Information Security Review 2023

Following a number of accidental personal data breaches across the public sector in the summer of 2023 and other high-profile incidents in the preceding five years, the Cabinet Office conducted an internal review in autumn 2023 to identify measures to reduce the Government's susceptibility to data protection incidents.

The review was conducted under the previous administration in 2023.

This report outlines the findings of that review. The names of junior officials within the Terms of Reference have been redacted.

Cabinet Office, 2025

Information Security Review: Final Report

2 November 2023

Executive summary

1. This report is the output of a 3-week review of accidental personal data breaches across the public sector over summer 2023 and other high-profile incidents over the past 5 years. The review was undertaken in September 2023 by a small team of Cabinet Office officials drawn from the Government Security Group (GSG) and the Central Digital and Data Office (CDDO). The report's findings and recommendations were subject to targeted stakeholder consultation in October 2023.

2. The incidents studied were varied in nature. There was no single cause common to all incidents. However, three themes were common to the incidents:
    - a lack of sufficient controls over ad-hoc downloads / exports of aggregations of sensitive data from databases;
    - the release of sensitive information via 'wrong recipient' emails, and the release of membership of sensitive groups through the placing of their addresses in visible fields;
    - the presence of hidden personal data within spreadsheets destined for publication or release.

3. In almost all the incidents public servants were acting in good faith in pursuit of a legitimate business objective, however the common themes suggest a set of short and medium term interventions which we could make across the civil service to help reduce the risk of similar incidents occurring. We have grouped these into four areas:

    - process and governance
    - technology
    - policy
    - culture and training

4. We have identified a set of short term checks aimed at departmental Permanent Secretaries which they can run through with their teams in the very short term to reduce the risk of accidental data breaches in their organisations. These are designed to prompt internal conversations and action - they will not necessarily apply to all organisations and in all circumstances.

5. We have also made a number of recommendations on what central interventions we could make to achieve this aim. These are not prioritised, however there are a number which relate to the cross-government data protection community, both in terms of its oversight but also its standing. This community is critical to driving the data security culture we need if we are to achieve our data ambitions more generally in a resilient and sustainable way. While good information security is at the heart of the recommendations, they are also designed to support responsible information sharing and effective cross departmental working.

2 November 2023

Main report

Aims of the Information Security Review

6. The aims of this review were to:
    - Analyse recent data breaches in the public sector to identify recurring patterns and underlying causes
    - Recommend immediate actions to mitigate the risks of recurrence
    - Recommend longer term actions that build more robust information governance and data safety practices

Summary of recommendations

No.	Action Owner	By end
	PROCESS AND GOVERNANCE	
1	**The Civil Service Chief Operating Officer** should write to Permanent Secretaries providing guidance on practical, user-friendly and business efficient actions to mitigate information security risks.	November 2023
2	**Permanent Secretaries / Accounting Officers** should assure themselves that key principles and processes within their departmental guidance on information security and data protection (including risk management responsibilities) have high visibility on staff intranets.	November 2023
3	**Permanent Secretaries / Accounting Officers** should assure themselves that lead responsibility for data protection in their department is clear and is at the right seniority level relative to the department's risk environment.	November 2023
4	**The Civil Service Operations Board** should commission the Central Digital and Data Office (CDDO) to provide recommendations on strengthening the cross-government approach to information governance, and to deliver an initial scoping action plan.	March 2024
	TECHNOLOGY	
5	**Permanent Secretaries / Accounting Officers** should commission internal business change advice on the adoption of data protection controls set out in the 'Microsoft 365 Guidance for UK Government - Information Protection' and report back to the Civil Service Chief Operating Officer (CS COO) on their intentions by end-January 2024.	January 2024

6	**The Government Security Group and the Central Digital and Data Office in consultation with the National Cyber Security Centre** should jointly undertake a review exercise to assess existing guidance on technical controls for products and services hosting OFFICIAL information.	March 2024
	POLICY	
7	**The Civil Service Operations Board**, or an alternative cross-government board with appropriate decision-making authority, should assume sponsorship from the Chief Operating Officer's Network of the Cross Government Data Protection Committee's review of the data protection community.	November 2023
8	**The Government Security Group** should issue an interim update that addresses clear inconsistencies in its published guidance on the mandated Information Asset Owner role in departments.	November 2023
9	**The Government Security Group and Central Digital and Data Office** should jointly review the Information Asset Owner (IAO) role.	September 2024
10	**The Government Security Group** should update the description in the Government Security Classifications Policy (GSCP) of the Additional Marking 'Personal Data', as part of a scheduled review of the GSCP policy.	March 2024
11	**The National Security Secretariat** should update and strengthen the requirements and the guided best practice for information management and data protection practices in Departmental crisis management arrangements, which are set in the Lead Government Department Guidance.	August 2024
	CULTURE AND TRAINING	
12	**The Government Security Group with the National Technical Authorities** should deliver a cross-government and wider public sector behavioural influence communications campaign to address persistent poor information handling practices. This activity should be reviewed and repeated when appropriate.	November 2023
13	**The Government Security Group** should review, and strengthen where appropriate, the guidance given on data protection and handling of aggregated data sets in the Security and Data training course (which is mandated training for all civil servants).	January 2024
14	**The Government People Group (GPG)** should review sanctions for negligence, including in contexts beyond information security, and make	January 2024

	recommendations accordingly, with a particular focus on situations in which serious injury or loss of life might result from the release of personal data.	

Background

7. A number of serious data breaches took place across the public sector between July and August 2023. These incidents have followed other high-profile breaches over the last five years.

8. The Civil Service Chief Operating Officer commissioned the Government Security Group and Central Digital and Data Office on 4 September 2023 to carry out a three week sprint review of information management and security practices in the Civil Service. The review was completed over 11-29 September 2023.

9. The review took place alongside reviews initiated within the affected public bodies between July and August 2023 and which are exploring the specific incidents in-depth.

Scope

10. The scope of the review was set out in the Terms of Reference which are attached at Appendix 1. In summary, we were to assess:

    - recent major accidental data breaches in the public sector putting individuals at risk.

    - weaknesses in technology, processes, guidance, training and culture that have contributed to the incidents, and/or that may cause future incidents.

11. Although many of the incidents assessed were across the wider public sector, the aim of the review was to identify what lessons could be learnt by central government from these incidents. A full list of the incidents assessed is at Appendix 2.

Methodology

12. The review team researched recent high-profile data beaches to identify if common factors were shared by the incidents. This research was predominantly a desk-based review of open and closed source materials, augmented with in-person insights from relevant stakeholders.

13. The team identified three themes shared by the incidents: the publication of hidden data; the release of sensitive information via email; and, issues associated with the overall management and day-to-day handling of sensitive datasets (including ad-hoc downloads/exports of aggregated data).

14. The review team's focus then switched to exploring the efficacy and feasibility of a wide range of policy, governance, process, technology, cultural and training interventions.

15. Over the course of the review, the team engaged with a range of stakeholders including: Cabinet Office teams (including the National Security Secretariat, the COBR Unit, the Northern Ireland & Ireland Unit, GSG Cyber Directorate and CDDO teams), the Foreign Commonwealth and Development Office, the Ministry of Defence, the National Cyber Security Centre and the heads of the Cross Government Data Protection Committee and the Government KIM Profession.

Assumptions and Limitations

16. The following should be noted of the review's findings and recommendations :
    - The findings are predominantly based on open source materials relating to the incidents reviewed; there was not time to consult all of the affected public bodies. As a result, there are gaps in the review team's understanding of some of the incidents. Where appropriate, the review team has filled some of these gaps by applying reasonable assumptions based on their professional expertise.
    - The review recommendations have not been tested fully with relevant interested parties across government. Neither have we had sufficient time to identify the resources and dependencies required for their implementation. This reflects the sprint nature of the review.
    - In focusing on measures that could prevent recent data breaches across the public sector being repeated in central government, we have not considered the existing or emerging broader information risk landscape i.e. measures to get ahead of underlying causes of the next type of personal data breach.
    - In conducting the analysis and given the limited time available, we deprioritised the assessment of the ransomware attack on Digital ID - a supplier of ID cards and other service to the Metropolitan Police Service, the Greater Manchester Police and other public sector organisations. This has enabled the review to focus more explicitly on accidental data losses and how best to prevent these. There may be some value in a similar review of supply chain incidents to help inform work being taken forward under the Supply Chain Security Strategy and the Government Cyber Security Strategy.

Findings

17. All the incidents reviewed involved an unintended release of information. Each incident had its own specific causes and circumstances - there is no single pattern fitting all of the incidents. However some important shared factors were present across multiple incidents:
    - A reduction in control over data when ad-hoc downloads/exports are made from databases to spreadsheets.
    - The release of sensitive information and identities via email, through 'wrong recipient' emails and through email addresses of people in sensitive groups being placed in visible fields.
    - The risk of accidental publication of 'hidden data' (for example in hidden rows/ columns, obscured tabs and pivot tables), when spreadsheets are published containing statistical data.

18. In almost all the incidents public servants were acting in good faith in pursuit of a legitimate business objective, however the common themes suggest a set of short and medium term interventions which we could make across the civil service to help reduce the risk of similar incidents occurring. We have grouped these into four areas:

    - process and governance
    - technology
    - policy
    - culture and training

19. We have designed the process and governance recommendations as a series of checks that Permanent Secretaries could run through with their teams in the very short term to ensure that the shared factors identified in our analysis are being addressed. Central to these are: a concept of triaging information requests to make sure that those which may involve personal data are identified and additional controls put in place; a strengthening of guidance on data handling for staff working in crisis; a review of guidance to ensure it is accessible and pitched at the right level; and, prompts to adopt the new O365 guidance developed alongside the new security classifications policy, which will help build checks into departments' IT systems. The outline of a draft checklist is at Appendix 3.

20. As well as developing actionable recommendations for departments, the review also considered what central interventions could be made to reduce risk, across the governance, policy, technology and culture and training themes.

21. There is a case to be made that the central governance arrangements for information and data security need strengthening. Information governance cuts across the DDaT and Security functions and the GKIM profession. The GKIM profession and the Cross-Government Data Protection Committee are led on a part-time basis, which impacts their ability to co-ordinate improvements to information governance and achieve consistency across departments. Over the longer term it is also likely to require a clarification of the different roles that exist within departments to protect specific data sets / information assets.

22. Technology can play a key enabling role in reducing the risk of accidental data loss, particularly through work to strengthen our technological controls for users to protect information at the OFFICIAL tier; Microsoft 365 is the day to day working environment of the majority of public servants. The Microsoft Purview Information Protection (MPIP) Guidance for UK Government available on Microsoft.com was developed by Microsoft in collaboration with the Government Security Group GSG), Central Digital and Data Office (CDDO) and National Cyber Security Centre (NCSC). Configuring IT platforms in line with the 365 guidance was recommended to departments (but not mandated) by GSG in June 2023, alongside a substantive update to the Government Security Classification Policy. Amongst other things, adopting this guidance will strengthen perimeter controls and automatically limit distribution of certain kinds of protectively marked information. There is a short term opportunity to drive adoption of this guidance and in the medium term review the guidance available for other similar products. However, the introduction of

technological controls may require concerted business change activity (where departments have varying levels of maturity in this space) and needs to be balanced against the need for collaboration, interoperability and usability.

23. Similarly central policies, standards and even centrally-led lessons sharing are not as well developed in this area as they perhaps might be, falling as they do between different functions and professions. There is a short-term requirement to ensure that the Information Asset Owner policy is brought up to date - it was last refreshed in 2018. However over the medium term, GSG and CDDO should do a more thorough review of this policy with the aim of establishing a single data ownership model for government, and the COBR unit in the National Security Secretariat should embed data handling policy into the central concept of operations for crisis management to complement the actions we are recommending for departments.

24. There is a need to build a data safety culture in which public servants are able to spot unsafe data practices and willing to take action to address such practices. Doing so will also help promote a data sharing culture - confidence in consistently applied safeguards and frameworks will help with some of the broader issues of data management, sharing and re-use. In the short term, we would recommend an internal comms campaign, run by GSG with support from the National Technical Authorities and Security Centres, designed to raise awareness of the risk around sensitive data and signpost where support is available. In the medium term we should review the central training provided on this to ensure it is appropriately hard hitting, engaging and practical.

25. Finally, several individuals we spoke to raised the issues of sanctions and queried whether there was sufficient understanding of what sanctions might be available and how to employ them. Several people noted the potential severity of the consequences associated with some of these accidental data loss incidents and the comparative lack of consequential action. There may be value in exploring further how permanent and temporary employees of central government are held to account where significant data breaches are demonstrably the result of acts of gross negligence.

Recommendations

Process & Governance

Short term process and governance recommendations

Note: While good information security is at the heart of the recommendations, they are designed to also support responsible information sharing and effective cross departmental working.

Note: Recommendations 1-3 are aimed at central government, including Arm's Length Bodies (ALBs). Lead departments will need to assess the extent to which their ALBs should be supported and monitored in implementing the recommendations relevant to them.

26. **Recommendation 1: The Civil Service Chief Operating Officer** should write to Permanent Secretaries by end-October 2023 providing central guidance on practical, user-friendly and business-efficient actions that can be implemented in departments to:
    a. Mitigate risks relating to ad-hoc downloads / exports of personal data from databases
    b. Reduce the risk of 'visible addressee' and 'wrong recipient' email breaches.
    c. Guard against the publication of 'hidden data'

    The Central Digital and Data Office should prepare this letter, with support from the Government Security Group and the National Cyber Security Centre.

27. **Recommendation 2: Permanent Secretaries / Accounting Officers** should assure themselves immediately that key principles and processes within their departmental guidance on information security and data protection (including risk management responsibilities) have high visibility on staff intranets and are drafted in language accessible to all users, and that the guidance is otherwise up to date.

28. **Recommendation 3: Permanent Secretaries / Accounting Officers** should assure themselves immediately that lead responsibility for data protection in their department is clear and is at the right seniority level relative to the department's risk environment. They should have sufficient authority to act as a point of consultation within the department and sufficient time and supporting resources to do so effectively (they would normally be expected to be SCS1 in larger departments). The Joint Heads of the Cross Government Data Protection Committee should be consulted for specific advice on this.

Medium term process and governance recommendations

29. **Recommendation 4: The Civil Service Operations Board** should commission the Central Digital and Data Office (CDDO) to provide recommendations on strengthening the cross-government approach to information governance, with CDDO aiming to deliver an initial scoping plan by end-March 2024. This work should include progressing the Government KIM profession's plans to develop an information governance job family and looking at potential standards and guidance. The Government Security Group should be consulted during the development of these recommendations, along with other key stakeholders across government. Lessons from departmental data handling / information security and governance experiences should be considered in developing a cross-government approach.

Technology

Short term technology recommendation]s

30. **Recommendation 5:** ***(For departments using Microsoft 365 as a core IT platform for working at the OFFICIAL classification)*** **Permanent Secretaries / Accounting Officers** should commission internal business change advice on the

adoption of data protection controls set out in the 'Microsoft 365 Guidance for UK Government - Information Protection' and report back to the the Civil Service Chief Operating Officer (CS COO) on their intentions by end-January 2024. Implementation should be done within existing departmental resource allocations. If appropriate, GSG and CDDO should assist in resolving implementation issues relating to the technical guidance; monitor departmental implementation plans; and, facilitate learning exchanges across departments.

Medium term technology recommendations

31. **Recommendation 6: The Government Security Group and the Central Digital and Data Office in consultation with the National Cyber Security Centre** should jointly undertake a review exercise to assess existing guidance on technical controls for products and services hosting OFFICIAL information by the end-March 2024 (akin to the Microsoft 365 Guidance for UK Government - Information Protection guidance) suitable for all core IT platforms. This exercise might also consider how sensitive OFFICIAL information is currently being processed on third party collaboration tools (such as Trello and Confluence) and knowledge repositories (such as Basecamp and Knowledge Hub).

Policy

Short term policy recommendations

32. **Recommendation 7: The Civil Service Operations Board** (or an alternative cross-government board) with appropriate decision-making authority, should assume sponsorship immediately from the Chief Operating Officer's Network of the Cross Government Data Protection Committee's review of the data protection community. The Board should agree and champion a path to establishing a strong senior leadership voice for consistent data protection practices across government, which feels under-resourced compared to other government functions / professions, in the context of the reputational and financial risks to government of sensitive personal data breaches. The Board should consider arrangements / implications for the Government KIM profession (in which the data protection community currently sits) concurrently in taking a decision. It should also sponsor the formal sharing of lessons from significant government data breaches, drawing on the work of the Information Commissioner's office in this area. The board should also consider recruitment challenges faced by the data protection community.

33. **Recommendation 8: The Government Security Group** should issue an interim update that addresses clear inconsistencies in its published guidance on the mandated Information Asset Owner role in departments, by end-October 2023. The guidance was published in 2013, with a minor refresh in 2018 to reflect the UK GDPR. Inconsistencies have developed in the guidance over time as it has not been maintained in line with related developments in central government. A more substantive update to the guidance is the subject of a separate long-term policy recommendation.

Medium term policy recommendations

34. **Recommendation 9: The Government Security Group and Central Digital and Data Office (CDDO)** should jointly review the future of the Information Asset Owner (IAO) role by September 2024, in tandem with CDDO progress on developing a single data ownership model for central government, as part of the beta phase. If the IAO role is retained, a substantive update of the IAO role guidance should be issued by end-December 2024 and consideration given to a transfer of policy ownership from GSG to CDDO.

35. **Recommendation 10: The Government Security Group (GSG)** should update the description in the Government Security Classifications Policy (GSCP) of the additional marking 'Personal Data', as part of a scheduled refinement of the GSCP policy by end-March 2024. The update should clearly convey for users the potential sensitivities of the Personal Data marking and related handling considerations. GSG should consult the Cross Government Data Protection Committee in developing the updated description.

36. **Recommendation 11: The National Security Secretariat (NSS)** should update and strengthen the requirements and the guided best practice for information management and data protection practices in departments' crisis management arrangements, which are set in the Lead Government Department Guidance (of which a broader refresh is currently being scoped), by end-August 2024. The update should include: signposting data protection expertise within departments and the Information Commissioner's Office (ICO) expectations on preparing for crisis events (including establishing data sharing agreements with likely partners in advance that identify who the lead Department will be), reasonable actions during crisis / threat to life events and a controlled return to business as usual data protection arrangements post-crisis. When departments return to business as usual, a short evaluation should take place, to identify which high-risk data sets need to be moved to more secure platforms (which provide stronger security controls, auditing and manageable processing). The Government Security Group, Central Digital and Data Office, and the Cross Government Data Protection Committee, should support the NSS take this recommendation forward.

Culture & Training

Short term culture and training recommendations

37. **Recommendation 12: The Government Security Group (GSG)** should commission a cross-government and wider public sector behavioural influence communications campaign to address persistent poor information handling practices, for launch by end-November 2023. Lessons (including risk to life, reputational, financial and other significant real world impacts) from recent high profile incidents are an opportunity to shift the dial on these persistent poor practices. GSG should collaborate with the National Protective Security Authority, National Cyber Security Centre and the Security Education and Awareness Centre in developing this campaign. The campaign should emphasise to all civil servants that everyone has a role to play in protecting sensitive information and personal data. The campaign should be repeated, informed by evaluation activities, following future high-profile incidents.

Medium term culture and training recommendations

38. **Recommendation 13: The Government Security Group (GSG)** should review, and strengthen where appropriate, the guidance given on data protection and handling of aggregated data sets in the Security and Data training course (which is mandated training for all civil servants), by end-January 2024. Consideration should also be given to developing in FY24/25 a further optional module that sits within the Security and Data training course focused on data protection considerations in emergency events. The revised training should be produced in conjunction with the planned cross-government comms campaign. It could be promoted to the crisis management community via the National Security Secretariat COBR Unit's Crisis Management Excellence Programme. GSG should consult the Cross Government Data Protection Committee (CGDPC) in taking forward this recommendation, with advice sought from the Information Commissioner's Office via existing CGDPC arrangements.

39. **Recommendation 14: The Government People Group (GPG)** should review sanctions for negligence, including in contexts beyond information security, and make recommendations accordingly, with a particular focus on situations in which serious injury or loss of life might result from the release of personal data. The issue of what sanctions were available to departments when serious accidental data breaches have occurred came up with several individuals we interviewed during the review. The anecdotal evidence they provided was that there was limited guidance available on this within departments. Given the severity of some of the potential impacts in these incidents, we recommend a short GPG-led exercise to determine what options are available and test whether we could go further.

List of appendices

Appendix 1: Terms of Reference

Appendix 2: Overview of incidents reviewed

Appendix 3: Checklist for Permanent Secretaries and Accounting Officers

Appendix 1: Terms of Reference

Internal Review of Information Security Practice 2023
Terms of Reference and Project Plan

Time frame

6-29 September 2023

Objectives

The objective of this diagnostic review is to reduce the vulnerability of central government to harmful data breaches. A series of recent incidents have involved the inadvertent and inappropriate sharing of sensitive information about individuals, putting them at risk of harm.

This short review analyses these incidents and their context with a view to:

- establishing commonalities in their causes;
- arriving at recommendations for central government technology, processes, policy, training and culture to improve information security; and/or where further research is required.

Scope

The scope of the review is:

- recent major data breaches that have put individuals at risk;
- any weaknesses in technology, processes, guidance, training and culture that have contributed to such leaks, and/or that may cause future leaks.

The risk of cyber attack, and incidents involving actual cyber attacks, are out of scope of this review (with the exception of the Met Police ransomware incident, from which lessons about supplier-held sensitive information may be derived).

Review Team

The team will comprise:

- Tom Bramley, Government Security Group [Lead]; supported by [redacted] and [redacted]
- Sue Bateman, Central Digital and Data Office; supported by [redacted] and
- [redacted], the Civil Service Chief Operating Officer's Private Office

Methodology

The team will make use of previous lessons learned studies, supplemented by interviews with key experts and stakeholders.

The team will produce three short reports:

- 15 September: findings from analysis of incidents under review
- 22 September: findings from analysis of themes
- 29 September: recommendations of the review

Stream 1 - analysis of incidents

The review will examine the data breaches listed in Appendix 2. For the purposes of the review the incidents have been assigned to two tiers. The majority of attention will be focused on two (tier 1) incidents. The review will also take into account a further eight (tier 2) incidents.

The themes listed below will frame the review of these incidents. The analysis may identify additional common themes.

Stream 2 - exploration of themes

The team will:

- assess the adequacy of government technology, guidance, processes and culture in the identified thematic areas;
- Identify the government's strengths, weaknesses, opportunities and threats in each thematic area.

The team will also seek to identify examples of good data safety practices from highly regulated industries and safety critical industries.

Stream 3 - recommendations

The team will arrive at recommendations for improving practice around the creation, maintenance, protection and sharing of sensitive datasets, including when the government is working at pace; and/or where further research is required outside this review**.**

Thematic areas

- Pre-publication procedures for the release of government information;
- Risks of redaction failures in different digital tools and formats;
- Management of information in the transition from crisis response to business-as-usual;
- Identification and management of sensitive datasets
- Awareness of risks arising from ad hoc aggregations of data
- Risks of use of spreadsheets when handling sensitive data
- Controls and training on the interface between OFFICIAL systems and the external world
- Accountability and responsibilities at senior and individual levels;
- Promptness and effectiveness of Government responses to serious data breaches

Appendix 2: Overview of incidents reviewed

1. Police Service of Northern Ireland (PSNI), 2023

What happened: Three data breaches in August 2023. The review focused on the 8 August incident where personal details (surname, initials, rank/grade, role, service number, department, location, duty type and gender) of all serving c10,000 PSNI officers and staff were published in an FOI response.

The data was accessible on the WhatDoTheyKnow website for up to three hours before it was removed. The then PSNI Chief Constable, Simon Byrne, guided in a public statement on 14 September 2023 that the PSNI was confident that Dissident Republicans had secured access to the data.

Causes: The personal data was contained in a separate worksheet within the main spreadsheet and was not spotted during checks. The spreadsheet was a routine download from a Human Resources database.

Impacts: Serious consequences have resulted from the data breach: there are concerns about the safety of individuals and their families; the reputation of the PSNI as an employer has been undermined; and, there is a significant financial cost to the incident - “recovery” and future litigation costs were estimated at £174-217m by PSNI Assistant Chief Constable Chris Todd at a House of Commons evidence session on 5 September 2023.

2. Digital ID, 2023

What happened: Digital ID (a supplier of ID cards to the Metropolitan Police Service and Greater Manchester Police) was the victim of a ransomware attack in August 2023. Digital ID had access to 47,000 ID records for Met Police officers, staff, and contractors - the name, rank, vetting status, vetting expiry date and a photograph of individuals. A criminal investigation led by the National Crime Agency is underway.

**This incident was de-scoped in Week 2 of the review. The central government response to issues arising from this cyber attack are being taken forward as part of the Supply Chain Security Strategy and the Government Cyber Security Strategy.*

3. Norfolk Police and Suffolk Police, 2021-2023

What happened: In August 2023, Norfolk and Suffolk police announced the accidental publication of personal data relating to 1,230 sexual abuse victims, witnesses and suspects. These were published on their website between 2021 and 2022. It followed a November 2022 announcement from Suffolk police that personal information about victims of sexual abuse had been made accessible via the constabulary’s website

Causes: The data was present (hidden) in files provided in response to a series of FOI requests between 2021 and 2022 for crime statistics.

Impact: Details of the serious consequences of this data breach are not publicly available. An ICO investigation is ongoing.

4. Ministry of Defence, 2023

What happened: In July 2023, it was reported that the MoD had opened an investigation after a 'small number' of emails had been misdirected to an email domain registered in Mali (the '.ml' domain, as opposed to the US military operated '.mil' domain). Some emails contained sensitive defence research into hypersonic missiles and names of staff working on the project.

Causes: Human error in inputting email addresses.

Impact: The incident could have caused serious damage to the operational effectiveness or security of UK or allied forces. Media attention on the incident focused on Mali's close relationship with Russia.

5. Ministry of Defence, 2021

What happened: In September 2021, 245 applicants for Afghan Relocation and Assistance Policy (ARAP) were emailed in copy rather than blind copy. The applicants had all provided services for the British forces in Afghanistan. There was a risk that if the email was intercepted (or forwarded to) the Taliban authorities that reprisals could be taken against them.

Causes: The email addresses of the applicants were placed in copy rather than blind copy field; profile pictures were also involved.

Impact: Increased risk of threat to life, safety and liberty of individuals.

6. NHS Lanarkshire, 2020

What happened: Confidential patient information was shared on over 500 occasions during the pandemic through an unauthorised WhatsApp group with 26 staff members. Images and videos, which included clinical information, were also shared. A non-staff member was added to the WhatsApp group by mistake, resulting in the disclosure of personal information to an unauthorised individual.

Causes: WhatsApp was not approved by NHS Lanarkshire for processing patient data and was adopted by staff without the organisation's knowledge. The WhatsApp group was initially set up in April 2020 to deal with Covid admin and crisis planning, but its purpose gradually drifted. No Data Protection Impact Assessment was in place for use of WhatsApp and information governance around the use of WhatsApp was unclear.

Impacts: NHS Lanarkshire received an ICO reprimand available here. The ICO noted there is potential for distress to be caused to data subjects if they were to be made aware of this matter i.e. concerns that their personal data has been processed inappropriately and result in a lack of trust with NHS Lanarkshire overall, which could discourage them from using its services.

7. Department for Work & Pensions, 2020 & 2021

What happened: (2020) The Daily Mirror reported that National Insurance numbers and routine benefit payments of 6,000 disability claimants were published online by DWP for more than two years.

** This incident was de-scoped following a period of desk research. The review found no record of the incident in DWP's own report of recent data breaches and no record of any ICO investigation. DWP may be able to shed further light on this incident at a later date.*

What happened: 2021: On 24 August 2021 DWP were informed by an affected data subject that their Child maintenance appeals division (CM Appeals) had been sending out appeals bundles with personal information unredacted. This included the address of a data subject to their ex-partner with a history of domestic violence.

Causes: The personal information had been redacted in the digital version, but appeared unredacted when the documents were printed out. The cause of the incident was that the redaction software (which had been used successfully in other parts of DWP) proved not to be compatible with the system used by CM Appeals to investigate appeals. No testing or data protection impact assessment (DPIA) was completed before implementing the application into CM Appeals because DWP did not consider it necessary due to the application already being used in other service areas of DWP.

Impacts: In October 2022 the ICO issued a reprimand notice to DWP in relation to the incident. The impacts of the incident could have potentially had serious consequences directly threatening an individual's life, liberty or safety.

8. Public Health Wales, 2020

What happened: Details of 18,105 people (initials, date of birth, geographical area and sex) who had tested positive for coronavirus were mistakenly published and available online for 20 hours.

Causes: The incident was blamed on human error when the information was uploaded to a public server searchable by anyone using the site. A member of staff was uploading the data to Tableau, a business intelligence software used by PHW. They clicked to publish on the public facing server rather than the internal restricted one. The data was designed to be identifiable only by those with other detailed information on recent cases,

who already needed to have access to named patient data. PHW said the information was viewed 56 times before it was removed..

Impacts: An independent investigation was conducted. Its findings are publically available. We are unclear if the ICO investigation has concluded.

9. Cabinet Office, 2019

What happened: The Cabinet Office inadvertently published on gov.uk a comma separated variable (CSV) file on GOV.UK containing the names of more than 1,000 people recipients of honours due to be listed in the 2020 New Year Honours list.

Unbeknown to the Cabinet Office the list published contained personal address details of some of the recipients. The personal data was available online for a period of two hours and 21 minutes and it was accessed 3,872 times.

Causes: The Honours and Appointments Secretariat (HAS) in the Cabinet Office had introduced a new IT system in 2019 to process the public nominations for the New Year Honours. The IT system was set up incorrectly by the Cabinet Office, which meant that the system generated a CSV file that included postal address data. Due to tight timescales to get the New Year Honours list published, the HAS operations team decided to amend the file instead of modifying the IT system. However, each time a new file version was generated, the postal address data was automatically included in the file. The Cabinet Office confirmed that there was no specific or written process in place in HAS at the time to sign off documents and content containing personal data prior to being sent for publication.

Impacts: Details taken from the ICO penalty notice: there is evidence that the data breach has caused distress to some of the affected data subjects. The ICO has received three complaints from affected data subjects raising personal safety concerns resulting from the breach. The Cabinet Office has also been contacted by 30 affected data subjects with 27 of those contacts relating to concerns about the possible impact on the individual's personal safety, largely as a result of pre-existing considerations. The Cabinet Office was fined £500,000.

10. Independent Inquiry into Child Sexual Abuse, 2017

What happened: In 2017, 52 email addresses containing full names of 90 victims of child sexual abuse were entered into the ‘cc’ field. The breach was exacerbated when follow-up emails generated by IICSA asking for the emails to be deleted generated “reply all” responses from respondents.

Causes: The ICO report contains a detailed summary of how the error happened and how it was made worse. The ICO reported that IICSA failed to use an email account that could send a separate email to each participant and failed to provide staff with any guidance or training on the importance of double-checking that the participant’s email addresses were entered into the ‘bcc’ field. The ICO report highlighted two earlier

breaches that had raised awareness about the risks of sending bulk emails using the ‘bcc’ field.

Impacts: Taken from ICO reprimand: The recipients of the emails could infer that many of the other recipients were victims and survivors of child sexual abuse…that such a contravention would be of kind likely to cause substantial distress to the affected individuals. £200,000 penalty issued by the ICO.

**This incident was added in Week 2 of the review as a useful case study for email related incidents.*

11. HM Revenue & Customs, 2008

What happened: Loss of two compact discs containing details of 7.5 million child benefit claimants.

Causes: Auditors had requested a sample of data from the child benefit claimant. Instead of taking a sample, HMRC downloaded details of everyone in the dataset onto CDs. The CDs were sent by normal post, with no tracking and went missing.

Impacts: The incident prompted an external inquiry led by Sir Gus O’Donnell. Significant damage to public confidence in the Government’s ability to protect personal information. Creation of the Information Asset Ownership regime within government arose out of the O’Donnell review.

Appendix 3: Checklist for Permanent Secretaries and Accounting Officers

This is a short general checklist of measures to reduce the risk of accidental breaches involving personal data. If your department handles a large amount of high risk personal data sets then you may need to go further than these measures. None of these measures are designed to frustrate information sharing or staff working effectively across departments.

1. **Check that your department has safeguards in place to guard against hidden data breaches**

Several recent data breaches in the wider public sector have involved hidden personal data being published in spreadsheets. This is because original source spreadsheets can have hidden columns, hidden rows, obscured tabs and hidden pivot tables.

	Yes/No
Does your department triage information requests (of all descriptions) to identify those that might involve the processing of raw personal data and which therefore need extra checks when responses are released?	
Has your department implemented a moratorium on the disclosure of original source spreadsheets to online platforms in response to FOI requests? This was recommended by the Information Commissioner's Office in a recent Advisory Note to public authorities, which should be read in full. See: https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/information-commissioner-s-office-advisory-note-to-public-authorities/	
Does your department routinely convert spreadsheets and metadata to comma separated files (.csv) for the proposed release of statistical information? Unlike a spreadsheet (.xls) file, features cannot be hidden in .csv file. It makes visible to the reviewer the data that would actually be published.	
Is there a clear escalation process if staff have questions? Is the contact information easily available?	
Is your departmental guidance clear that data safety and publication deadlines are equally important?	

2. **Check that controls are in place when ad-hoc aggregations of personal data are downloaded from structured databases**

There are times when data needs to be extracted from a database, for example when an analysis needs to be performed on the data that cannot be performed inside the database. However once the raw data has left the database it no longer has the technological and

process controls to which it is subject within the database. Unless a similar level of controls is put in place the data is at increased risk.

The aim should not be to prevent aggregations of personal data from being processed outside its database of origin, but rather to ensure that such processing is done safely.

	Yes/No
Do your database owners / users check what justification is provided by internal requestors for personal data?	
Do your database owners / users provide anonymised data in response to requests for personal data where it is appropriate?	

If anonymised data is insufficient and an aggregation of personal data has to be provided…

	Yes/No
Do your database owners / users check that requesters have robust plans in place to protect the data throughout the time that they have custody of it and to ensure that no personal data is included in any analysis that they publish or release?	
Do database owners / users place controls on any spreadsheet that they provide? In the Microsoft 365 environment the ideal such control would be a label that prevents anyone other than listed recipients from opening the file, copying from the file, forwarding from the file or changing the label. In such a model the person performing the analysis would have to go back to the team which owns the database to get the label lifted.	
Are data requestors required to complete a return to the information asset owner (or nearest equivalent) that checks have been completed to remove any raw data from an analysis?	

3. Check that mitigations are in place to reduce the risk of 'visible addressee' and 'wrong recipient' email breaches

Several recent incidents have compromised the identities of people by placing the email addresses of a group in a visible field.The protection of identities of people with sensitive affiliations more generally, requires mitigations against the risk of revealing groups of people with sensitive identities through placing their addresses in visible email address fields.

	Yes/No
Is your department's email system configured to provide a prompt / warning for emails with more than a set number (e.g. 20) of non-government email addresses in a visible field? Such a prompt should advise colleagues to move addresses to bcc.	
Does your department have guidance in place for staff who deal with groups of people with sensitive information profiles or sensitive affiliations?	
Does this guidance cover the need to minimise the number of staff who have access to a distribution list of all the people with that affiliation?	
Is the guidance clear of the need to never place email addresses in visible fields when communicating with such groups? (Addresses should be placed in bcc, or tools such as mail merge should be used)	
Has your department considered using tools such as bulk email services, mail merge, or secure data transfer services when communicating with groups with sensitive information profiles or sensitive affiliations? See ICO guidance on the use of email and security: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/email-and-security/	

4. Check that your department's crisis management planning covers data protection issues

	Yes/No
Do your department's crisis management procedures contain data protection guidance for teams working in crisis, including contact details for your Data Protection Officer / other internal experts?	

Do these procedures articulate the need for a senior-level information asset owner of any ad-hoc sensitive data sets that are created and protocols for sharing the information with partners (including other government departments)?	
Do these procedures make clear that steps should be taken to regularise any sensitive data sets that may have been created / utilised post-crisis?	

5. Check that the information security and data protection advice that is provided to staff is sufficiently user friendly and context specific

Departmental guidance on information security and data protection is often comprehensive on legal and technical requirements. This meets the needs of dedicated specialists, but it can make the key principles of the guidance challenging to ascertain for non-specialists.

	Yes/No
Are the key principles (and related process guides) of your department's information security and data protection guidance highly visible to staff and set out in language accessible to all users?	
Does your department provide context specific guidance to staff who are likely to be handling high risk personal data?	

6. Check that responsibility for data protection is clear and at the right seniority level

The Data Protection Officer role is filled by a range of seniorities across government (ranging from SCS1-G7). The seniority of the role can have implications for the championing of the data protection agenda within departments.

	Yes/No
Are you content that lead responsibility for data protection in your department is clear and that it is at the right seniority level relative to your department's risk environment?	
Does your lead official have sufficient authority to influence within the department and sufficient time and supporting resources to do so effectively?	

Where your department holds a large body of personal data, which, if compromised, could cause palpable harm to individuals (and which may therefore constitute a tier 1 risk):

	Yes/No
Has ownership of the risks relating to that data been clearly assigned to a member of the senior civil service?	
Does your annual audit plan include provision for the audit of security controls on that data?	
Is the data hosted on a suitable IT system and is it correctly classified?	

7. Check that your cloud productivity suite is configured with information security features

Microsoft 365 is the day to day working environment for most departments at the OFFICIAL security classification.

The technical guide **Microsoft 365 Guidance for UK Government - Information Protection'** (produced jointly by Microsoft, GSG, CDDO and NCSC) provides configuration guidance on implementing information protection controls at the OFFICIAL security classification, using Microsoft Purview Information Protection (MPIP). For example, the guidances outlines how to reduce the likelihood of accidental data loss or oversharing by deploying MPIP features to protect access to documents, based on a label selected by a user, and then leveraging additional technical controls (e.g.encryption and restricted sharing) to supplement the visual markings as appropriate.

Adoption of the guidance may require a significant business change effort within departments.

	Yes/No
If your department utilises Microsoft 365 for OFFICIAL IT systems, does your department have a plan in place to adopt the information protection controls outlined in the Microsoft 365 guidance?	
If not, have you received internal business change advice on which you or another senior decision maker can make a decision on adopting the data protection controls set out in the Microsoft 365 guidance?	