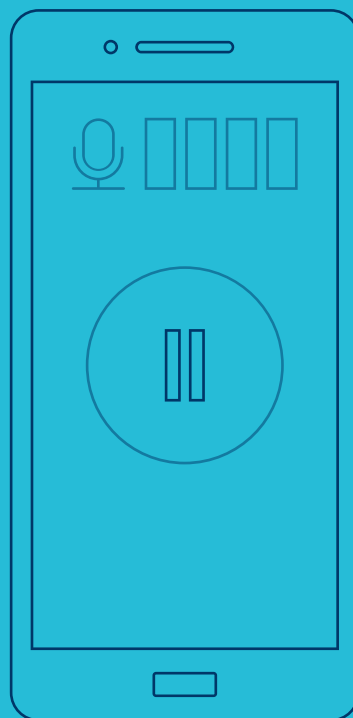
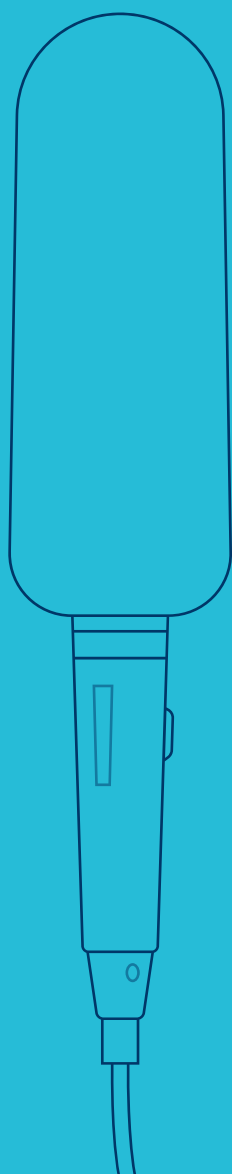
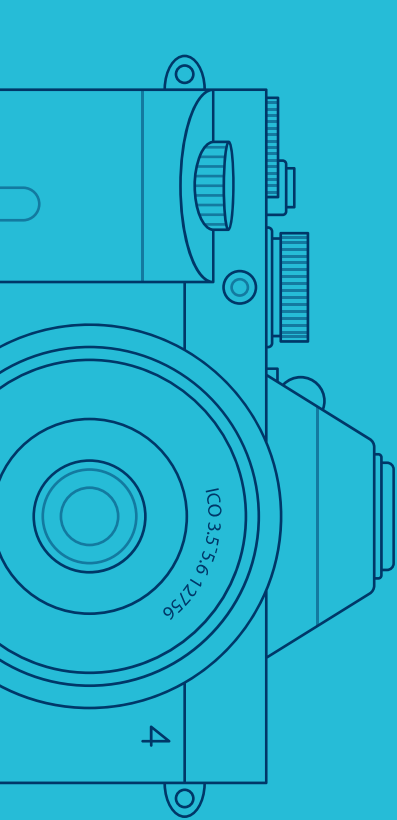
**What policy options has the Information Commissioner considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence base)**

As the code and its remit was mandated by Parliament in s124 DPA 2018, it was not appropriate for the Commissioner to consider any alternative course of action. To the extent that the Commissioner had discretion about which issues to cover or how to interpret them within the code, these are described in the body of this assessment.

**Will the code be reviewed?**

The code will be kept under review in line with good regulatory practice, with s124 (2) DPA 2018 allowing the Commissioner to make amendments or lay a replacement code.

# Data protection and journalism code impact assessment



## Contents

Executive summary.....	3
1. Introduction .....	7
2. Approach to the impact assessment .....	8
3. Context .....	11
3.1. Social and economic context.....	11
3.2. Policy context.....	12
3.3. Data protection harms related to processing personal data for the purposes of journalism .....	15
3.4. Rationale for intervention .....	19
4. The code.....	21
4.1. Approach to the code .....	22
4.2. Scope of the code .....	23
4.3. Affected groups .....	23
4.4. Regulatory constraints.....	26
5. Costs and benefits of the code.....	27
5.1. Direct costs and benefits of the code .....	28
5.2. Indirect costs and benefits of the code .....	35
5.3. Overall assessment of direct and indirect impacts .....	37
Annex A: Estimating familiarisation costs .....	39

## Executive summary

This impact assessment sets out the benefits and costs associated with the Data protection and journalism code of practice (the code). It draws on evidence including desk-based research, responses to an initial call for evidence, responses to our consultation, and previous analysis of related issues.

### Overall assessment

The code has a strong rationale and aligns well with relevant policy. Our overall assessment of the code is illustrated in Table 1. We generally consider that the direct impacts of the code do not add to the impacts which naturally arise as a result of the legislation (ie they are not attributable to the code). However, there is potential for the code to produce significant indirect, beneficial additional impacts. We consider that any potential additional costs are limited and outweighed by these benefits.

Table 1: Summary of Impacts

<b>Impact*</b>	<b>Positive, neutral or negative**</b>	<b>Level of attribution to the code</b>
<b>Reading the code or familiarisation</b>	Neutral	Not attributed to the code
<b>Specific elements of the code</b>	Neutral	Not attributed to the code
<b>Indirect impacts</b>	Positive	Attributed to the code

\*Descriptions of each of the impacts are provided in detail in Section 5

\*\*Positive (a net benefit); negative (a net cost); neutral (no impact)

### Context

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.

The Data Protection Act 2018 (DPA 2018) requires the Information Commissioner’s Office (ICO) to prepare a statutory code of practice. This is 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.<sup>1</sup> In particular, the code's key purpose is to protect freedom of expression, while also protecting people's right to privacy and data protection.

We consider that the code is well-aligned with current published policy that the Government and industry bodies are pursuing and work is ongoing to strengthen alignment with policy under development. The policies reviewed include: The Leveson inquiry; the National data strategy; the draft Online safety bill; data protection reform and relevant industry codes.

Although most journalism on a day-to-day basis does not lead to data protection harms or other concerns, there are some occasions when it does. When this does occur, the power and influence of the press means that harms stemming from processing personal data for journalism may be substantial.

In addition, an overarching societal harm that may occur is harm to the important public interest that journalism serves. Journalism has a special role in supporting the free flow of communication and holding 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).<sup>2</sup>

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 published government policy objectives provide further evidence for its need.

### **Cost-benefit analysis**

The assessment focuses on the impacts of the code that are additional to those of the legislation (direct or indirect impacts that can be attributed 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 to be additional 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 additional costs vary considerably depending on the circumstances, and the benefits are often intangible. It is also not possible to estimate how impacts might vary according to the characteristics of people or

---

<sup>1</sup> [Data protection and journalism: a guide for the media \(ico.org.uk\)](https://ico.org.uk)

<sup>2</sup> For more information on data protection harms, see [Data protection harms | ICO](#).

## Data protection and journalism code impact assessment

organisations within the affected groups (eg income level or geographical location). We are therefore unable to identify distributional impacts.<sup>3</sup>

The code's scope is appropriately broad, although the primary focus is on media organisations and professional journalists. Other affected groups are people 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 people and organisations indirectly. For example, through the code's impacts on society-wide harms. These impacts may also vary for different groups across society.

### Direct impacts

The direct additional costs of the code (costs we attribute to the code) are limited. The key direct impacts assessed are the costs and benefits of reading through the code, known as familiarisation. Although not possible to calculate with certainty, we have estimated an indicative range of £210,000 to £420,000 in familiarisation costs.

Where there is the potential for a perceived or actual additional burden for controllers, we believe this is balanced by the benefit of familiarisation in helping controllers to comply with existing legislation and providing greater regulatory certainty. We consider the costs of familiarisation are an inevitable consequence of DPA 2018 and the UK GDPR. These costs cannot therefore be attributed to the ICO's development of the code.

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 people's rights. These were the aspects of the code we considered most impactful.

We do not consider that these impacts can be attributed to the code because they arise from the Commissioner's duty to produce the code under section 124 of the DPA 2018.

### Indirect impacts

Indirect impacts are caused by a change in behaviour or later stage impacts once the code is implemented.<sup>4</sup> We do not consider that there are any significant

---

<sup>3</sup> More information on distributional impacts can be found in [HM Treasury's Green Book](#).

<sup>4</sup> Further discussion on direct and indirect impacts can be found in: [Regulatory Policy Committee, RPC case histories – direct and indirect impacts \(2019\)](#).

indirect costs. Although it is not possible to rule these out, we conclude that they are likely 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 and it is difficult to isolate the code's contribution to indirect impacts. As such, it is not possible to robustly estimate the benefits that could be attributed to the code. However, even a minor contribution could bring about significant impacts for both those processing personal data for the purposes of journalism and wider society.

## 1. Introduction

This document sets out the findings from our assessment of the impact of the code. The purpose of the impact assessment is to:

- provide an objective view of the costs and benefits of the code;
- guide and inform the design of the code and potential mitigation; measures; and
- set a baseline for future review and evaluation activity.

The report is structured as follows.

- **Section 2 – Approach to the impact assessment:** setting out the approach we took to assess the impacts of the code and the limitations of the impact assessment.
- **Section 3 – Context:** setting out the economic, social and political context for the code as well as the rationale for producing it.
- **Section 4 – The code:** overview of the objectives of the code, the approach to the code and the affected groups.
- **Section 5 – Costs and benefits of the code:** the cost benefit analysis covering both direct and indirect impacts of the code.
- **Annex:** details on the estimated familiarisation costs.



## 2. Approach to the impact assessment

We have assessed the impacts using cost-benefit analysis, which aims to identify the full range of impacts by assessing both the costs and benefits of the code. However, it is not practical nor necessary to consider in detail all the code's implications, in line with proportionality principles.

Our approach follows [HM Treasury's Green Book](#), [Regulatory Policy Committee](#), and [Business Impact Target](#) guidance on best practice for impact assessments.

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

- additional impacts that can be attributed to the code: these impacts are affected by how the ICO chooses to develop the code; or
- additional impacts that are not attributed to the code: these impacts are not affected by how the ICO chooses to develop the code. They simply arise from the legislative requirements. This includes the requirements under section 124 of the DPA 2018, including to create the code, and the general requirements of the UK GDPR and the DPA 2018. Controllers are already expected to comply with these requirements:  
<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

It is not always possible to categorise impacts distinctly, but our assessment identifies additional impacts and then focuses on those that can be attributed to the code.<sup>5</sup>

- **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.

Our assessment is split into two main parts considering the code's direct and indirect additional impacts.

To assess direct impacts, we 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 additional impact that can be attributed to the code. We then consider the potential indirect impacts as a whole and how likely it is there would be an additional impact.

---

<sup>5</sup> For more information on attribution see [OECD – Causality problems](#)

<sup>6</sup> For further discussion on direct and indirect impacts see [Regulatory Policy Committee, RPC case histories – direct and indirect impacts \(2019\)](#).

We collected evidence for the impact assessment using the following methods and sources:

- desk-based research and previous analysis of related issues;
- responses to the call for views; and
- responses to the public consultation.

We published a draft impact assessment alongside the code as part of the [public consultation](#). As expected, the feedback mainly focused on the code itself, which included comments about the code's impact. We have updated this assessment to take account of changes to specific parts of the code itself, but this has not changed our overall assessment.

Where there were specific comments, this has helped us to clarify parts of the impact assessment. This includes sensitivity analysis which is explained in detail in HM Treasury's Green Book.<sup>7</sup>

As the code is a statutory requirement, the Commissioner did not have an option to consider alternative action or regulatory intervention. For this reason, we have only considered the impact of the code in our assessment.

We adopted a similarly proportionate approach to complete the impact assessments for the Data sharing code of practice<sup>8</sup> and the Age-appropriate design code of practice.<sup>9</sup>

### Counterfactual

To help us measure the impact of the code, we have taken as our starting point what the situation is now, known as the counterfactual. The counterfactual is the baseline against which we estimate the additional impacts of introducing the code. If the code was not introduced, then the underlying data protection legislation and existing guidance would continue to apply and form the counterfactual for the purposes of this assessment.

In line with impact assessment guidance<sup>10</sup>, we assume 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.

As a statutory code of practice, it does not impose any additional legal obligations, which limits the code's additional impacts over and above that of the counterfactual. This is discussed further in Section 5.

---

<sup>7</sup> See para 5.59 of [HM Treasury's Green Book](#) for more information on sensitivity analysis.

<sup>8</sup> [ICO, Data sharing code of practice – Impact assessment \(2021\)](#).

<sup>9</sup> [ICO, Age appropriate design: a code of practice for online services – Impact assessment \(2020\)](#).

<sup>10</sup> [BEIS, Business Impact Target: appraisal of guidance \(2017\)](#).

### Monetising impacts

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.

Calculating the additional 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 people.

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

- reductions in harm;
- increased controller understanding; or
- 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.

### Uncertainty, risk and optimism bias

As set out in the Treasury's Greenbook, it is necessary to consider the significant levels of uncertainty surrounding the impacts of the code. Although optimism bias is typically only considered in capital projects<sup>11</sup>, we understand that there can be a tendency to overestimate engagement with guidance. To account for and demonstrate the implications of any potential bias, we have provided sensitivity analysis for the impacts we have been able to quantify.<sup>12</sup> This tests the sensitivity of impact estimates to changes in assumptions and is provided in [Annex A](#).

---

<sup>11</sup> See section 2.6.27 of [Department for Finance Northern Ireland's Risk and Optimism Bias Guidance](#).

<sup>12</sup> See para 5.59 of HM Treasury's Green Book for more information on sensitivity analysis.

## 3. Context

This section sets out the economic, social and political context for processing personal data for the purposes of journalism, the potential harms that can arise, as well as the rationale for the code.

### 3.1. Social and economic context

As set out in the code, freedom of expression and information is a fundamental human right that makes a vital contribution to our democracy alongside privacy, which is also central to broader data protection law.

A free press is a crucial part of a democracy because of its role in informing the public and holding powerful people to account.

“Each and every day we are reminded of how vital the information [the press, journalists and media workers] provides is for democracy, the promotion and protection of human rights, fighting corruption, sustainable development and preserving international peace and security.”

United Nations General Assembly, UNESCO General Conference and the Human Rights Council

On the other hand, a degree of privacy and limits on intrusion by the state and others with power is necessary for citizens’ physical, mental and social well-being and development.

The importance of both freedom of expression and privacy is recognised by the UK courts and the European Court of Human Rights. More broadly, privacy and data protection are two rights enshrined in the EU Charter of Fundamental Rights, which is reflected in the UK GDPR and the DPA 2018.

As well as delivering an important service to society, journalism also plays an important role in the economy. The ONS estimates that there are 110,000 professional journalists and editors in the UK, equivalent to 0.3% of all employment nationally.<sup>13</sup> Although it is not possible to accurately estimate the number of organisations whose main purpose is journalism, the ICO’s Data protection register has 6,566 organisations registered under ‘Journalism’ and ‘TV and radio’.

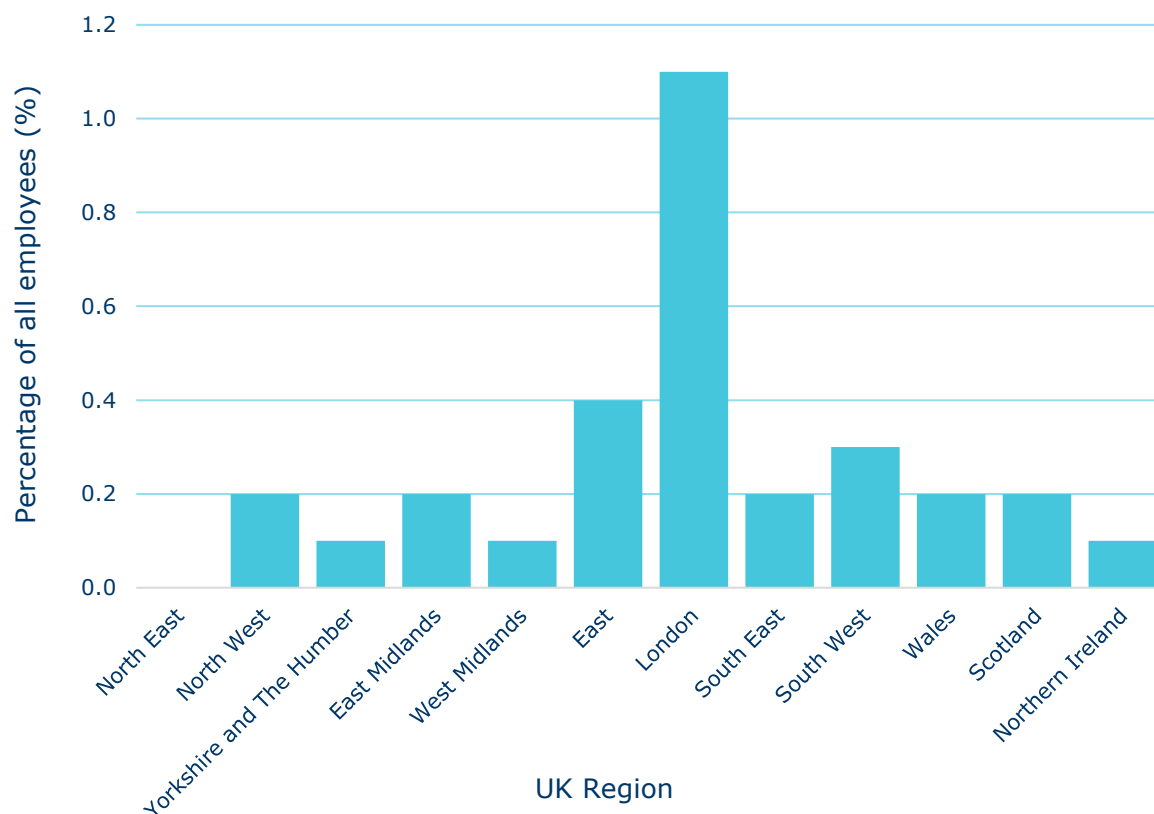
However, employment in the journalism industry is not evenly distributed across UK regions. Approximately half (47%) of these jobs are based in London with another 20% in the East of England and South East of England. Figure 1 shows that jobs in the sector make up a relatively significant percentage of all jobs in

---

<sup>13</sup> ONS Annual Population Survey – Employment by Occupation, Jan to Dec 2021.

London (1.1%), the East of England (0.4%) and the South West of England (0.3%). This suggests these regions are more sensitive to changes in the sector and impacts are unlikely to be evenly distributed.

Figure 1: Journalists as a proportion of employment by region, December 2021



Source: ONS Annual Population Survey – regional – employment by occupation, Jan to Dec 2021; Journalists defined as SOC 2417: Journalists, newspaper and periodical editors.

The media eco-system in the UK and globally has been transformed by the increased digitalisation of the economy and through a series of highly impactful events in recent years.

During the Covid-19 pandemic, the main television journalism outlets, the BBC, ITV and Sky News all increased their weekly reach. In contrast, the reach of national and local newspapers has fallen by an average of 10%, while freesheets has fallen by 40%.<sup>14</sup> While digital subscriptions have continued to rise, only a small minority (8%) regularly pay for online news.

### 3.2. Policy context

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. There are some changes expected in the policy landscape in the near future, however, at the

<sup>14</sup> [United Kingdom | Reuters Institute for the Study of Journalism \(ox.ac.uk\)](#).

## Data protection and journalism code impact assessment

time of drafting, the relevant policy context (including relevant inquiry findings) is as follows:

### 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 2013](#) and the creation of the [Press Recognition Panel](#).<sup>15</sup>

However, requirements to support future compliance were introduced, including a requirement for the ICO to produce a journalism code of practice under section 124 of the DPA 2018 as well as a review of processing personal data for the purposes of journalism under section 178 of DPA 2018.

### 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.

---

<sup>15</sup> [Leveson consultation response - GOV.UK](#).

## Data protection and journalism code impact assessment

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 involved them in the public consultation exercise which has allowed us to improve the code's alignment.

### Policy in development

There are also a number of relevant proposals being made by Government. It is not yet clear how, when or whether they will come into effect but we have attempted to outline alignment at a high-level.

- Data reform: Department for Digital, Culture, Media and Sport (DCMS) recently ran a consultation, [Data: a new direction](#), proposing reforms to data protection legislation to which [we have published a response](#). As the data protection authority, the ICO has been working closely with DCMS to understand the implications of the proposed reforms.
- Online safety: 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 DCMS and Ofcom to ensure consistency where appropriate. We have also [responded to the call for evidence](#).
- Human Rights Reform: Government recently consulted on proposals for [reform of the Human Rights Act](#). The code is underpinned by human rights focusing particularly on freedom of expression and privacy. The code aims to help organisations and people to balance these rights effectively. Alignment with proposals is not clear at this early stage, but implementation of the code will take into account any changes as they arise.
- Defamation: Government is [considering reform of the Defamation Act 2013](#) to strengthen the public interest defence. This refers to subject access requests as a potential means of legal abuse of process. The code aligns with the spirit of these proposals in explaining how to apply the special purposes exemption for journalism and the route for requests to be refused if they are manifestly unfounded or excessive. The code's supporting notes highlight more detailed guidance we have published about these protections.

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

Although most journalism, especially on a day-to-day basis, 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 people. This is due in part to its 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 people's 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.<sup>16</sup>

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 in 2021 (up from 28% in 2020, but down 14% on 2015).<sup>17</sup>

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".

Of course, there are numerous positive examples of journalism serving the public interest by holding powerful politicians to account and exposing wrongdoing. For example, in 2009 the Daily Telegraph exposed the wide spread abuse of the MPs expenses system.<sup>18</sup> The code takes into account the special public interest in freedom of expression and a free press.

However, to aid understanding of some of the harms the code seeks to address, we have provided some examples below. This list is not exhaustive or hierarchical.

### **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

---

<sup>16</sup> For more information on data protection harms, see [Data protection harms | ICO](#).

<sup>17</sup> [United Kingdom | Reuters Institute for the Study of Journalism \(ox.ac.uk\)](#).

<sup>18</sup> [MPs' expenses: The scandal that changed Britain - BBC News](#).

persistent or frequent invasions of privacy. This may put people's mental health under significant strain.

### **Example: Can't pay? We'll take it away!**

Channel 5 filmed and broadcast two claimants being evicted from their home in a programme called 'Can't Pay? We'll take it away!'.

The programme disclosed private information, including personal data, to millions of viewers, without sufficient justification. The judge found that the footage showed the claimants at their lowest ebb, being evicted without prior notice, in a state of shock and very distressed. Damages were awarded for the intrusion into their privacy.

### **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 expensive legal action.

### **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.

Sir Cliff Richard's 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. His evidence also made it clear that these events seriously affected him physically and mentally.<sup>19</sup>

### **Stereotyping, racism, and discrimination**

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

A key principle of the UK GDPR is to minimise processing of personal data. 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.

---

<sup>19</sup> Sir Cliff Richard OBE v the BBC [2018] EWHC 1837 (Ch).

### 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.<sup>20</sup>

Unlawful privacy intrusion violates the right to privacy that is a protected human right. It may cause a person 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 people 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 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.

### Confidentially and prejudice to the course of justice

There is a strong public interest in ensuring that the process of justice is fair and that legitimate duties of confidence are respected.

The legitimate starting point is that, pre-charge, suspects have a reasonable expectation of privacy in state investigations. A breach of privacy and confidentiality of this nature may cause a variety of the types of harm we have described, including reputational damage. There may also be a risk of prejudice

---

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

to the course of justice. For example, there may be a prejudicial impact on legal proceedings or people may be deterred from reporting crimes.

### **Example: Bloomberg LP v ZXC[2022] UKSC 5**

This case concerned Bloomberg's publication of an article based on information from a confidential letter of request sent by a UK law enforcement body to a foreign state.

The Supreme Court found that the suspect, pre-charge, had a reasonable expectation of privacy. It said that the reason for this starting point is that:

"...publication of such information ordinarily causes damage to the person's reputation together with harm to multiple aspects of the person's physical and social identify such as the right to personal development, and the right to establish and develop relationships with other human beings and the outside world...The harm and damage can on occasions be irremediable and profound". p71.

The court also acknowledged the strong public interest in observing duties of confidence generally and, more specifically, when it could prejudice an ongoing state investigation.

### **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.<sup>21</sup>

## 3.4. 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, such as those identified above. It is also well-aligned with published Government policy and industry codes. Taken together, there are strong reasons for this policy intervention.

Figure 2: Summary of context and rationale for the code

### **Context**

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

## Data protection and journalism code impact assessment

### Social and economic context

- Importance of freedom of expression and right to privacy
- Journalism industry is a significant employer
- Shift to digital formats due to the COVID-19 pandemic
- Employment mostly concentrated in London

### Policy context

- Importance of Leveson inquiry
- National data strategy
- The Cairncross review
- Policy in development:
  - Data reform
  - Online safety
  - Human rights
  - Defamation

### Data protection harms

- Bodily or emotional harm
- Financial loss and damage to reputation
- Stereotyping, racism and discrimination
- Unlawful privacy intrusion
- Confidentiality and prejudice to the course of justice

### Rationale

- Statutory duty to produce the code under s124 DPA 2018
- Existence of harms that result from processing
- Public policy seeking to address harms identified and enable safe processing

Source: ICO, Economic Analysis team

## 4. The 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 about processing personal data for the purposes of journalism in accordance with the requirements of the data protection legislation; and
- other guidance to promote good practice in processing personal data for the purposes of journalism, where appropriate.

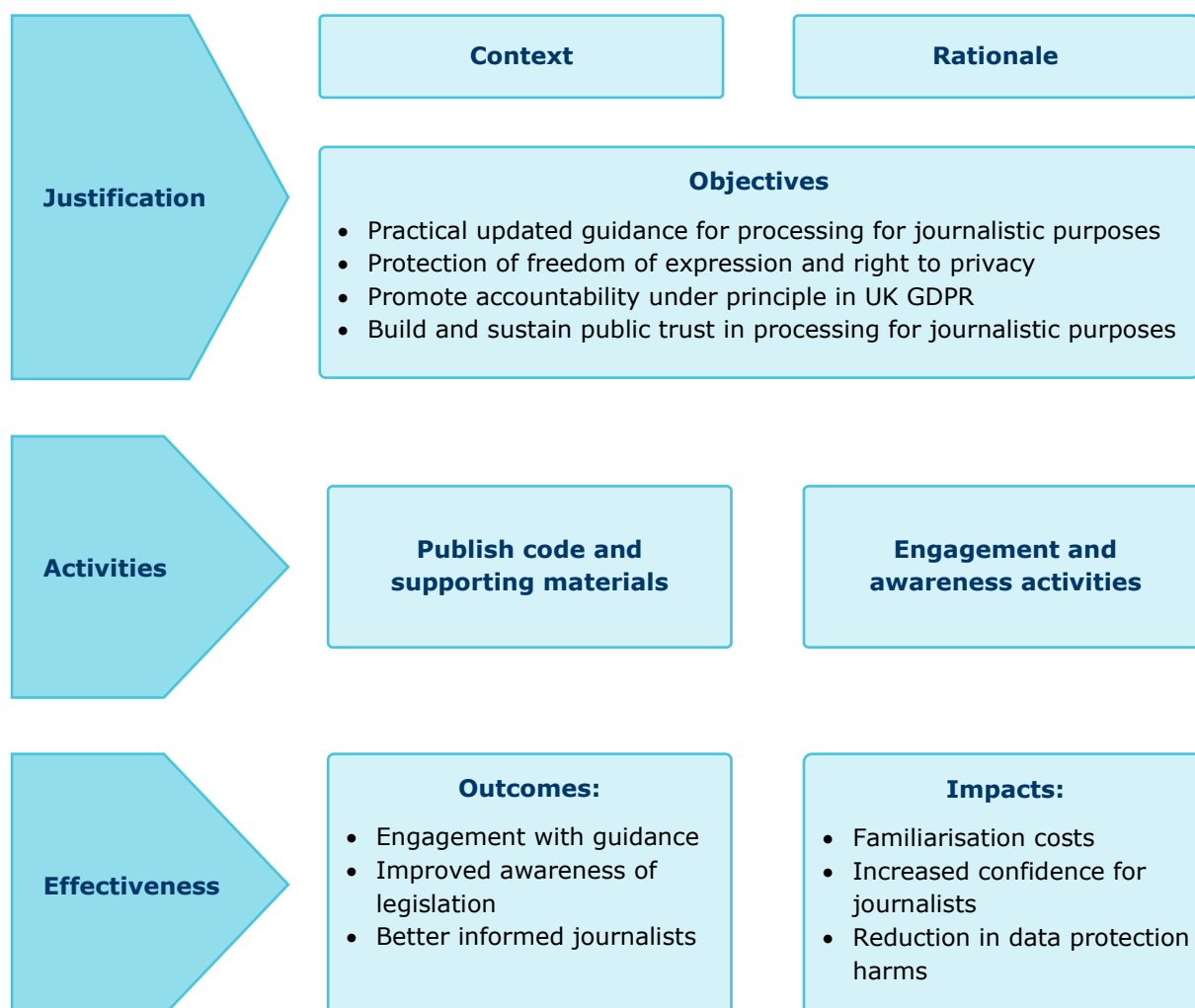
The code does not impose any legal requirements beyond those already in the legislation. It will help controllers to understand their legal obligations under the UK GDPR and the DPA 2018 and to comply effectively.

### **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 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;
- make sure we protect freedom of expression and information, while also protecting privacy, when applying data protection law. In particular, 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 processing 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'.

Figure 3: Code logic chain



Source: ICO, Economic Analysis team

#### 4.1. Approach to the code

Our development of the code was informed by responses to an [initial call for views](#) published in 2019, to which 39 organisations responded including media organisations, trade associations and the public.

We also published a draft of the code for public consultation in September 2021, as well as running more targeted engagement, such as workshops. We received 31 responses to the written consultation and more than 75 participants attended the workshops.

We made a series of significant changes to the original draft in response. These changes are intended to reduce adverse impacts on affected groups and increase the benefits of the code, including:

- shifting the audience for the code itself from being aimed largely at senior editorial staff and those with specific data protection expertise to include a broader audience covering more day-to-day journalistic staff;
- reducing the code as far as possible to core principles and rules;
- removing significant amounts of background information, such as case law references, to a set of supporting reference notes to be published alongside the code, but which will not form part of the code itself. This provides more ease and flexibility when we need to update any content;
- introducing a clear typology of 'must' 'should' and 'could' to more clearly indicate parts of the code that are legal requirements and good practice; and
- considering and incorporating the more detailed and technical legal points raised, as appropriate.

We have published a summary of the feedback along with individual responses, with some redactions as appropriate. The summary also includes ICO comments indicating the changes we have made to the draft.

### 4.2. 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 help people decide if personal data is being used for 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.

### 4.3. 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 people 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 people 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.

Figure 4: Affected groups



Source: ICO, Economic Analysis team

### Professional journalists and media organisations

It is estimated that there are 110,000 professional journalists and editors in the UK, equivalent to 0.3% of all person employed nationally.<sup>22</sup> Employment in journalism related industries is not evenly distributed across UK regions. Around half (47%) of these jobs are based in London, with another 20% in the East and South East.

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 2,434 people or organisations registered under 'Journalism' as well as 4,132 under 'Television and radio', which could provide a conservative lower-end estimate.<sup>23</sup> This affected group has been under significant economic pressure<sup>24</sup>

<sup>22</sup> ONS Annual Population Survey – Employment by occupation, Jan to Dec 2021.

<sup>23</sup> ICO, Analysis of the Data protection register as at February 2021.

<sup>24</sup> [THE CAJRCROSS REVIEW A sustainable future for journalism \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/91444/the-caj-cross-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 people involved in processing personal data for the purposes of journalism**

It is not possible to quantify the size of this group given how wide and varied these people 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.

### **People whose data is processed for the purposes of journalism**

It is not possible to quantify the size of this group of people given the very broad scope of journalism. We have no way of estimating how many people's 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) of the DPA 2018, 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**

There could be wider impacts on people whose personal data is not processed for the purposes of journalism. These may arise either as a result of the impact on people who consume journalism or because of broader societal impacts, such as trust in journalism or prejudice to the course of justice.

There could also be impacts on organisations and businesses that are not journalists but whose activities are connected to them, for example, businesses that supply journalism organisations. This could include law firms, website hosting providers or freelancers, such as photographers, who serve organisations involved in processing personal data for the purposes of journalism.

### 4.4. Regulatory constraints

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

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

## 5. Costs and benefits of the code

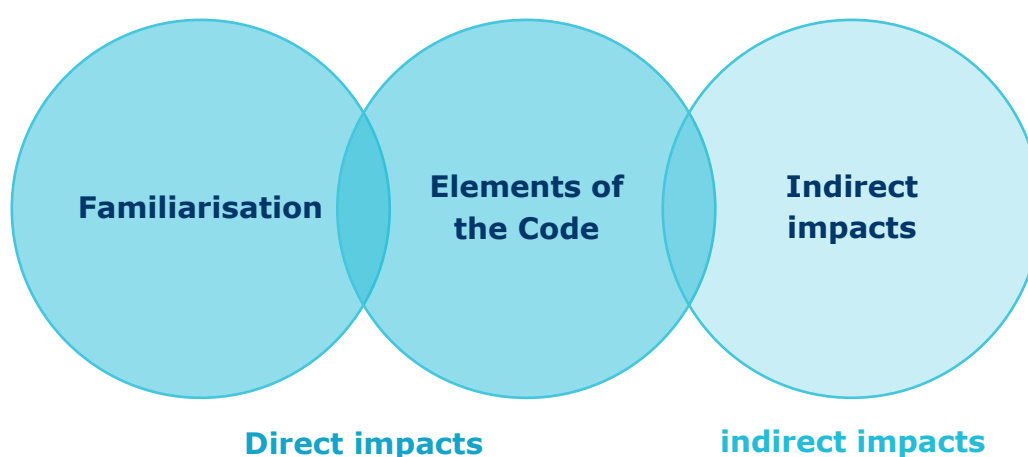
In this section, we consider the code's potential costs and benefits. Our aim is to understand whether there are likely to be significant impacts on affected groups (both positive and negative) and to judge the code's overall impact on society.

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.<sup>25</sup>

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.

### Impacts considered in this assessment



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:** where possible, additional impacts are categorised as negative (a net cost), positive (a net benefit), or neutral and either attributable or not attributable to the code.

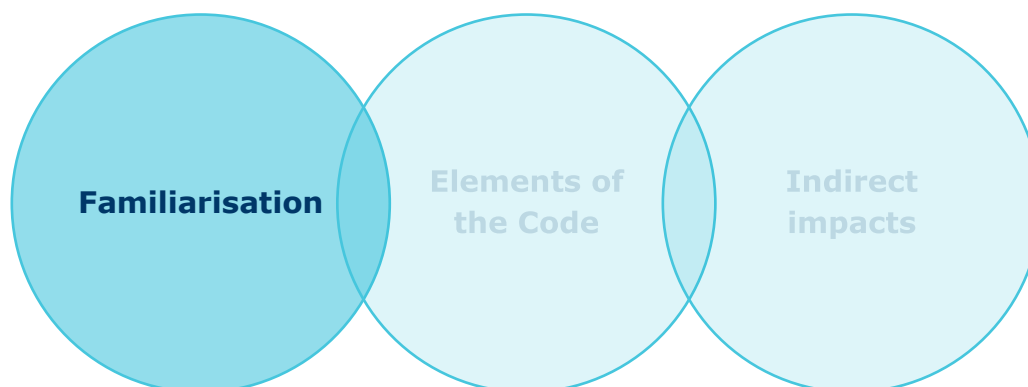
---

<sup>25</sup>For further discussion on direct and indirect impacts, see [Regulatory Policy Committee, RPC case histories – direct and indirect impacts \(2019\)](#).

## 5.1. 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.

### 5.1.1. 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 4.3).

The code will be supported by reference notes that are not part of the familiarisation considered here, as they will not be laid before Parliament.<sup>26</sup> The supporting notes refer to key legal provisions, case law examples and further reading.

We have also developed quick reference guides that are aimed at day-to-day journalism. In the future, we plan to develop further resources specifically supporting smaller organisations and individuals. These materials are considered as mitigation in providing a range of options for controllers to help them comply with the relevant legislation.

### Cost-benefit analysis of familiarisation

#### 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 it. These are referred to as familiarisation costs.<sup>27</sup> 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

---

<sup>26</sup> The analysis is currently restricted to the code itself but will be adjusted to include the mitigating impact of the supporting documents once these are finalised.

<sup>27</sup> For guidance on familiarisation costs, see BEIS, BIT Appraisal of Guidance: Assessments for Regulator-Issued Guidance (2017).

## Data protection and journalism code impact assessment

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 £210,000 to £420,000. However, this is only to indicate the scale of this impact in aggregate. The costs are estimated using the best available information on the number of organisations in the media industry and the likely time taken to read it. These estimates can change significantly depending on the estimated number of organisations in scope. See [Annex A](#) for more detail on the implications of our estimates.

We recognise that the level of engagement with the code will vary significantly across different media organisations. For example, large organisations may engage multiple professionals and organise staff training to become familiar with the code; other smaller organisations may devote significantly less time.

It is not possible to accurately estimate the number of organisations or people that will need to familiarise themselves with the code, and as such the figures provided are an indicative estimate only.

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 the public; and
- increases confidence to process data responsibly (discussed further under indirect costs and benefits in Section 5.2). This leads to a more effective media, better flows of information to the public and higher levels of trust.

### Categorisation of impact

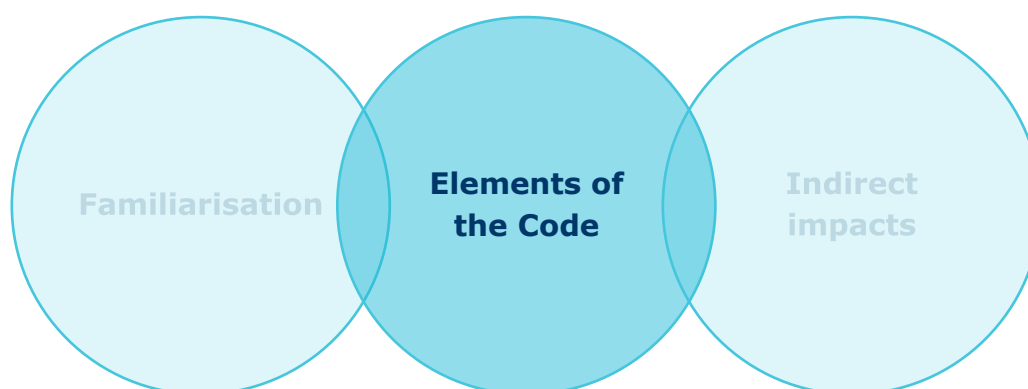
The impact on controllers of needing to become familiar with the code is the natural consequence of the requirement to produce a statutory code of practice under section 124 of the DPA 2018.

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 additional

impact. A similar assessment was also made for the impacts of familiarisation of the data sharing code and age-appropriate design code.<sup>28</sup>

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 to be additional, these are limited and likely to be at least balanced by the benefits to controllers. In the absence of further evidence, the impacts are assessed as **neutral** and **not attributable to the code**.

### 5.1.2. 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 additional 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.

For example, journalism may be carried out by other organisations or people, such as those posting journalistic material online (sometimes known as citizen journalists). Online services which include journalistic material produced by someone else can also be covered by the code, if editorial control goes beyond moderation.

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

---

<sup>28</sup> ICO, Age appropriate design: a code of practice for online services – Impact assessment (2020) see section 3.1.

### Special purposes exemption

The code provides guidance on the application of the special purposes exemption for journalism.

We include guidance on the meaning of “with a view to publication”. This builds on our earlier media guidance, clarifying the breadth of this part of the exemption and indicating the circumstances in which journalists may apply it.

Drawing on relevant privacy case law, the code also provides greater clarity about the meaning of “reasonable belief” in the context of this exemption and carrying out the public interest balancing exercise.

The code includes further guidance on the meaning of “incompatible” in the context of this exemption, including in circumstances where this may be less obvious.

### Accountability

The code is clear that controllers must be able to demonstrate their compliance, known as the accountability principle.

The code refers to the ICO’s separate tool known as the Accountability framework. This is to help controllers 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. The concept of accountability is risk-based and proportionate, so the code includes practical details to support journalism. For example, there is guidance about how to assess risk and make use of existing processes.

The code also includes guidance on undertaking compulsory risk-assessments when using personal data is likely to cause a high risk, known as Data protection impact assessments (DPIAs). However, we highlight that it is not necessary to do a DPIA for every story and that there is significant flexibility surrounding how to carry out this requirement in practice. The code includes guidance to help journalists assess when there is likely to be a high risk.

The code recognises the special context of journalism. It helps journalists to understand the ways in which they could demonstrate the requirement to have a “reasonable belief”, which include keeping a proportionate record of the decision. The code highlights the key role of risk as a key factor to support proportionate record-keeping. It does not impose a prescriptive approach, which would not be appropriate.

### Using personal data fairly, lawfully and transparently



## Data protection and journalism code impact assessment

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 legislation and case law that is relevant to data protection, although actual case examples are set out in supporting notes.

We explain in the notes that there are some similarities between data protection and other privacy laws that can support the consideration of data protection law. However, we are also clear that each law is distinct and serves different purposes.

### 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.

Accuracy is obviously key to wider industry guidance, and we believe this section is well-aligned and complements other codes and guidelines (see Section 3.2). This includes guidance about considering reasonable checks, the impact of the source of data used, and the importance of separating facts, opinions and putting data into its appropriate context.

This section of the code includes guidance about some practical measures that controllers could consider to demonstrate accountability. As mentioned above, the accountability principle that underpins these considerations is flexible and risk-based. These are not prescriptive requirements, but options to help journalists consider the ways in which they could demonstrate compliance. This varies depending on the circumstances.

### 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. The code acknowledges that such information is vital to journalism and that controllers are best placed to judge how long to keep information based on journalistic experience. The code includes some factors that controllers could consider to help with this, but no prescriptive requirements.

### 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 helps journalists to understand the difference between controllers, joint controllers and processors in plain, practical language.

Guidance in the code about data sharing is aligned with the separate ICO Data sharing code of practice<sup>29</sup> produced under the DPA 2018. For example, this includes guidance 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.

### People's rights

The code contains practical guidance to help support people's rights. This is in line with ICO's existing guidance. For example, good practice recommendations that also appear in the Guide to the UK GDPR<sup>30</sup> include:

- factors to help controllers to assess whether a request is "manifestly unfounded or excessive";
- personal data could be restricted while accuracy is in dispute when the person has not specifically requested it; and
- a note could be added to explain that the person disputes the accuracy of the data.

Controllers should consider whether it is appropriate to add a note when a correction has been made to ensure that records are not misleading. In the context of journalism, these are often called corrections, which may take a variety of forms. We acknowledge that where these are very minor, for example, when there has been a typographical mistake, it is usually reasonable to simply edit this.

As requested by stakeholders during the code's call for views and consultation, the code includes guidance about the right to erasure, particularly around the in-built protection for freedom of expression and information. In line with case law, the code recognises the importance of news archives and the special public interest role they play in helping people to understand and access information. The code is clear that this is generally a weighty factor in favour of not erasing data from news archives.

The code also acknowledges that there is precedent in human rights law for requiring anonymisation of a digital archive and it refers to the criteria that has been used to consider whether this is proportionate.

## Cost benefit analysis of the specific elements of the code

### 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 distinguishes between legal requirements and good practice,

---

<sup>29</sup> <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/>.

<sup>30</sup> [Guide to the UK General Data Protection Regulation \(UK GDPR\) | ICO](#).

and the relative importance of good practice points. 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.

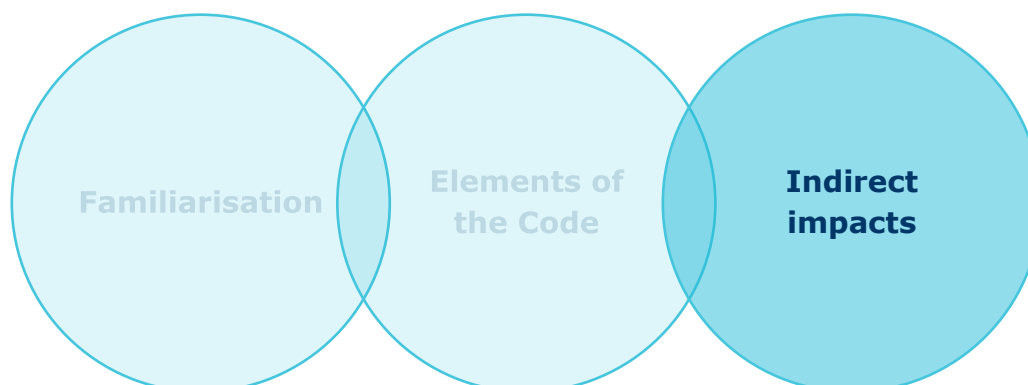
We are required to reflect the special public interest in protecting freedom of expression and information when producing the code. Where there is scope for some discretion, we have considered the context in which journalists need to operate. This has been informed by our extensive engagement with stakeholders, including an initial call for views, a public consultation on the draft code and a series of targeted workshops. The code will help journalists to understand the flexibility permitted within the law in this special area, act proportionately, and comply with data protection.

Parts of the code should also help the ICO to review compliance and investigate where necessary. For example, the code gives example of good accountability practices which is likely to help us 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 additional impacts is limited and the direct impacts of the code are assessed as **neutral** and **not attributable to the code**.

## 5.2. Indirect costs and benefits of the code



### Costs

Although it is not possible to rule out indirect costs, it is difficult to identify any that are likely to be significant and attributable to the code.

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 attributable indirect costs.

### 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 people 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 additional 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.<sup>31</sup> 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 guide. It 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 3.3, 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 that are relevant to journalism, 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 people.

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.

### **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

---

<sup>31</sup> [United Kingdom | Reuters Institute for the Study of Journalism \(ox.ac.uk\)](https://www.reutersinstitute.org.uk/our-work/reports-and-publications).

reduce harms. The indirect impact of the code is assessed as **positive** and **attributable 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.

### 5.3. Overall assessment of direct and indirect impacts

The direct and indirect impacts identified in this assessment are summarised in Table 1 below.

Table 1: Summary of Impacts

<b>Additional impacts</b>	<b>Positive, neutral or negative</b>	<b>Attributable to the code</b>
Familiarisation	Neutral	Not attributable
Specific elements	Neutral	Not attributable
Indirect impacts	Positive	Attributable

Source: ICO, Economic Analysis team

We consider that the majority of impacts are not attributable to the code. 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 and public consultation;
- the special public interest in freedom of expression and information; and
- the circumstances in which journalists often operate.

There is limited potential for additional 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 additional 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.

There was not enough evidence to assess how impacts would be distributed amongst different groups and as such we were not able to specifically identify any distributional impacts.

## Data protection and journalism code impact assessment

Overall, any costs associated with the code are considered to be significantly outweighed by the additional 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 estimate familiarisation costs for the code, which follows a standard approach. This is currently restricted to the code itself but we will adjust it to include the mitigating impact of the supporting documents once these are finalised.

### Organisations or people in scope

As with identifying affected groups in section 4.3, 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 people on the data protection register related to journalism and television and radio broadcasting. As of May 2022, this was 6,566. Some organisations or people 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 **6,566 to 13,132**. 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.<sup>32</sup>

### Familiarisation costs

Drawing on impact assessment guidance<sup>33</sup>, we have estimated the total time for reading the code at one hour and 22 minutes. This is based on a word count of around 5,000 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 person will read the code once in its entirety. However, this is only intended to provide an indicative average for the assessment of familiarisation costs. It is not a recommendation on how organisations or people 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.

The impact of familiarisation on organisations can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings (ASHE).<sup>34</sup> Assuming

---

<sup>32</sup> See BEIS, BIT Appraisal of guidance: assessments of regulator-issues guidance (2017) sections 2.3 and 2.4.

<sup>33</sup> BEIS, BIT Appraisal of Guidance: Assessments for Regulator-Issued Guidance (2017).

<sup>34</sup> See [https://ec.europa.eu/eurostat/statistics-explained/index.php/Hourly\\_labour\\_costs](https://ec.europa.eu/eurostat/statistics-explained/index.php/Hourly_labour_costs) and [Employee earnings in the UK - Office for National Statistics \(ons.gov.uk\)](https://www.ons.gov.uk/employment-and-labour-markets/earnings-and-wages).



that the relevant occupational group is 'Managers, Directors and Senior Officials', the 2021 median hourly earnings (excluding overtime) for this group is £22.01.

This hourly cost is up-rated for non-wage costs using the latest figures from Eurostat and in line with Regulatory Policy Committee guidance,<sup>35</sup> resulting in an uplift of 22% and an hourly cost of £26.84.

Using this hourly cost, and making the simplifying assumption of one person being responsible for familiarisation for each of the relevant organisations<sup>36</sup>, the total estimated familiarisation costs for the code ranges from £210,000 to £420,000.

### Sensitivity analysis

There are two variables in our model that are subject to sensitivity analysis.

- 1) The number of times that an organisation reads the code

Table 2: Sensitivity test – number of reads

Number of companies affected	Number of reads				
	0.5	1	2	5	10
Low estimate	£105,000	<b>£210,000</b>	£420,000	£1,050,000	£2,100,000
High estimate	£210,000	<b>£420,000</b>	£840,000	£2,100,000	£4,200,000

Source: ICO, Economic Analysis team

- 2) The time taken for one person to read the code

Table 3: Sensitivity test – reading time

Number of companies affected	Time		
	-10%	1.2hrs	+10%
Low estimate	£189,000	<b>£210,000</b>	£231,000
High estimate	£378,000	<b>£420,000</b>	£462,000

Source: ICO, Economic Analysis team

The impact estimates are linearly related to the two assumptions tested above. This means an increase or decrease in one of the assumptions leads to a

<sup>35</sup> See guidance in [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/827926/R\\_PC\\_short\\_guidance\\_note\\_-\\_Implementation\\_costs\\_August\\_2019.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/R_PC_short_guidance_note_-_Implementation_costs_August_2019.pdf).

<sup>36</sup> In reality there may be one person responsible for understanding the code for multiple organisations or multiple people in one organisation, but in the absence of data to make a precise estimate, the simplifying assumption is deemed appropriate.

## Data protection and journalism code impact assessment

proportionate increase or decrease in the impact estimate. Using the indicative increases or decreases shown above to produce sensible upper and lower bounds, familiarisation costs could be as low as £105k or as high as £4.2m.