Information Commissioner's Office

Behind the screens – maintaining government transparency and data security in the age of messaging apps

Report of the Information Commissioner to Parliament, July 2022

ico.
Information Commissioner's Office

INFORMATION COMMISSIONER'S OFFICE

"Behind the screens – maintaining government transparency and data security in the age of messaging apps"

Report of the Information Commissioner to Parliament, July 2022

Presented to Parliament pursuant to Section 139(3) of the Data Protection Act 2018

This publication is available at www.gov.uk/official-documents

Any enquiries regarding this publication should be sent to us at behindthescreens@ico.org.uk

ISBN: 978-1-5286-3513-4

E02762926 07/22

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of Her Majesty's Stationery Office

Contents

Information Commissioner's message

Despite the challenges we have all faced during the pandemic, we must not lose sight of the fact that transparency and accountability are fundamental to a functioning democracy. That is as true today as it was before the events of the last two years.

I am, and will remain, an advocate for the advantages that new communication platforms provide. However, their use does not remove the requirement for government officials, departments and the wider public sector to continue to be accountable to the people they serve. This goes to the heart of why the findings across this report matter. It is also why the government must act upon these findings if we are to retain public trust in the public institutions that serve us all.

Background

Following widespread media reports, the ICO received complaints in July 2021 about the alleged use of private correspondence channels for official business by Ministers in the Department of Health and Social Care (DHSC). The complainants were concerned that such practices could result in information being lost from the public record.

Information not recorded in this way would not be available to help the public and official inquiries to understand decisions taken by Ministers and officials. It is also information that the public has a right to seek access to under the Freedom of Information Act (FOIA). Such claims also raise concerns about the confidentiality and security of personal data conveyed and stored on messaging apps.

Following careful consideration of these complaints, my predecessor decided to launch an investigation into the allegations. This investigation has found failings at DHSC in compliance with both transparency and personal data protection obligations. I have therefore made several recommendations to the department for improvements.

The investigation was launched under the authority of the UK General Data Protection Regulations (UK GDPR), the UK Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000. This report summarises the findings of our investigation and the actions we have recommended DHSC should take as a result.

Whilst these recommendations are for DHSC to address, this report also highlights issues that other public authorities (especially those within central government) will want to learn lessons from. For instance, there should be stronger protocols about

how Ministers and Non-Executive Directors (NEDs) are provided with access to official information. Also, more consideration could be given to how that information is communicated, stored and deleted, if this is done over non-corporate channels.

But as we set out in the final chapter of this report, which looks beyond our investigation into DHSC, more fundamental work is also needed. There have been rapid changes in technology in the two decades since Parliament passed FOIA. This mean there is a risk that policies and procedures in place across Whitehall no longer reflect how Ministers and officials work and interact in practice. It is essential we examine and address the impact these technology changes are having and that clearer methods are put in place to ensure this happens each time new technology becomes available. As was made clear by my predecessor at the outset of this investigation, it is not unlawful for ministers and officials to use private channels for conducting official business.

The pandemic placed extreme demands and stress on our public services. It is understandable, therefore, that some Ministers, advisors, NEDs and senior officials have relied on new technologies to make their work and their lives more manageable.

In our view, however, the deployment of these technologies failed to appreciate the risks and issues around the security of information and managing transparency obligations. This is not solely a product of pandemic exigencies. But rather a continuation of a trend in adopting new ways of working without sufficient consideration of the risks and issues they may present for information management across government over several years preceding the pandemic.

I am therefore recommending that Government should now establish a separate review to look at how different, non-corporate communication channels are being used across Government. This should identify any systemic risks and areas for improvement, as well as whether there should be greater consistency in approach across departments. This is in addition to any considerations by the COVID-19 Inquiry of issues specific to the pandemic.

The review could also consider whether there is a case for a stronger duty on Ministers, public servants and others who are responsible for maintaining the public record. This is not a novel idea. Similar duties already exist in Canada, New Zealand and the USA, which could provide a foundation for an updated approach in the UK. Alternatively, it may be that the Ministerial and Civil Service codes could be strengthened specifically for the issues identified in this report.

I am presenting this report to the UK Parliament for the relevant Select Committees to consider, as well as to the UK Government, so Ministers can consider my recommendations. This will help inform the future debate about how we can make the best use of new technology, while protecting and preserving our public records for future generations and maintaining the security of personal and official information.

It is only by tackling these issues at this crucial time that we can maintain public trust in the institutions of government and preserve transparency and accountability now and in the years to come.

John Edwards
Information Commissioner
July 2022

Executive summary

This report summarises an investigation by the Information Commissioner's Office (ICO) into the use of private correspondence channels by Ministers and others working at the Department of Health and Social Care (DHSC). It considers the impact that these practices have had on information security and the quality of records management and outlines our findings and recommendations.

It also considers other information in the public domain that relates to the issues raised by our investigation that affect other UK Government departments. Drawing on this evidence, it then summarises what further action is necessary to review and strengthen information handling and records management practices across the public sector.

The scope of the report

Chapter 1:	Introduces the report and summarises the factors that prompted the investigation into the Department of Health and Social Care (DHSC).
Chapter 2:	Establishes the scope of the issues under the UK General Data Protection Regulations (UK GDPR), Data Protection Act 2018 (DPA) and the Freedom of Information Act 2000 (FOIA) that have formed part of the investigation.
Chapter 3:	Sets out the approach we have taken to the investigation into DHSC. It explains the powers we have available to us under each piece of legislation, as well as how we have used these and the evidence we have gathered as a result.
Chapter 4:	Outlines our key findings following the investigation into DHSC.
Chapter 5:	Establishes the regulatory action we propose for DHSC and the next steps it needs to take. The recommendations we make in Chapter 5, while aimed at DHSC following our investigation to help improve its policies and procedures, may also be relevant to other departments that have been operating in similar ways both before and during the pandemic.
Chapter 6:	The final chapter of this report looks beyond our investigation into DHSC and considers some of the evidence we have seen alongside other information in the public domain. It reflects on the wider lessons that public bodies can take from this investigation and includes recommendations for Government as a whole to consider.

Our key findings

- There was extensive use of private correspondence channels by Ministers, and staff employed by DHSC. Evidence more widely available in the public domain also suggests this practice is commonly seen across much of the rest of Government and predates the pandemic.
- The allegations in the media that the Secretary of State at the time 'only' used private correspondence channels are not accurate. In practice, a mix of channels were used by him and the other Ministers we have considered as part of our investigation.
- There is clear evidence that all Ministers we issued information notices to were regularly copying information to government accounts to maintain a record of events.
- The scale of the use of private channels suggests that, on the balance of probabilities, there is a risk that mistakes may have been made by individuals in preserving parts of the public record during a historically significant period.
- DHSC did not have appropriate organisational or technical controls in place to ensure effective security and risk management of such channels.
- DHSC's policies and procedures were inconsistent with a Cabinet Office policy and had some significant gaps based on how key individuals were working in practice. This presented a risk to the effective handling of requests for information in line with the relevant codes of practice under FOI.
- The use of such channels presented risks to the confidentiality, integrity and accessibility of the data exchanged.
- DHSC have been clear that the use of private channels brought real operational benefit at a time in which the UK was facing exceptional pressures throughout the COVID-19 pandemic. However, it is of concern that such practices continued without any review of their appropriateness or the risks they presented.

Although not a focus of our investigation, during our enquiries we identified that protectively marked government information was being held outside government IT systems. Cabinet Office have indicated that it considered this information once we highlighted it and said that it had no concerns over how the information was held.

Our key recommendations

We have issued DHSC with both a Practice Recommendation under FOIA and a Reprimand under the UK GDPR and DPA 2018. These outline how DHSC can more effectively manage risk and improve its processes and procedures. We have included the full detail of the action we have taken against DHSC at Annex A and B.

1. Introduction

In July 2021, the then Information Commissioner received complaints about media reports in the Sunday Times regarding the alleged use of private correspondence channels by DHSC Ministers to conduct official government business during the pandemic.

The key complaint was from the COVID-19 Bereaved Families for Justice Campaign. In particular, the Campaign set out their concerns about what such practices, if happening, "may mean for those seeking transparency and accountability regarding the many life and death decisions taken in the Department of Health during the pandemic".

They also raised questions about any potential implications for the subsequent inquiry into the handling of COVID-19 that the UK Government had already committed to.

The Commissioner is required by law to ensure compliance with a range of information rights legislation. Under FOIA, there are codes of practice that the Commissioner is required to promote. These explain how departments should manage information and handle FOI requests. Under data protection law, the Commissioner has a duty to ensure that:

- public bodies comply with their obligations to process personal information lawfully and securely;
- data is accurate and not retained for longer than necessary; and
- data subjects' rights are upheld.

After considering the information available at that point, on 6 July 2021, the then Commissioner announced[1] that she was launching an investigation into the alleged use of private communication channels at DHSC.

In setting out her reasons for launching the investigation, the Commissioner noted:

> "my worry is that information in private email accounts or messaging services is forgotten, overlooked, autodeleted or otherwise not available when a freedom of information request is later made. This frustrates the freedom of information process and puts at risk the preservation of official records of decision making. I also worry that emails containing personal detail are not properly secured in people's personal email accounts".

This report sets out the background to how we conducted this investigation, what we found and the action we have taken.

[1] Blog: ICO launches investigation into the use of private correspondence channels at the Department of Health and Social Care | ICO

It concludes by highlighting some wider recommendations for the UK Government about reviewing working practices across the public sector more fundamentally. This is based on our findings and evidence outside our investigation that both highlight similar issues far beyond the working practices of DHSC during the pandemic.

2. Scope of the investigation

The ICO's investigation considered the Commissioner's statutory obligations as a regulator under both FOIA and its related codes of practice, as well as the requirements of the UK GDPR and the DPA 2018.

The use of private correspondence channels does not in itself break freedom of information or data protection rules. This was made clear by the Commissioner at the outset of the investigation.

In November 2021, we updated our guidance on how public authorities should handle information held in private channels under FOI[2]. This updated the pre-existing guidance in place during the period we have investigated. The Cabinet Office has also issued guidance on this issue[3], which dates from 2013. These pieces of guidance indicate that using such channels creates a few risks and potential challenges to complying with FOIA and the code. It is the scale of these risks and the extent to which DHSC have mitigated them that we have examined as part of our investigation under FOIA.

Similarly, we do not take the view that DHSC should never send information containing personal data to private communication channels. However, where there are alternatives in place, public bodies should consider the necessity and appropriateness of these communications. For example, they could use corporately issued and controlled accounts or platforms.

Where public bodies use private platforms, our view is that they should have sufficient controls in place to ensure that they handle:

- people's personal data securely; and
- in a way that they can properly retrieve it, if requested.

Without this, it is difficult to see how public bodies and the individuals that work for them can have confidence in how they are properly protecting any personal data entrusted to them.

We have outlined below the relevant sections of each piece of legislation that were relevant to the Commissioner's considerations.

The Freedom of Information Act

Under section 47 of FOIA, it is "the duty of the Commissioner to promote the following of good practice by public authorities". This duty applies to both the general provisions of the Act itself, as well as to the codes of practice that FOIA requires the Government to produce. We have outlined below the relevant provisions of FOIA and its codes that we considered as part of the investigation.

[2] Official information held in non-corporate communications channels | ICO
[3] Private_Email_guidance.pdf (publishing.service.gov.uk)

The Section 45 code

The Section 45 code is produced by Ministers in line with the requirements of FOIA. It provides guidance on the practice public authorities can follow to meet their obligations under FOIA. Adhering to the code will result in positive benefits for a public authority, and in practical terms helps them deliver good customer service to those making requests. The code of practice provides guidance for public authorities on best practice in meeting their responsibilities under Part I of the Act (access to information). It sets the standard for all public authorities when considering how to respond to freedom of information requests. The code is issued by the Minister for the Cabinet Office, who is required to consult the Commissioner before making or revising the code. The code is laid before Parliament.

A new section 45 code[4] was revised and reissued following feedback from a public consultation and in consultation with the then Information Commissioner and issued on 4 July 2018. It provides practical advice for public authorities on dealing with requests for information and covers the provision of advice and assistance, fees, transferring requests, consultation with third parties, confidentiality obligations and complaints procedures.

The Commissioner's investigation into practices at DHSC has focussed on sections 1.8 to 1.12 of the Section 45 code. Section 1.10 sets out that "Information is 'held' by the public authority if it is retained for the purposes of the public authority's business … Public authorities need to search for requested information in order to communicate to the applicant whether the information they are seeking is held or not held by that public authority. These searches should be conducted in a reasonable and intelligent way based on an understanding of how the public authority manages its records".

Section 1.12 states that:

> "Public authorities need to search for requested information in order to communicate to the applicant whether the information they are seeking is held or not held by that public authority. These searches should be conducted in a reasonable and intelligent way based on an understanding of how the public authority manages its records. Public authorities should concentrate their efforts on areas most likely to hold the requested information. If a reasonable search in the areas most likely to hold the requested information does not reveal the information sought, the public authority may consider that on the balance of probabilities the information is not held."

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/744071/CoP_FOI_Code_of_Practice_-_Minor_Amendments_20180926_.pdf

The Section 46 code

Guidance for public authorities on good records management is provided by the Section 46 code[5], which was most recently updated in July 2021. The code of practice is issued by the Secretary of State for DCMS, following consultation with the Information Commissioner, the Minister for the Cabinet Office and the appropriate NI Minister.

This code provides guidance to authorities which helps them to create a framework for keeping, managing and destroying their records. Complying with this code will help authorities to account for their activities. It will also help them to comply with FOIA, the Environmental Information Regulations (EIR) and other information rights legislation such as the UK General Data Protection Regulation (UK GDPR). It will assist them in complying with the Public Records Act 1958 (PRA) and The Public Records Act (Northern Ireland) 1923 (PRA (NI)), if they apply. It will also help public authorities to fulfil their duty to publish information about their activities and to comply with the Re-use of Public Sector Information Regulations 2015.

The Section 46 code was in the process of being updated by the Government at the time we launched this investigation. The revisions which were made (in consultation with ICO) were partly to provide guidance to relevant authorities to reflect contemporary information management practice and the modern digital working environment. It was subsequently laid before Parliament during our investigation. It makes clear that public authorities should take various factors into account when they decide what records they should keep.

Clear provisions of the previous code which are relevant to the ICO's investigation, given DHSC's central role in the pandemic, are about:

> - the need to refer to authoritative information about past actions and decisions for current business purposes;
> - the need to explain, and if necessary justify, past actions in the event of an audit, public inquiry, or other investigation; and
> - [the need to] set business rules identifying [w]hat records should be kept … [b]y whom this should be done …. [and at] what point in the process or transaction this should be done.

It also sets out that all staff should be aware "of which records the authority has decided to keep and of their personal responsibility to follow the authority's business rules and keep accurate and complete records as part of their daily work".

The updated version of the Section 46 code is relevant to the broader recommendations we have made for Government later in this report. Relevant

[5] Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (publishing.service.gov.uk)

elements from this code for our investigation include sections making clear that public authorities should:

- collect and keep technical and contextual information about their records in order to understand their value;
- endeavour to hold information in an appropriate environment;
- make reasonable efforts to recover contextual information for "orphaned information" which they judge to have value, and keep a record of any action they take; and
- have appropriate tools to identify, locate and retrieve information when required, which includes maintaining an effective search capability alongside controls to protect sensitive information.

This latest version of the Section 46 code also makes clear that public authorities must be able to trust their information. In order to do so, they should:

- be able to establish when information was created and who it was created by;
- have policies and processes for information security that comply with relevant legislation, guidance and codes of practice;
- apply access and permission controls throughout the life of the information to prevent unauthorised or unlawful access; and
- have appropriate technical and organisational measures to prevent accidental loss, destruction or damage, to their information.

The Data Protection Act

We also investigated whether DHSC met its data protection obligations. A key question was how it used non-official messaging systems, such as Gmail, Hotmail and WhatsApp. Did DHSC use them in a way that was compliant with its obligations to ensure personal information was accurate, secure, and could be accessed easily? For example, what happened if someone asked for a copy of their data?

The UK GDPR and DPA 2018

The Commissioner's functions are set out in Article 57 of the UK GDPR. The specific grounds for investigating this case arise from the media reports and subsequent complaints about the alleged use of private correspondence channels. These reports prompted concern that DHSC may not have processed messages containing personal data, and potentially special category personal data, in accordance with its data protection obligations.

Under section 115 (3) (a) of the DPA 2018, the Commissioner has "a duty to advise Parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data".

We have considered a number of aspects of data protection law as part of this investigation, including whether DHSC had:

- an appropriate basis for processing any of the personal data contained in the messages (Article 6 and Article 9 UK GDPR);
- put in place suitable ways of working and technical controls to ensure personal information (eg about officials and connected individuals) was kept safe (Article 5 (1)(f) and Article 32 UK GDPR);
- only processed any personal data contained in the messages for its intended purpose (Article 5(1)(b) UK GDPR); and
- considered data protection as a matter of design in any processes and procedures it used to handle personal data (Article 25 UK GDPR).

We have highlight later in the report the specific areas where we have found contraventions across these provisions.

3. Our approach to the investigation

We wrote to DHSC on 5 July 2021 to inform it that we were launching our investigation. In this chapter we outline the approach we took to gathering the evidence that has informed our conclusions.

Issuing information notices

Our first priority was to use our statutory powers to ensure that DHSC appropriately retained information relevant to our investigation. The Commissioner can issue statutory information notices to require public bodies to provide information by a specific deadline, under both FOIA and the DPA.

We issued two such notices to DHSC on 5 July 2021 under each piece of legislation, requesting a response within 30 working days.

The FOIA notice required information including:

- any policies used by DHSC to inform its compliance with FOIA and its related codes;
- copies of emails sent to and from private correspondence channels by departmental accounts, including any summaries made by private offices and others to summarise these exchanges; and
- examples of recorded contact with Ministers to confirm checks of private email accounts to inform responses to FOIA requests.

The DPA notice required information about a wide range of areas linked to the GDPR, UK GDPR and the DPA 2018 including:

- the principles relating to the processing of any personal data applied by DHSC (Article 5);
- how DHSC had taken into account its responsibilities as data controller and its approach to data protection by design and default (Articles 24 and 25);
- the security of any processing of personal data conducted by DHSC over private channels (Article 32);
- the use of data protection impact assessments by DHSC to inform its approach (Article 35);
- DHSC's approach to purpose limitation, accuracy and retention (Articles 5 (1) (b), (c) and (d));
- the extent of records of processing of personal data linked to DHSC's processing activities (Article 30); and
- the rights of any data subjects whose personal data was captured over private channels by DHSC (Articles 12-22).

We cannot issue information notices under FOIA on individuals, although we do have this power under the DPA. Given the evidence available at the outset of our

investigation, we also issued notices under s142(1)(a) and s142(1)(b)(i) of the DPA to other parties of relevance to the Commissioner's investigation. Their purpose was to obtain information relevant to the investigation. We issued a number of notices, including:

- **The Rt Hon Matthew Hancock MP** – Mr Hancock was appointed as Secretary of State for Health and Social Care on 9 July 2018 and resigned from this position on 26 June 2021. He was therefore the Secretary of State for the majority of the period investigated, covering the time between 01 March 2020 to 05 July 2021.
- **Lord Bethell of Romford** – Lord Bethell was appointed as a Parliamentary Under Secretary of State at DHSC on 9 March 2020. This role ceased on 17 September 2021. He was therefore the Parliamentary Under Secretary of State for the majority of the period investigated.
- **Helen Whately MP** – Helen Whately MP was appointed as Minister of State (Minister for Care) at DHSC on 13 February 2020. She was therefore the Minister of State for the majority of the period investigated. On 17 September 2021, Ms Whately moved from her role as Minister of State for Social Care to become the Exchequer Secretary to the Treasury.

The notices required each individual to answer a series of questions about their use of private messaging channels, their knowledge of relevant policies and procedures. They were also asked to provide examples of information exchanged between DHSC and them via private platforms that they used. DHSC responded on each individual's behalf with the examples of information exchanged.

We also issued notices under the s142(1)(b)(i) of the DPA to:

- **Gina Coladangelo** – Ms Coladangelo was appointed to DHSC's Departmental Board as a NED on 7 September 2020 and resigned from this role on 26 June 2021. She was therefore employed at DHSC for a key part of the period investigated. We served this notice on 9 July 2021.
- **Oliver Bonas Ltd** – Oliver Bonas Ltd was Ms Coladangelo's substantive place of employment from 1 May 2017 to 30 June 2021. Reports at the outset of the investigation suggested that Ms Coladangelo used her Oliver Bonas email account to receive emails sent by DHSC. The company withdrew access to this account by Ms Coladangelo on 2 July 2021, albeit its IT department staff continued to have access. We served this notice on 6 July 2021. The response to the notice indicated that information relating to DHSC matters had been exchanged via an Oliver Bonas Ltd account.

Both notices required responses to a series of questions about Ms Coladangelo's employment with Oliver Bonas Ltd and information relating to the Oliver Bonas Ltd account in use at the time.

We have published all of these information notices on our website.

The response to our information notices

DHSC were clear from the outset that the ongoing impact of the pandemic meant that it would not be able to comply with the original deadline. We accepted that the impact of the pandemic was unprecedented and offered extensions and advice to support DHSC in responding to the notices so that we received sufficient detail to inform this report. DHSC also noted that it would be acting on behalf of the relevant former Ministers and Non-Executive Director subject to the information notices we issued. The individuals also provided some initial responses directly to the ICO.

DHSC's use of private communication channels over which it did not have direct control organisationally presented a clear challenge for them to:

- identify where information falling within scope of the notices would be held; and
- conduct the necessary searches to obtain such information.

The time required by DHSC to respond to the ICO's information notice is indicative of the scale of the task. Had such information been exchanged by a single corporately controlled system, a centralised search may have been more achievable and timely.

As accepted by DHSC in correspondence, the ICO did highlight ways the department could reduce the volume of information it had to search by focussing on the matters at the heart of the investigation. We recommended, for example, that it should initially focus on accounts linked to the specific individuals on whom notices had also been issued. We clearly indicated that further work may not be needed if it provided sufficient evidence through a phased response. We reiterated the likely benefits of this approach at several points throughout the investigation.

Following the responses to the notices sent by DHSC in October, it agreed to refocus its efforts this way. This refinement in approach meant that DHSC could send the final tranches of evidence we considered necessary to help us conclude the investigation between January and March 2022.

Interviews

In light of the written responses we received to the notices, we extended invitations to attend voluntary interviews to each of the individuals on whom we had served the notices. Each individual accepted and we held interviews during January 2022.

The purpose of these interviews was to further ascertain each individual's understanding of DHSC's policies and procedures. Specifically, the use of private correspondence channels, the rationale for the use of these channels and the specific circumstances in each case.

We also conducted interviews with DHSC's Data Protection Officer and Senior Information Risk Officer in post during the investigation. These interviews helped inform our understanding of:

- the level of awareness across DHSC of the use of private accounts;
- the security implications that they had considered; and
- the support made available to Ministers and others using private channels.

Each interview subject engaged openly with the interview process.

What we received

In total, we reviewed:

- more than 4,800 emails located in an account outside DHSC's official systems, the majority of which related to exchanges between the department and the account holder. The emails related in the main to meeting arrangements, minutes and associated agendas;
- over 100 pages of evidence containing screenshots of multiple emails and messages shared from various DHSC accounts with the non-corporate accounts of Ministers working at the department;
- 100s of pages of policies and procedures made available to those working across DHSC; and
- evidence from six official interviews, multiple meetings held with officials and an official site visit at DHSC's offices held over the duration of the investigation.

We are satisfied that this evidence gave us a good insight to the way in which the department, its Ministers and officials were using private messaging channels.

Other information

As indicated above, over the course of the investigation we met and corresponded regularly at both a senior and an operational level with relevant officials at DHSC. This included meetings between the Second Permanent Secretary and the then Information Commissioner and Deputy Commissioner. This helped us to monitor DHSC's progress and provide support and clarification on the requirements set out in the notices, as indicated above.

To inform some of the broader recommendations in this report, we also reviewed evidence in the public domain that was relevant to the issues we looked at during our investigation at DHSC. We have outlined this information in more detail in the final chapter of this report.

4. What we found during the investigation

Our investigation found that private correspondence channels at DHSC were used at both Ministerial and official level.

For some individuals, based on what we have seen, this was often focussed on meeting arrangements and related material. For others, it also included more substantive issues linked to the handling of the pandemic. At times, this included officials directly emailing from their corporate account to Ministers on their private account. In many cases, the evidence provided by DHSC included direct contacts from private sector organisations to Ministers on their private accounts, offering support and services during the pandemic. Any calls for action that Ministers issued were then appropriately forwarded to the department to deal with.

It is worth reiterating that, as we made clear at the outset of the investigation, using private channels in these ways is not in itself against the law. FOIA does not include a duty to create or preserve any records. However, once a request is received, there are potential criminal sanctions for anyone who "destroys or conceals any record held by the public authority, with the intention of preventing … disclosure"[6]. Although subject to challenge, a recent ruling by the High Court[7] has also made these points clear.

The use of such platforms did not in itself constitute a breach of either freedom of information or data protection laws and rules. This is provided that DHSC had sufficient controls in place to keep and consider public records when requested for disclosure by the public. Also, that it safeguarded the accuracy and security of any personal information. The investigation found, however, that such controls were lacking.

We have set out in this chapter what our investigation found in detail.

Policies and procedures

DHSC had a number of policies in place that it shared with us in response to the notices we issued. These included its:

- **Information management policy.** This policy prohibited the use of personal email accounts for work purposes, other than in exceptional circumstances as agreed by DHSC Information and Security Team. The policy also prohibited them sending emails containing personal data outside DHSC without the agreement of the Information Asset Owner or the Head of Information and Security or both. It also required any personal data taken outside DHSC premises on an electronic device to be encrypted.
- **Acceptable use of IT policy.** This policy set out requirements for employees to create secure passwords and protect usernames and passwords appropriately. It prohibited the use of personal devices, email accounts and

[6] See s.77 of FOIA
[7] AtC GLP final judgment (judiciary.uk)

messaging apps for work purposes. It also identified trusted government addresses and the procedures to follow when encryption was not required for sharing information outside departmental systems.

- **Cabinet Office's Guidance for Departments on the use of private email.** This guidance from 2013[8] stated that "Civil servants and Ministers are generally provided with access to Government email systems. Other forms of electronic communication may be used in the course of conducting Government business. Departments' security policies will apply when generating and communicating information." Whilst issued by the Cabinet Office, this guidance was adopted by DHSC and used by departmental Ministers and officials. The guidance was aimed at helping departments manage information with the growing use of emails.

The local DHSC policies stated that the use of private communication channels was prohibited by DHSC employees, except in exceptional circumstances. As with any policies where this caveat applied, it is noted that the pandemic did clearly present an exceptional circumstance. However, these polices did not apply to Ministers or NEDs.

The Cabinet Office guidance did however apply to Ministers and civil servants. There was therefore a disconnect between DHSC polices that applied to employees and those applied to Ministers and NEDs.

Within the Cabinet Office guidance, it was explained that departments' own security policies would apply when generating and communicating information. There was therefore also a conflict between the Cabinet Office guidance and DHSC Information Management and Acceptable Use of ICT Policies. This prohibited the use of personal email accounts by DHSC employees other than in exceptional circumstances.

The Cabinet Office guidance stated that "The originator or recipient of a communication should consider whether the information contained in it is substantive discussions or decisions generated in the course of conducting Government business and, if so, take steps to ensure the relevant information is accessible (eg by copying it to a government email address)".

Departments were not routinely expected to search individuals' private email accounts in order to locate information that had been requested under information law. Departments were advised that it would generally be reasonable to search only within Government systems. Also, that only in exceptional circumstances should it be necessary to approach the individual directly.

There were contradictions between DHSC's own policies and the Cabinet Office guidance. DHSC has acknowledged the need to align departmental and cross-government guidance.

The contradictions between guidance were confusing. Our investigation found that DHSC's expectations of Ministers and senior staff was not clear about the

[8] Private_Email_guidance.pdf (publishing.service.gov.uk)

circumstances under which they could use private communication channels. Similarly, where they did, it was not clear what measures should have been in place to ensure that they used such channels appropriately.

In addition to the above, the Commissioner's investigation also considered DHSC's:

- records management policy;
- data protection policy;
- data breach notification policy;
- right of access, right of erasure, right to correct inaccuracies procedures document; and
- freedom of information guidance for staff.

DHSC's freedom of information guidance for staff aimed to cover the full range of responsibilities that FOIA identifies. Whilst comprehensive, it was last updated in 2015. It was therefore significantly out-of-date as it did not reflect the changes made to the code in its most recent iteration in 2018.

DHSC's records management policy, published in May 2021, contained broken links to the Section 46 code. This made it more difficult for staff using the guidance to understand what they needed to do. This guidance also failed to provide any specific depth on the nature of the information covered by its provisions except to say "all information, regardless of format, held and processed by or on behalf of DHSC". It did not make any reference to the wide variety of information handling practices clearly undertaken across the department.

However, our enquiries showed that the practical implementation of such procedures at the highest levels across the department was inconsistent at best.

There is clear evidence that Ministers and NEDs were making regular use of private correspondence channels. It is also the case that DHSC was aware of this at senior levels.

We have found that the policies about the use of private correspondence channels for official business were inconsistent, unclear and not up-to-date. This is not conducive to good information management nor reflective of good practice.

The use of private correspondence channels

In response to the notices we issued, DHSC sent out a questionnaire to a wide range of staff to identify information that may have been caught within their scope. As part of this exercise, DHSC notified us that it had identified that official information had been shared through:

- 29 private WhatsApp accounts;
- 17 private text accounts;

- eight private email accounts; and
- one private LinkedIn account.

These channels included private accounts linked to each of the individuals we had also served individual notices on.

DHSC told us it had reviewed 2,261 emails in support of its response to both our FOIA and DPA notices. A smaller subset of 241 emails were also considered by the department to fall specifically within the scope of the DPA notice. Over a 100 pages of evidence was shared with us by DHSC following its reviews. We have also reviewed thousands of emails located outside DHSC systems following the notices we issued.

The evidence we saw from DHSC and other sources proves that the use of private correspondence channels was extensive across DHSC during the period we investigated.

We also found that although early media reports suggested that 'only' private channels were being used by the then Secretary of State for Health and Social Care in particular, this was not the case. In practice, a mix of private and official accounts were in use to varying degrees by the Secretary of State and the other DHSC Ministers involved in this investigation.

There is also clear evidence that all the Ministers caught by the scope of our investigation regularly forwarded material from their private accounts to official accounts to ensure information was recorded appropriately. This demonstrates that there was a level of commitment by those involved to maintain a record of events and comply with the relevant guidance and codes of practice.

DHSC's systems and processes

DHSC told us that to respond to parts of the notices, it created a dedicated investigation team to co-ordinate its internal actions in gathering the necessary information. One of the mechanisms it employed was the distribution of a survey to "Departmental Special Advisers (SpAds), Directors, Directors General (DGs), Ministers and Private Offices to understand the numbers of staff potentially in scope and to help assess the scale of the task".

Implicit in this action is an acknowledgement that existing control mechanisms were insufficient to confidently supply the answers to the questions asked in the notices. Therefore, it also suggests that there was no clear corporate knowledge of the extent and scale of what it may hold in these formats in order to conduct appropriate searches for requests.

Section 1.12 of the Section 45 code under FOIA states that:

> "Public authorities need to search for requested information in order to communicate to the applicant whether the information they are seeking is held or not held by that public authority. These searches should be conducted in a reasonable and intelligent way based on an understanding of how the public authority manages its records. Public authorities should concentrate their efforts on areas most likely to hold the requested information. If a reasonable search in the areas most likely to hold the requested information does not reveal the information sought, the public authority may consider that on the balance of probabilities the information is not held."

From a records management perspective, it is clear that the use of non-corporate messaging services was allowed to increase without co-ordinated oversight of their control and use. There was confusion about who ultimately controlled access. There was little, if any, evidence of control of the ongoing departmental access for retrieval or security requirements.

The specific evidence we saw about the type of information being shared across private correspondence channels was wide-ranging. It included often unsolicited emails from external individuals (such as potential PPE and testing suppliers) contacting Ministers on private accounts, as has already been widely reported. Matters relating to procurement have also been evidenced through other reports, such as those by the National Audit Office (NAO). NAO found, for example, that DHSC "did not document key decisions adequately, disclose ministerial meetings … fully or keep full records of ministerial discussions".

However, the evidence we saw was not simply related to these matters. It included inter-departmental communication between Ministers and various officials and advisors, as well as direct emails from officials at bodies, such as Public Health England, to Ministers' private accounts.

It is perhaps the latter that is of most concern. It demonstrates that the private accounts of Ministers were widely distributed across Whitehall. They were used not only by other Ministers, Special Advisors and their Private Offices. But also by a range of other officials who were sending formal advice and official information directly to them on these private accounts. In effect, it seems to have become custom and practice.

By definition, the evidence DHSC has provided to us represents information that it has retained on its corporate systems.

We are concerned that the scale of the use of private channels means that, on the balance of probabilities, mistakes will have been made in maintaining the public record during a period of historic significance.

An example of the risks related to the practices that DHSC allowed to develop were highlighted by the NAO in one of its reports on procurement:

> "messages not forwarded [to DHSC] at the time were kept by [Matt Hancock MP] and made available to Parliament as part of the publication of the Humble Address material in February 2022. These messages were not inconsistent with what the then Secretary of State saw as his ministerial responsibility to drive progress, rapidly building testing capacity with Randox and other suppliers."

Awareness of these practices was high. We saw emails copied to the most senior levels of DHSC that included private correspondence channels on the copy list. The Departmental Senior Information Risk Officer (SIRO) also confirmed their awareness of this practice at interview. (Although, it should be noted that the department's Data Protection Officer was not aware and, he suggested, neither were his predecessors).

Even allowing for the pressures of the pandemic, it would have been sensible for the department to have put in place a more systematic way to capture information for the public record. Simply requiring individuals to copy Private Offices into all exchanges or arranging for the regular capture of accounts for officials to sift may have helped. But, this does not seem to have happened as a matter of course based on the evidence we saw.

Ministers therefore had to make assessments themselves about significant volumes of material sent to their private accounts and what they should forward to the department. We consider it surprising that for such a prolonged and busy period a more efficient process with reduced risk to information management was not put in place that would also reduce the potential impact on Ministers' time.

It also meant that handling information requests was over-complicated. This risked information that was relevant to requests being missing from departmental systems. Given the scale of use of these channels, those responsible for looking for it may have been unaware that it may exist elsewhere.

Awareness of policy

Throughout the investigation we considered the working conditions during the pandemic. The pressures placed on DHSC, Ministers and NEDs were no doubt exceptional.

During the voluntary interviews, Matthew Hancock MP, Helen Whately MP and Lord Bethell all set out clear examples of where their combined ministerial, parliamentary and political roles required them to balance competing time and diary demands. They were of the view that funnelling email contact via a single account often helped to meet these demands.

For example, Lord Bethell explained that he would often need to respond to emails about multiple aspects of his role, whilst physically in session at the House of Lords. Being able to access such emails on one device and funnelled through one account, assisted him with the efficiency and practicality of responding during a period where communications were time critical.

If the pandemic necessitated greater use of private communication channels, then clearer policies needed to be put in place by the department. In the ICO's view, DHSC should have considered what steps it should take to ensure it met its obligations under information rights law. These could have included, for example:

- introducing an information risk management process;
- ensuring all staff and Ministers knew what was acceptable;
- periodic checks on the security of records with a risk assessment; and
- ongoing checks on security and monitoring of compliance.

Even if the use of private channels and devices was seen as necessary in the early days of the pandemic, it is of concern that such practice still continued, with little oversight, over a year later. This is indicative of a 'cultural drift' to such ways of working that pre-dated the pandemic and go beyond DHSC to practices in Whitehall more widely. Indeed, as highlighted in a later chapter of this report, it is likely that across much of Whitehall these practices pre-dated the pandemic by several years.

The DHSC did not have sufficient measures in place to ensure Ministers and NEDs could properly manage the risks of using private communication channels. This means that DHSC's policies were not fit for purpose and the absence of appropriate organisational controls was in contravention of Article 25 of the UK GDPR.

Security of information

Article 5(1)(f) of the UK GDPR requires that personal data shall be:

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

Article 32 also requires that:

> "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate

> technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> - the pseudonymisation and encryption of personal data;
> - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
> - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
> - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
> - In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
>
> Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
>
> The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law'.

Our investigation determined an absence of appropriate security controls by DHSC concerning the use of private correspondence channels.

This is because the use of private correspondence channels created an unnecessary level of risk. This is because they were undertaken without sufficient controls in place to ensure that personal data contained in the communications was processed securely. DHSC could easily have mitigated this, if it had relied on its corporate accounts, which had been provided to communicate with Ministers and NEDs. Or, if it had put in controls to mitigate the risks of using private correspondence channels where it could not avoid such use.

DHSC also confirmed that:

- it was not aware of the terms of use for third-party applications (for example Google or Hotmail) as these were not corporately managed;

- it expected that the standard terms of use were likely in place between the provider and the user;
- it did not hold information about where data on third-party accounts was hosted. This is because it did not manage third-party applications outside its corporately managed services; and
- there were security measures in place for departmentally issued devices. However, the DHSC did not regulate the use of personally owned devices.

Our investigation determined that it was through personally owned devices that access to the private accounts in question was most likely to have been undertaken. No evidence was presented to us suggesting that department-issued devices were used to access private accounts. This presents a clear area of potential risk to the security of personal data shared across private accounts.

Under Article 4 (7) of the UK GDPR, DHSC is the data controller who determines the purposes and means of the processing of personal data it processes as part of its functions. It is also the controller subject to the Commissioner's investigation and this report.

In relation to all four individuals issued information notices as part of this investigation, we determined that any security arrangements in place for their private correspondence channels were left to the discretion of the account holder and their provider. DHSC as the data controller did not have any involvement in the security arrangements for those accounts, despite awareness at senior levels of the Department of their use.

For example, there is no evidence of DHSC conducting a risk assessment or any similar exercise that might have assessed and identified any potential security issues such processing would create.

These were significant failings by DHSC in relation to its obligations under the DPA. As well as to ensure that proper processes were in place to underpin any ways or working that sat outside the department's usual policy.

Technical issues

As DHSC determined why and how it processed the personal data it held and created as part of its functions, it is responsible as a controller for that data.

DHSC did not hold accounts with any providers outside their corporately managed applications. It suggested that in relation to the use of private communication channels, the standard terms of use were likely to be in place between the provider and the account user.

DHSC did apply a number of measures to its devices to ensure the device and data on the department's systems were secure and only accessed by the intended user. For

example, the department required passwords to access all its devices, with minimum standards for password strength and automatic locking after a short period of inactivity. It could also enable biometric unlocking.

Conversely, DHSC did not regulate the use of personally owned devices by adding similar restrictions to those devices. No 'bring your own device' or similar policy was provided to us. The only security measures that applied to data stored in private accounts which were accessed via such devices were the passwords on department-issued mobile devices and various departmental policies. These stated that such accounts should not be used for official business.

The department also had limits on the number of unsuccessful password attempts before a device was locked and all data stored on that device was remotely deleted. This included third party application data stored on the device but not data stored in another location, for example in cloud storage.

However, as private email accounts could be accessed from any device, the use of departmental issued equipment in this context is of limited direct relevance. There were no directly applied departmental controls in place for the security and use of Gmail, Hotmail or other private correspondence channels, including messaging apps.

DHSC confirmed that it did not hold information about where any data held in third party accounts was hosted. This demonstrates a lack of knowledge that accounts holding DHSC related data, exchanged through private correspondence channels, could therefore be hosted outside the UK.

DHSC had not satisfied itself that third parties had appropriate measures in place to protect DHSC material that was being held within the systems or platforms. It also had not documented any risk assessments.

Ministers and NEDs were issued with, or had the option to be issued with, corporate accounts. Therefore, the information exchanged between the department and such individuals could have been handled within the DHSC estate. The failure to do so introduced the risk of inappropriate access, the potential loss of integrity or confidentiality, and the possibility of data loss, including material that was of relevance to the long-term public record.

The ICO's examination of DHSC's policies, procedures and approach shows that there were no steps in place to monitor, assess or otherwise check the use of third-party platforms. This would have allowed it to take a view on its appropriateness or to consider any related risks. For example, DHSC could have:

- assessed the security controls in place for the platforms in use to confirm their appropriateness and compliance with UK GDPR and DPA 2018;
- reviewed the platforms terms and conditions and privacy notices to understand how information would be processed, where it would be stored, and to consider any implications for the potential for third party access;

- limited the conditions for the use of such accounts to prevent routine processing on such platforms;
- required users of the platforms to adhere to set guidance about:
    - minimum authentication requirements;
    - remote access controls (taking into account the ability to access from multiple devices; to remain logged into accounts etc);
    - the deletion of information from the accounts once added to the official record; and
    - data minimisation.
- extended the application of DHSC specific policies and procedures relating to email use to all holders of @dhsc.gov.uk accounts (including NEDs and Ministers); and
- explored secure 'bring your own device' options for controlled access to DHSC accounts via personal devices.

The use of private correspondence channels, without appropriate technical controls to assess the security and access provisions of those accounts, represents a failure to put in place appropriate technical controls in accordance with Article 25 of the UK GDPR.

Storage limitation

As part of its responsibilities as a data controller, DHSC should have ensured that personal data could not be retrieved by an unauthorised person and that it did not keep it for longer than it needed it.

When official material containing personal data was held on private communication channels, this increased risks as the information could not be controlled or managed by DHSC.

There is a distinct danger that material could therefore be retained for much longer on such communication channels and DHSC did not have a system in place to enforce its document retention policies or assess the risk of retention.

The ICO FOI guidance published on 9 March 2017 (updated in December 2021) "Official information held in private email accounts" provided guidance about official information held in private email accounts and other media formats when held by a public authority:

> "It is accepted, that in certain circumstances, it may be necessary to use private email for public authority business. There should be a policy which clearly states that in such cases an authority email address must be copied in to ensure the completeness of the authority's records. In this way, records management policies will make it easier for public authorities to

> determine whether information is held and to locate and retrieve it in response to requests. If the information is contained within the public authority's systems, it can also be subject to consistently applied retention and destruction policies."

DHSC did not follow this guidance, nor did it put in place any similar alternative measures.

We found that the absence of appropriate systems to enforce DHSC's document retention policies, or assess the risk of retention, is in contravention of Article 5(1)(e) of the UK GDPR.

5. The action we have taken

In light of our findings, we have required DHSC to take a number of steps to improve its systems and processes. This includes the use of our statutory powers under both FOIA and the DPA.

FOIA practice recommendation

The statutory powers available to the Commissioner, where we identify practices that do not constitute good practice under FOIA and its codes, are relatively narrow.

Under section 48 of FOIA, the Commissioner does have the power to issue a formal Practice Recommendation (PR). This sets out steps he thinks are needed to promote conformity with the codes.

Following our investigation and pending the outcome of the recommended wider review, we have issued a PR to DHSC to improve its current ways of working. We have published this alongside this report (in line with our usual practice), together with other PRs we have issued under the Act.

In summary, the PR issued to DHSC sets out steps that it should take to ensure compliance with the Section 45 code:

- Update guidance for staff on the use of non-corporate channels so it is consistent across the different policies currently used by the department. We recommend following the ICO's guidance.
- Establish a centrally held register of the individuals permitted to use private channels and devices.
- Establish a process for granting this permission that includes confirmation of how, and with what frequency, individuals will transfer official information onto official systems. This should include specific provision for when individuals leave the department suddenly.
- Review and update DHSC's existing information request handling policies and training to ensure they are consistent with the changes made in response to the measures outlined above.
- Follow up with any DHSC Ministers, NEDs or senior staff who have left during the pandemic period and may have used private devices and correspondence channels. This is to seek confirmation in writing that they have transferred all relevant records onto the department's systems and, if not, seek to ensure they do so.
- In light of any material that may be received as part of this exercise, review DHSC's FOI request log to ensure that it considers this information for release, if relevant to any requests.
- Write to the Commissioner by the deadline set out in the notice to confirm that it has complied with his recommendations and how it has achieved this.

DHSC should take these actions in a consistent way and to the same timeframe as the steps set out in the DPA provisional enforcement notice outlined below.

In relation to the Section 46 code of practice on record keeping, the Commissioner has not specifically made any recommendations for DHSC. This is because the recommendations we have made under the Section 45 code will support not only better handling of information requests, but also address many of the risks we have identified about the quality of DHSC's record keeping. We have also made wider recommendations later in this report that address the work that we think is needed to tackle any similar issues across Government. This is given our concerns that the issues we have identified through this investigation are relevant not just for DHSC, but the wider public sector.

Under FOIA, any statutory recommendations we issue that relate to the Section 46 code are subject to consultation with the Keeper of Public Records at The National Archives (TNA). We have not made such a recommendation to DHSC specifically and have instead made a broader recommendation to the UK Government as a whole. However, we have updated TNA and sought its views on the broader issues we have identified in the next chapter, prior to laying this report before Parliament.

Prior to concluding this report, the Commissioner has also written to Baroness Hallett, the Chair of the Inquiry into the handling of the pandemic. He has recommended that the Inquiry consider the quality of record-keeping during this period as part of its work. An extract from that letter is at Annex C. This was also shared with TNA once issued and we are pleased to report that Baroness Hallett accepted this recommendation, which is now incorporated into the final Terms of Reference agreed by the Prime Minister on 28 June[9].

DPA18 and UK GDPR

As part of our investigation, we have made findings in the following areas of the UK GDPR and DPA18:

- **Article 5(1)(e)** – Storage limitation
- **Article 5(1)(f)** – Security
- **Article 25** – Data Protection by Design and Default
- **Article 32 –** Security of processing

To address the concerns identified, and to improve compliance going forward, it is recommended that if DHSC is to continue to incorporate the use of private correspondence channels, that it takes the following steps:

1. In order to improve compliance with article 5 (1) (f) and article 32 of the UKGDPR, the DHSC should undertake a review to assess the security and access controls in place in relation to the platforms in regular use (Google Mail,

[9] UK Covid-19 Public Inquiry (covid19.public-inquiry.uk)

Hotmail, Whatsapp) when exchanging communications that contain personal data, and to confirm their appropriateness and suitability to support DHSC's compliance with the UKGDPR and DPA18.

2. As part of that review process, to assess the aforementioned platforms terms and conditions and privacy notices to understand how information would be processed, where it would be stored, and to consider any implications for (a) the security of those platforms in relation to the potential for third party access, (b) the extent to which storage limitation is place, (c) the extent to which the data protection by design and default requirements can be met if use of the platforms is to continue.

3. The DHSC should also require users of the platforms to adhere to appropriate security guidance, such as that issued by the National Cyber Security Centre (NCSC) with regard to:

    - Minimum authentication requirements, for example, two factor authentication controls; and
    - Remote access controls (taking into account the ability to access from multiple devices; and to remain logged into accounts)

4. The Department should also review secure 'bring your own device' options for controlled access to official DHSC accounts via personal devices, in line with NCSC Guidance.

5. In order to improve compliance with article 5 (1) (e) of the UKGDPR, the DHSC should limit the situations under which such accounts (Google Mail, Hotmail, Whatsapp) can be used to prevent routine processing on such platforms.

6. In addition, the DHSC should set clear requirements for the deletion of information from personal accounts once added to the official record.

7. Further, the DHSC should ensure that the use of personal devices when exchanging personal data adheres to data minimisation principles.

8. In order to improve compliance with Article 25 of the UKGDPR, the DHSC should extend the application of DHSC specific policies and procedures relating to email use to all holders of @dhsc.gov.uk accounts as standard (including to Non-Executive Directors and Ministers). If this is not possible, tailored information to official account holders exempted from the policies, should be provided as part of their induction processes.

6. The importance of good record keeping

The COVID-19 pandemic helped shine a light on the importance of good record keeping both domestically and internationally.

The International Council on Archives and the International Conference of Information Commissioners, supported by our office and a wide range of other organisations, drew attention to the global need to recognise this issue in their statement in April 2020. A joint statement was also issued last year by the Australian and New Zealand Information Access Commissioners, which drew attention to the ever increasing need to maintain records of decision-making processes during the COVID-19 pandemic.

But these statements highlighted obligations already anticipated and planned for in the UK. For example, the version of the Section 46 code in force at the start of the pandemic made clear the importance of record keeping in crisis situations. This included maintaining good quality records in situations where public bodies may "need to explain, and if necessary justify, past actions in the event of a … public inquiry". The debate about the likelihood and timing of an inquiry started relatively early in the course of the pandemic.

What perhaps had not been anticipated as effectively, was how the pandemic would accelerate a cultural drift in working practices that was likely already well-advanced in parts of the public sector. Together with the risks this could pose to the public record. This report has highlighted some of these risks for one Government department. But there is also a wider context for the issues we have highlighted that goes much further than simply the actions of DHSC.

The role of the ICO

The Commissioner has a range of duties under the legislation he regulates. Relevant to this chapter of the report, in particular, are his duties under Section 47 of FOIA, which make clear that:

> "It shall be the duty of the Commissioner **to promote the following of good practice by public authorities** and, in particular, so to perform his functions under this Act as to promote the observance by public authorities of—
>
> (a) the requirements of this Act, and
>
> (b) the provisions of the codes of practice under sections 45 and 46."

The same section of the Act makes clear that:

> ""good practice", in relation to a public authority, means such practice in the discharge of its functions under this Act as appears to the Commissioner to be desirable, and includes **(but is not limited to)** compliance with the

> requirements of this Act and the provisions of the codes of practice under sections 45 and 46"

At the same time, under the section 139 of the DPA:

> "The Commissioner may produce … reports relating to the carrying out of the Commissioner's functions and arrange for them to be laid before Parliament".

As we have made clear throughout this report and when we launched the investigation, the use of private communication channels is not unlawful. However, the Commissioner is required to look beyond simple lawfulness. As set out above, he also has a duty to consider whether the working practices he sees constitute good practice.

We have mentioned in a number of places in this report the context in which DHSC were operating during an unprecedented global pandemic. The pressures they faced were real and significant and we have taken this into account throughout the investigation.

However, it is impossible to look at the evidence we have seen and consider that good practice was being followed in information management terms. This is why we have taken the action we have set out in the preceding chapters under both FOIA and the DPA in relation to DHSC. These measures are designed to support improvement, rather than utilise some of our stronger statutory powers. Our view is that this is a proportionate approach given the pressures faced by the department and those working in it at all levels.

In addition to the FOIA practice recommendation we issued in relation to the Section 45 code, we also considered whether to issue a similar recommendation under the Section 46 code in relation to records management (the relevant provisions of which are set out in Chapter 2). As part of these considerations, we decided to look more widely at information in the public domain to inform our thinking.

We concluded that, based on the evidence set out in this chapter, it was right to take a different approach. On the balance of probabilities, we think that, while we have investigated DHSC for the reasons outlined, if we had investigated a number of other departments, it is likely we would have found similar risks and issues.

Therefore, instead of issuing a section 46 code of practice recommendation to DHSC alone, we have made broader recommendations for the Government to consider at the end of this chapter. These are in line with the Commissioner's duty to promote good practice and are designed to ensure there is appropriate reflection and learning across Government as a whole following the findings we have made in this investigation. This is to ensure that the right balance is struck between maximising

the benefits of technology, while meeting the obligations and good practice outlined in the DPA, FOIA and their codes of practice.

Given the nature of our findings and the recommendations we have made, we have also published this report and laid it before Parliament in line with our statutory powers, in case relevant Committees of the House also want to consider these issues. We have also set out actions we will take as the regulator when considering future complaints that may touch on the issues in this report.

The wider legislative context

In the UK, the pandemic hit almost immediately after the fifteenth anniversary of the implementation of FOIA and two decades after its passage through Parliament. This itself updated public records legislation that had largely remained untouched since the 1950s and 60s.

When FOIA was first drafted at the end of the last century, it was a radically different working world. The internet and email were still relatively recent tools. The role that social media, smartphone and messenger apps would play in how we now communicate were largely the stuff of science fiction. Government was still mostly operating in a paper-based world, where telephone calls and meetings were formally minuted and what constituted a public record was a matter of longstanding fact.

That is arguably no longer the case. The pandemic has simply accelerated us towards ways of working that were already increasingly in use.

Conversations now take place over messenger apps rather than in person or on the phone.

Video calls, with chat functions on short retention schedules, are more frequently used, following the impact of the pandemic on how we work.

While more staff are likely to spend their working week at home rather than in the office.

The question that our investigation into practices at DHSC has brought to the fore, is whether these changes are having unintended consequences for the quality of record keeping by public authorities. At the same time, it is important to understand what impact these changes may be having on the ability to follow the statutory duties set out in FOIA, such as the swift location of records subject to requests.

Looking beyond DHSC

Although our investigation has only looked at the handling of information by DHSC, it is highly likely that some of the issues we have identified are not restricted to just one Government department. We have seen direct evidence demonstrating this, both during our investigation and emerging in the wider public domain during the pandemic.

For example:

- Evidence provided by DHSC during our investigation which outlined separate exchanges between a Minister on a personal email account and officials at two other departments, that were not copied to DHSC officials. These were in fact saved on corporate systems (as indicated by the fact that DHSC was able to share them as evidence) but is indicative that the risks highlighted about DHSC apply to other departments.
- The Prime Minister's former Chief Advisor, Dominic Cummings, provided detailed oral evidence to Parliament on 26 May 2021. This included extensive reference to WhatsApp exchanges with the Prime Minister and others about matters relevant to the handling of the pandemic. The extent to which the Cabinet Office itself has retained these records remains unclear. Although, this is an issue we are keeping under review as we consider FOI complaints that may be relevant in this area. The Commissioner's own decision notice[10] on a related matter is also relevant.
- A recent ruling by the High Court[11] has highlighted how parts of Government actively facilitate the use of private communication channels.

Outside the issue of private communication channels, there are also issues with the use of different technologies. In a witness statement[12] published as part of Judicial Review proceedings, Lord Bethell set out how WhatsApp account on his phone often became "overwhelmed" due to the volume of pandemic communications he was involved with over that channel. He said he would delete and reinstall WhatsApp to clear space, working on an assumption that a back up was 'automatically' created. He also notes in the witness statement that the DHSC IT team had subsequently told him that this 'may' not be the case. This demonstrates a lack of certainty at multiple levels about how such technology was working in practice and what its impact on the quality of record keeping may have been during this period.

Evidence elsewhere in the public domain suggests that DHSC and its Ministers are not necessarily isolated examples of failing to account for the impact of such working practices. In the recent Greensill lobbying case, for example, there have been reports about both Ministers[13] and senior officials[14] deleting or losing information on their phones for different reasons. Some of this information had subsequently been requested under FOI or as part of parliamentary proceedings[15] and indicates the need for more consideration about how non-corporate technology is working in practice across Government and what improvements could be made in this area.

[10] https://ico.org.uk/media/action-weve-taken/decision-notices/2022/4020076/ic-40467-c7k2.pdf
[11] AtC GLP final judgment (judiciary.uk)
[12] Lord Bethell's witness statement
[13] Minister deleted his texts with Cameron about Greensill | News | The Times
[14] Greensill: Treasury releases perm sec's texts to Cameron (civilserviceworld.com)
[15] Lessons from Greensill Capital (parliament.uk)

The Institute for Government also published a report in March 2022 'WhatsApp in Government', which looked at the use of private correspondence channels across Government.

This report included a range of evidence, including the response to an FOI request it submitted across Whitehall about the use of non-corporate communication channels and messenger apps. The responses it received clearly showed significant inconsistencies in practice across Whitehall. The report highlighted concerns, which we agree with, about "major risks to good decision making in government" if these practices continue unchecked.

Such ways of working, without proper processes and procedures in place, run the risk of potentially serious breaches of the requirements of the Section 46 code, as well as various provisions of the DPA 2018 and UK GDPR.

Immediate actions for public bodies

It is the Commissioner's view that many of the measures he has outlined that DHSC should take, should also be taken by other Government departments.

That is why we are writing to all Departmental SIROs, DPOs and officials responsible for handling FOI requests. We recommend that they should review their internal guidance and working practices to ensure they are consistent with the recommendations we have made to DHSC.

We also recommend that departmental Permanent Secretaries or SIROs write to their arms-length bodies to recommend they conduct a similar exercise. However, they should retain records of the versions of the guidance in place during the time of the pandemic, in case they are required by the COVID-19 Inquiry.

Other public bodies should also consider reviewing their current practices in light of our recommendations and findings, if they are subject to the relevant information rights legislation.

The case for a review of working practices and the law

As our investigation has highlighted, there are clear issues in parts of Government with how clear and consistent the framework, policies and procedures are in practice, that Ministers, officials and others are expected to follow.

To help address this, we have also considered whether there is learning from elsewhere that would inform any wider recommendations.

Recent years have seen an increasing focus on the idea of a 'duty to document' in some Western democracies. The principle is to move the requirement to create records towards a stronger legal requirement on the public officials and elected representatives responsible for creating them. This can then be underpinned by strong

record management practices and standards, with independent oversight and sanctions for non-compliance.

For example, New Zealand and Canada have relatively recently both updated their statutory requirements around the creation of records. Closer to home this has also been a live issue. The Functioning of Government (Miscellaneous Provisions) Act (Northern Ireland) 2021 at sections 6 and 8, and The Public Records (Scotland) Act 2011, both contain a duty to document in relation to various aspects of public administration. The UK is therefore arguably out of step by not having considered its current practices in more detail in recent years.

A new duty to document does not need to be onerous or require much change to current expectations. It may, however, stop the erosion we think may be occurring to the public record due to more modern ways of working.

The focus of an updated duty to document is not likely to be on the creation of more records. But rather on respecifying the need to create and retain the right records. As well as clarifying the responsibilities that exist on individuals across the public sector to adhere to this duty.

Of course, it may be the case that our current legislation is considered strong enough. On closer examination, it may be that there is instead a stronger case for keeping the law as it stands and perhaps updating some of the policies and procedures that sit around it.

For example, this may include:

- updating the section 45, section 46, Civil Service or Ministerial codes or both, to make clearer the responsibility of individuals for maintaining the quality of the public record;
- creating single, consistent processes to ensure records are kept of which individuals are allowed to operate outside departmental systems; and
- updating how relevant information is regularly captured from these accounts and devices.

Whatever the answers may be, we think that these are issues that Government need to consider separately. We have requested that the COVID-19 Public Inquiry update its terms of reference to consider the quality of record keeping. However, some of the wider evidence highlighted in this chapter demonstrates that the issues stretch beyond simply the handling of the pandemic.

They are instead representative of a cultural drift across significant pockets of the public sector towards the benefits of new technology. Unfortunately, this drift has not also included a strategic appraisal of the risks and issues they may present. Nor has there been a system-wide consideration of the measures that Government may need to put in place to mitigate these.

There now needs to be more strategic consideration by the civil service of how to better support the Ministers and others that come in and out of departments to comply with information law. This includes supporting them to understand the importance of maintaining an accurate, complete and up-to-date public record.

To that end, we are also recommending that the Cabinet Office establishes a strategic review into how different, non-corporate communication channels are being used across Government. This should identify any systemic risks and areas for improvement, as well as whether there should be greater consistency in approach across departments. This is in addition and separate to the more immediate measures we have outlined for DHSC.

Our initial suggestions for what such a review could explore include:

- What consistent protocols could or should be developed for public bodies that balance an assessment of the benefits that new technologies can bring with the risks they may present. This could inform decisions about how or whether they are appropriate for official use. This may include keeping central records of all those individuals 'permitted' to use private accounts, channels and devices. As well as clear processes for regularly capturing this information, including when individuals leave post quickly, such as at Ministerial reshuffles.
- Whether the Ministerial, Civil Service or other codes should be strengthened to make clearer the responsibilities of officials and key decision-makers to maintain a public record and ensure compliance with information rights law.
- How effective the arrangements are for Ministers, NEDs, consultants, expert advisers, and others who are active professionally outside their departmental roles, to conduct their official business safely and securely and comply with their information management responsibilities.
- The review may also usefully consider, either initially or in a second phase depending on its findings, whether there are ways that information rights law itself needs to be strengthened to take account of the changes in technology that have developed over the last two decades. This could include consideration of how more recent international law examples around the duty to document could be adapted for the UK or whether FOI and its codes could be strengthened and updated. We appreciate that these are areas that will require wider discussion around government, however.

The ICO's regulatory approach

The ICO stands ready to support individual departments in implementing any changes they identify as necessary following this report. As well as any overall review that is established in line with the recommendations we have made in this report. We hope our recommendations for the review we have outlined are accepted and that this is set up quickly.

In the meantime, we will be looking at what more we can do to ensure that working practices across government remain consistent with both the law and the good practice that the Commissioner has a duty to promote.

To that end, we will take the following actions:

- Ensure our future audits of public bodies examine the use of private messaging channels in the context of the issues highlighted in this report.
- Scrutinise carefully the responses we receive from public bodies regarding complaints about the handling of information requests where information may be held in private communication channels. Use our statutory powers more proactively to ensure public bodies provide a complete record (including confirmation that private messaging channels have been checked where this may be relevant). This means we can be confident they are following good practice.
- Discuss with the National Archives how we can put in place a streamlined consultation process for practice recommendations related to the Section 46 code, where we identify these may be necessary.
- Publish new guidance on the Section 46 code to highlight further the good practice that organisations should follow in meeting their responsibilities. Issue guidance on the data protection compliance considerations we expect to be in place, where the use of non-corporate communication channels is permitted.

Annex A

Data Protection Act 2018 and General Data Protection Regulations 2016 and UK General Data Protection Regulations – key findings

The investigation has determined that personal data has not been appropriately handled, in the main relating to the professional roles of DHSC employees and others associated with DHSC's work during the compliance period of concern.

This is due to the use of private correspondence channels, without appropriate controls in place to sufficiently manage the risks such processing presented.

This, in combination with other linked compliance requirements, led to serious contraventions of the following requirements of the UK General Data Protection Regulations:

- **Article 5 1 (e)** – Storage limitation
- **Article 5 (1) (f) & Article 32** – Security
- **Article 25** – Data Protection by Design and Default

To address the concerns identified, and to improve compliance, it is recommended that if DHSC is to continue to incorporate the use of private correspondence channels, that it take the following steps:

1. In order to improve compliance with article 5 (1) (f) and article 32 of the UKGDPR, the DHSC should undertake a review to assess the security and access controls in place in relation to the platforms in regular use (Google Mail, Hotmail, Whatsapp) when exchanging communications that contain personal data, and to confirm their appropriateness and suitability to support DHSC's compliance with the UKGDPR and DPA18.

2. As part of that review process, to assess the aforementioned platforms terms and conditions and privacy notices to understand how information would be processed, where it would be stored, and to consider any implications for (a) the security of those platforms in relation to the potential for third party access, (b) the extent to which storage limitation is place, (c) the extent to which the data protection by design and default requirements can be met if use of the platforms is to continue.

3. The DHSC should also require users of the platforms to adhere to appropriate security guidance, such as that issued by the National Cyber Security Centre (NCSC) with regard to:

    - Minimum authentication requirements, for example, two factor authentication controls; and

- Remote access controls (taking into account the ability to access from multiple devices; and to remain logged into accounts)

4. The Department should also review secure 'bring your own device' options for controlled access to official DHSC accounts via personal devices, in line with NCSC Guidance.

5. In order to improve compliance with article 5 (1) (e) of the UKGDPR, the DHSC should limit the situations under which such accounts (Google Mail, Hotmail, Whatsapp) can be used to prevent routine processing on such platforms.

6. In addition, the DHSC should set clear requirements for the deletion of information from personal accounts once added to the official record.

7. Further, the DHSC should ensure that the use of personal devices when exchanging personal data adheres to data minimisation principles.

8. In order to improve compliance with Article 25 of the UKGDPR, the DHSC should extend the application of DHSC specific policies and procedures relating to email use to all holders of @dhsc.gov.uk accounts as standard (including to Non-Executive Directors and Ministers). If this is not possible, tailored information to official account holders exempted from the policies, should be provided as part of their induction processes.

Annex B

Freedom of Information Act 2000 (Section 48)

Practice Recommendation

Date:	**11 July 2022**
Public Authority:	**Department of Health & Social Care**
Address:	**39 Victoria Street** **London** **SW1H 0EU**

Foreword

In response to the notices that we issued, the Department of Health & Social Care (DHSC) sent out a questionnaire to a wide range of staff to identify information that may be caught within their scope. As part of this exercise, DHSC notified us that it had identified that official information had been shared through:

- 29 private WhatsApp accounts;
- 17 private text accounts;
- 8 private email accounts; and
- 1 private LinkedIn account

1. In July 2021, the Information Commissioner received complaints, including from the COVID-19 Bereaved Families for Justice Campaign, about media reports in the Sunday Times regarding the alleged use of private correspondence channels by Ministers in the DHSC to conduct official government business during the pandemic.

2. In particular, the Campaign set out their concerns about what such practices, if happening, "may mean for those seeking transparency and accountability regarding the many life and death decisions taken in the Department of Health during the pandemic".

3. They also raised questions about any potential implications for the subsequent Inquiry into the handling of COVID-19 that the UK Government had already committed to at the time of the media reports.

4. After consideration of the information available at that point, on 6 July 2021, the then Commissioner announced[16] that she was launching an investigation into the alleged use of private communication channels at the DHSC. This included investigating DHSC's Freedom of Information Act (FOIA) handling practices.

5. The Commissioner is required by law to ensure compliance with a range of information rights legislation. Under FOIA, there are codes of practice that the Commissioner is required to promote about how departments should manage information and the handling of FOI requests.

6. The Commissioner issued a FOIA Information Notice (IN) to DHSC on 5 July 2021, requiring it to provide specific information by a set deadline, 6 August 2021. DHSC requested and were given extensions to this deadline.

7. On 17 September, DHSC, as requested, provided an indicative timeline for providing the outstanding information by 31 October and confirmed its agreement to an on-site visit at DHSC.

8. A virtual site visit took place on 7 October 2021 and an on-site visit followed on 25 October 2021. DHSC gave a presentation during the on-site visit which included some informative information and illustrative examples. However, when asked to send this presentation and information to the Commissioner to assist with the investigation, DHSC stated it would not provide it.

9. Prior to the virtual site visit, DHSC provided some additional information on 4 October 2021. This was mainly around when it communicated relevant policies and procedures to staff, officials, Ministers and SPADs; information about the use of private communications channels; and a log of FOI requests over a set period.

10. The Commissioner has now investigated and considered in detail the information and explanations DHSC has provided in response to the FOIA IN and the subsequent follow-up enquiries.

11. The Commissioner has reached the view that DHSC's request handling practices do not conform to the section 45 Freedom of Information Code of Practice, issued by the Cabinet Office in July 2018 (the Code).

[16] Blog: ICO launches investigation into the use of private correspondence channels at the Department of Health and Social Care | ICO

12. The Commissioner considers that DHSC's practices do not conform with the following sections of the code:

    - Part 1 – relating to right of access
    - Part 4 – relating to time limits for responding to requests
    - Part 10 – relating to communication with the requester

13. Therefore, in accordance with section 48(1) of the Freedom of Information Act 2000 (FOIA), the Commissioner has elected to issue the following practice recommendation in relation to DHSC's performance under the s.45 Code. The Commissioner has also made broader recommendations to the UK Government as a whole in relation to its record management practices in a separate report he has laid before Parliament. This recommendation should be read alongside that report, which provides further detail on the evidence informing this practice recommendation.

Summary

14. Given the practice at DHSC of some Ministers and Non-Executive Directors using non-corporate, private correspondence and communication channels for conducting official business, the Commissioner has genuine concerns that information which should form part of DHSC's official record may not have been retained or accessible for the purposes of properly responding to legitimate FOI requests. These practices, which senior officials within DHSC were aware of, had the effect of undermining the concept of all official information being held and accessible via a single corporately controlled system.

15. To ensure that information relevant to our investigation was appropriately retained a FOIA IN was issued. It required information including:

    - any policies used by DHSC to inform its compliance with FOIA and its related codes;
    - copies of emails sent to and from private correspondence channels by departmental accounts, including any summaries made by private offices and others, and to give an outline of these exchanges; and
    - examples of recorded contact with Ministers to confirm checks of private email accounts to inform responses to FOIA requests.

16. In practice, DHSC required multiple extensions and provided information in response to the FOIA IN in stages in August, September and October 2021, and January 2022. Subsequent enquiries made on 3 February were responded to on 11 March 2022. DHSC did request

extensions throughout the course of the investigation. It provided the reasons and explanations why it needed such extensions.

Nature of non-conformity

17. The actions of DHSC in response to the IN indicate that its handling of non-corporate communications was not consistent with the expectations set out in the s.45 code.

18. It is clear that the use of non-corporate messaging services was allowed to increase without co-ordinated oversight of their control and use. There was confusion about who ultimately controlled access and there was little, if any, evidence of control of the ongoing departmental access for retrieval or security requirements.

19. During the investigation, DHSC wrote to the ICO confirming that it had located one example of Ministers being requested to search their records for the purposes of an FOI request. Following review of DHSC's request log, the ICO requested information about whether a similar process had been followed in relation to eight specific requests, where it seemed likely such searches may also have been necessary. DHSC refused to provide specific details of the search processes it adopted when dealing with these eight requests. It challenged whether the IN actually covered this line of inquiry and suggested such searches would be too burdensome. The Commissioner can only conclude in light of the evidence available that it is likely such searches did not take place in at least some of these requests.

20. The Commissioner considers that the practices of DHSC in relation to the exercise of its functions under FOIA do not conform with parts 1, 4 and 10 of the code.

Part 1 – Right of access

21. Section 1.1 of the code sets out requestors' rights to be informed whether or not the public authority "holds information meeting the description set out in the request".

22. During the course of the Commissioner's investigation it became clear, as is evidenced by the specific examples in the section below, that this right was not being met.

23. It is also clear from the evidence provided by DHSC, that this right of access was not met on numerous occasions, as referred to in paragraph 29 below, during the period considered in the Commissioner's investigation.

Part 4 – time limits for responding to requests

24. Section 4.1 of the code highlights the "clear" requirement that public authorities respond to requests for information promptly, and within 20 working days of receipt. It should be noted that this was in the context of a significant increase in information requests to DHSC, at a time when resources were extremely stretched as a result of the pandemic. The Commissioner has taken this into account in formulating his regulatory approach.

25. In this case, significant numbers of requesters did not receive a response to their information requests in the period considered by the Commissioner. Many who did receive responses, received them well outside of the expected, in the majority of cases, 20 working days.

26. Based upon the information initially provided by DHSC on 4 October 2021, there were 18 requests over 12 months old; 27 requests over nine months old; 21 requests over six months old; and 113 requests over three months old.

27. The Commissioner asked for further information about eight specific requests on 3 February 2022 (six of which had still been outstanding as at 4 October 2021); a limited response was provided by DHSC on 11 March. This information confirmed that five of the six outstanding requests had received responses since the FOI log was originally provided on 4 October 2021.

DHSC reference	Date of request	Date of response
1268836	04/11/20	24/02/22
1298943	29/01/21	11/03/22
1308894	23/02/21	28/02/22
1330417	14/05/21	Ongoing
1341025	28/06/21	10/03/22
1341231	29/06/21	18/10/21

Part 10 – Communicating with the requester

28. Section 10.2 of the code states that initial responses to requests for information should include:

    - a statement that the request has been dealt with under the Act;

- confirmation that the requested information is held or not held by the public authority or a statement neither confirming or denying whether the information is held;

- the process, contact details and timescales for the public authority's internal review appeals process;

- information about the applicant's further right of appeal to the Information Commissioner and contact details for the Information Commissioner's Office; and

- if some or all of the information cannot be disclosed, details setting out why this is the case, including the sections (with subsections) the public authority is relying on if relevant. When explaining the application of named exemptions, however, public authorities are not expected to provide any information which is itself exempt.

29. Given the evidence in the preceding section on "time limits", it is clear that DHSC has again, in numerous cases, failed to conform with the rights of individual requesters. Again, this is in the context of the volume increases and wider pandemic pressures noted above that the Commissioner has taken into account.

Action recommended

30. In relation to parts 1, 4 and 10 of the code, DHSC must ensure it has appropriate procedures in place to both record and have access to official records. This is necessary to meet its obligations and respond fully, accurately and appropriately to information requests. Also, DHSC must ensure that it issues responses that give effect to the requester's rights of access within 20 working days of receipt of the request. The Commissioner recommends that DHSC should take the following steps to ensure conformity with the Section 45 code:

    - Update guidance for staff on the use of non-corporate channels so it is consistent across the different policies currently used by the department. Cabinet Office have previously indicated that it is updating its own guidance on the use of private correspondence channels, which has been in place since 2013. The Commissioner will work with Cabinet Office, DHSC and others as needed to support the development of this new guidance.

    - Establish a centrally held register of the individuals permitted to use private channels and devices.

- Establish a process for granting this permission that includes confirmation of how, and with what frequency, official information will be transferred onto official systems. This should include specific provision for when individuals leave the department suddenly including, for example, following a Ministerial reshuffle.
- Review and update DHSC's existing information request handling policies and training to ensure they are consistent with the changes made in response to the measures outlined above.
- Follow up with any DHSC Ministers, Non-Executive Directors or senior staff who have left during the pandemic period who may have used private devices and correspondence channels to seek confirmation in writing that all relevant records have been transferred onto the department's systems and seek to secure these where this may not be the case.
- In light of any material that may be received as part of this exercise, review its FOI request log to ensure that this information, if relevant to any requests, is considered for release.
- Write to the Commissioner by the deadline set out in the notice to confirm that it has complied with its recommendations and how it has achieved this.

31. Furthermore, in relation to part 4 of the code, the Commissioner recommends that DHSC should consider using the Commissioner's FOI self-assessment toolkit to improve its timeliness compliance[17]. It is noted that DHSC has already taken steps to improve its performance since the highest point of the pandemic, which is welcomed.

32. In relation to part 10 of the code, DHSC should ensure that it communicates with applicants in accordance with their rights, as set out above.

33. The Commissioner will review progress in these matters after three months to assess the improvements in these areas and feedback his observations to DHSC.

Failure to comply

34. A practice recommendation cannot be directly enforced by the Commissioner. However, failure to comply with a practice

[17] FOI self-assessment toolkit | ICO

recommendation may lead to a failure to comply with FOIA, which in turn may result in further regulatory action. Further, a failure to take account of a practice recommendation may lead in some circumstances to an adverse comment in a report to Parliament by the Commissioner.

35. The Commissioner will have regard to this practice recommendation in his handling of subsequent cases involving DHSC.

Signed .....

Warren Seddon
Director of FoI & Transparency
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Annex C

Extract from correspondence with the Covid Inquiry

05 April 2022

Dear Lady Hallett,

ICO response to consultation on Covid-19 Inquiry draft Terms of Reference

I am writing in response to the consultation you are conducting on the draft Terms of Reference of the UK Covid 19 Inquiry.

The Information Commissioner's Office (ICO) is responsible for regulating data protection and freedom of information law; the following suggestions and questions on the draft terms of reference therefore reflect my statutory remit and how it interacts with the public interest. My predecessor has already set out some key learning points related to the role of data protection and freedom of information during the pandemic[18].

Record keeping during the pandemic

I believe that the quality and standard of record keeping during the pandemic will be an important question when the Inquiry addresses wider issues of decision-making, particularly around policy and procurement. My office is currently undertaking an investigation into the use of private communication channels and the implications for record keeping and freedom of information[19]. Openness and transparency can only work effectively with the underpinning of effective governance and record keeping. It is also vital that this keeps pace with digital technology. The accelerated use of technology during the pandemic exposed the risks.

I also highlight that that under s46 of the Freedom of Information Act 2000 (FOIA), the Secretary of State is required to issue a Code of Practice which provides a framework for public authorities to manage information and records and to comply with their obligations under FOIA and other relevant legislation, such as the Public Records Act 1958. S.2.3.2 of the Code makes clear that public bodies should keep information if it 'needs it for reference or

[18] COVID-19 and information rights: reflections and lessons learnt from the Information Commissioner (November 2021) https://ico.org.uk/media/about-the-ico/documents/4019157/covid-19-report.pdf

[19] Blog: ICO launches investigation into the use of private correspondence channels at the Department of Health and Social Care (July 2021) https://ico.org.uk/about-the-ico/news-and-events/blog-ico-launches-investigation-into-the-use-of-private-correspondence-channels/

accountability purposes' and also in 'exceptional' circumstances including where there may be a public inquiry.

I would therefore suggest amending the second bullet of the first section of the Terms of Reference to read 'how decisions were made, communicated, **recorded** and implemented'.

Transparency

The Inquiry might also want to consider how the cross cutting theme of transparency can be reflected in the Terms of Reference. The 2011 UK Influenza Pandemic Preparedness Strategy noted that 'openness and transparency is central to an effective pandemic response'[20]. This will therefore be relevant to the bullet point above, but will also be an important consideration when looking at the use of personal data in developing and delivering key public health responses, the delivery of government procurement contracts and the safeguarding of public funds.

The Terms of Reference specifically mentions *testing, contact tracing and isolation,* but doesn't refer to *covid status certification*. I would recommend referencing this explicitly on the face of the Terms of Reference as this was also one of the key data driven public health responses during the pandemic and should be included as part of the analysis on *'the availability and use of data and evidence'.* It will also be relevant when the Inquiry looks at the impact on hospitality, leisure and travel. The ICO also recently took enforcement action in respect of the scheme in Scotland[21].

[20] UK Influenza Pandemic Preparedness Strategy - GOV.UK (www.gov.uk)
[21] ICO reprimands Scottish Government over need to be upfront about NHS Scotland COVID Status app's use of people's details (February 2022) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/02/ico-reprimands-scottish-government-over-need-to-be-upfront-about-nhs-scotland-covid-status-app-s-use-of-people-s-details/

E02762926

978-1-5286-3513-4