Description of the nature and timing of the data breach
On the evening of 30th March 2017 4 spreadsheets containing details of MP Staff pay, holiday entitlement and working patterns were accidentally published on the IPSA public website (http://www.parliamentarystandards.org.uk)
Data subject(s) affected
8,850 lines of data were published which equated to 3,295 unique individuals
Assessment of the risks to the affected individual(s)
The risk has been assessed as [MEDIUM RISK - DISTRESS THAT DOES NOT POTENTIALLY CAUSE SERIOUS DAMAGE]. The justification for this risk assessment is that the data breach spans the three potential damage areas of Financial, Security and Reputational. Although the incident is likely to cause significant distress, there is little risk of it causing serious damage to the individuals concerned. The ICO guidance contains the following definitions: • *"Financial*, if any bank or card details, or other information which may allow someone to impersonate them, find their way into the wrong hands. • *Security*, if personal addresses or other information with which is relevant to a person's security (for example detailed travel arrangements for Northern Ireland MPs) is misplaced. • *Reputational*, if information which could be misused by the media, political opponents, or other individuals, goes astray." Although specific salary information was released, there were no accompanying bank details or National Insurance Numbers. The specific working patterns of individuals were released alongside the name of the MP whom the staff member works for. This may pose a security risk and should be investigated further with security services subject to further review. There is a significant reputational risk for IPSA following this data breach. There is also a reputational risk for MPs who may be targeted by political opponents or the media for the salaries they pay their staff or reward and recognition payments.
The cause of the data breach and the individual(s) responsible

At 16:19 on the day in question, the [redacted] (X) sent an email to the [redacted] (Y) and a [redacted] (Z) asking them to publish new payroll/forms onto the old IPSA website.

At 16:29 the [redacted] replied by email seeking clarification on the content to be published. Email thread as follows:

From: *X*
Sent: *30 March 2017 16:29*
To: *Y, Z*
Subject: *RE: New Payroll Forms*

X,

So delete all the old ones (except HMRC guidance) and upload all of the files in that folder? What about the subfolders?

Y

> ***From:*** *X*
> ***Sent:*** *30 March 2017 16:19*
> ***To:*** *Y, Z*
> ***Subject:*** *New Payroll Forms*
>
> *Hi both,*
>
> *This is where the new payroll forms/letters are; I:\Payroll Forms*
>
> *Sorry I didn't get them over sooner today, if you can get them on the old website for me please. Just in the Staffing folder.*
>
> *You can delete all the other forms/letters in there besides the one called HMRC Tax Guidance 2016.*
>
> *We've spent most of the day tidying them and still have spotted a few anomalies but they are nearly perfect!*
>
> *Thank you*

Y

[redacted]

Independent Parliamentary Standards Authority (IPSA) 4th Floor

30 Millbank

London SW1P 4DU

info@theipsa.org.uk

www.parliamentarystandards.org.uk

Watch our training videos on YouTube to help guide you through IPSA's online expenses system.

This was followed up by a face-to-face discussion where the [redacted] and the [redacted] reviewed the folder contents to be published.
The [redacted] published the agreed contents to the staging website before 16:45.
A scheduled job which copies published content from the staging site onto the live site triggered by 17:00.

In the event, the folder location was incorrect and should have been one of the sub-folders in that directory by the same name. The sub-folder was renamed to 'Payroll Forms for Publication' at 08:53 on 31st March, the morning after the incident.

The face-to-face meeting between the [redacted] and the [redacted] was a missed opportunity to realise the mistake and prevent this incident from occurring.

Remedial action already taken

The [redacted] was made aware of the incident at 20:20 by a staff member from a MPs office.
The [redacted] immediately contacted IPSA internal stakeholders including the interim [redacted] who acted to remove the content from the live public site. This was completed by 21:20.

The interim [redacted] then sought to understand the scale of the exposure by interrogating log files and on the morning of the 31st March the [redacted] also disabled the content publishing scheduled jobs.

Further action that needs to be taken, with timescales

IPSA need to contact each of the affected parties, including the MPs as the employers, individually informing them of the data breach and the specific nature of the breach and how it affects them. This should be completed by Friday 7th April. It might be the case that the contact details we hold for former staff are out of date. We should therefore send these letters by recorded post to ensure that a) we have received back undeliverable letters and b) to evidence that contact was clearly attempted.

IPSA should review its procedures for publishing content onto its old website specifically but across the web platform as a whole. This should be completed by Friday 28th April.

Recommendation as to whether the ICO needs to be informed

In the opinion of the [redacted], this incident is serious and significant and should be reported to the ICO immediately.

Data protection breach notification form

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. Organisation details

(a) * What is the name of your organisation – is it the data controller in respect of this breach?

The Independent Parliamentary Standards Authority (IPSA). IPSA is the data controller in respect of this breach.

(b) Please provide the data controller's registration number. Search the online Data Protection Public Register.

Z2136128

(c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

[redacted]

IPSA
4th Floor, 30 Millbank
London, SW1P 4DU

2. Details of the data protection breach

(a) * Please describe the incident in as much detail as possible.

Four spreadsheets containing data about MPs staff members were accidentally published on our website (http://www.parliamentarystandards.org.uk). The spreadsheets contained data of their employment including salaries, contracted hours, working patterns, holiday entitlement, special arrangements and reward and recognition payments. In two cases there was an indication that the salary was being paid out of a disability budget. There were no details of any specific disability relating to any individual.

(b) * When did the incident happen?

The incident occurred at 17:00 on the evening of the 30th March 2017.

(c) * How did the incident happen?

The data owner for the data to be published sent an incorrect link to the [redacted].

(d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

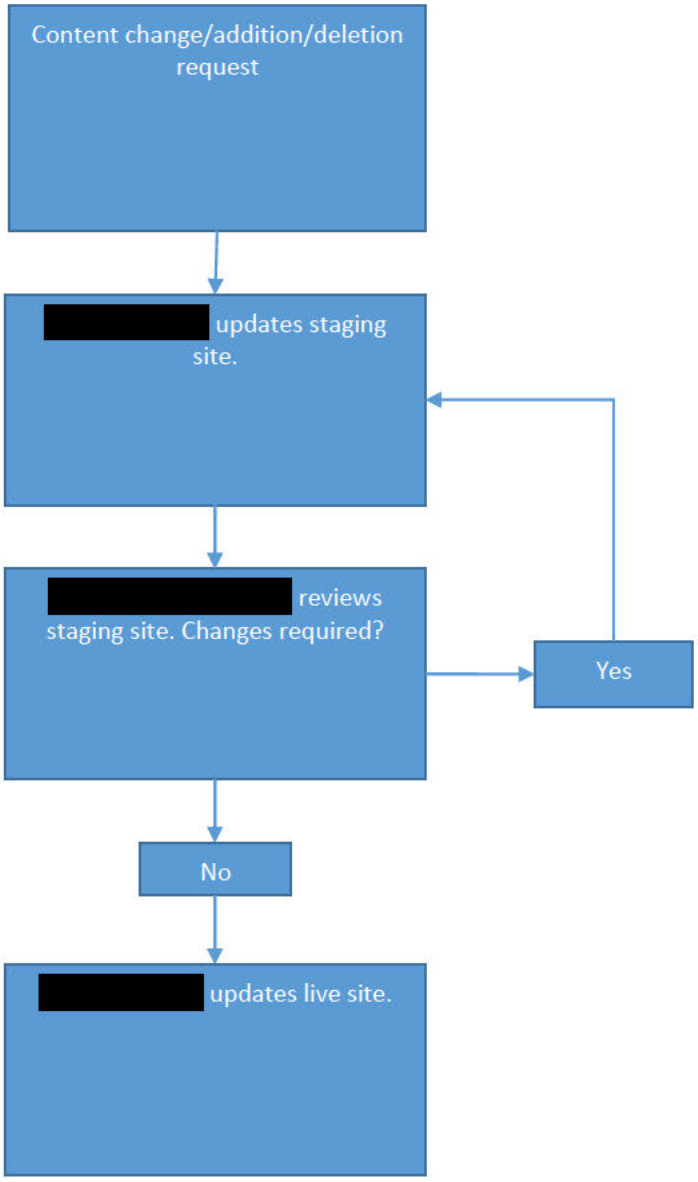
(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

The responsibility for signing off and approving content deployment is devolved to data owners who are expected to review the materials prior to deployment. The content is only published by the [redacted]

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

Process

Content changes will be managed as per below:



3. Personal data placed at risk

(a) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

Staff member names and their employer, salaries, contractual working hours, working patterns, holiday entitlements, special leave arrangements, and reward and recognition payments specific to individuals.

(b) * How many individuals have been affected?

3,295

(c) * Are the affected individuals aware that the incident has occurred?

Those staff members in current employment with an MP have been informed, along with their employer, by way of a personal letter from the CEO but sent as general mailshot. Tailored letters will be sent to each affected individual and MP during week commencing 3rd April 2017. We will attempt to contact former staff members using the contact details we hold by way of a personalised letter sent by registered post. We may not have up to date contact information for some of those individuals.

(d) * What are the potential consequences and adverse effects on those individuals?

The risk has been assessed as [MEDIUM RISK - DISTRESS THAT DOES NOT POTENTIALLY CAUSE SERIOUS DAMAGE]. The justification for this risk assessment is that the data breach spans the three potential damage areas of Financial, Security and Reputational. Although the incident is likely to cause significant distress, there is little risk of it causing serious damage to the individuals concerned in these three areas.

Although specific salary information was released, there were no accompanying bank details or National Insurance Numbers.

The specific working patterns of individuals were released alongside the name of the MP whom the staff member works for. We have consulted on this with NaCTSO who advise that they could not immediately see any risk implications arising from the publication of the working patterns.

However, a slight risk might arise from the release of MPs' staffs' names. For instance, if an individual is easily identifiable, eg if they have an unusual name and a significant internet footprint, and now linked to an MP.

The assessment therefore is that the risk to MPs' security is minimal.

There is a reputational risk for MPs who may be targeted by political opponents or the media for the salaries they pay their staff or reward and recognition payments.

(e) Have any affected individuals complained to the organisation about the incident?

Three individuals had written in to complain at the time of completing this form.

4. Containment and recovery

(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

The data accidentally published was removed from the site immediately upon us becoming aware. It was available on our website for 4 hours and 20 minutes.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

We have contacted a number of the people who had contacted us informing us of the incident and requested that all copies made are permanently deleted.

(c) What steps has your organisation taken to prevent a recurrence of this incident?

In the short term we have disabled all automatic content publication jobs and introduced a mandatory additional check before any new content is published.

For the longer term, we will be reviewing our procedures for publishing content across our entire web platform.

We will also be reinforcing data protection responsibilities across the organisation.

5. Training and guidance

(a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

All staff receive data protection training upon joining and this is repeated on an annual basis.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

Training is mandatory for all staff and was last run in April 2016.

(c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

The ICT Code of Conduct contains guidance on using the protective marking scheme which IPSA applies. This is also covered in mandatory training.

'The Security Classifications System is an administrative system designed to protect information (and other assets) from accidental or deliberate compromise. We use it to ensure access to information and other assets is correctly managed and safeguarded throughout their lifecycle; including creation, storage, transmission and destruction.
Everyone who works at IPSA has a duty to respect the confidentiality and integrity of all information and data

that they access, and is personally accountable for safeguarding assets in line with this policy.
Within IPSA, the Security Classifications System classifies sensitive material into one category, OFFICIAL, which is split into two sub-categories; OFFICIAL and OFFICIAL SENSITIVE. Security Classifications above OFFICIAL must not be transmitted, stored or processed using IPSA systems. These classifications indicate the level of protection required and are usually applied to paper-based documents, electronic documents or data, although they can also be applied to valuables, equipment and operating systems.

It is the responsibility of the originator of the information to apply a security classification as necessary in capitals in the header and footer of every page. The originator should bear in mind the following before applying any protective marking:

- the sensitivity of the information; and
- the possible consequences of that information being compromised or misused

Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of threats.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

Yes

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

We reported an accidental release of a reproduction P11D to the wrong recipient on 8th February 2016, Case Reference Number COM0615690

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

We have spoken to officers at NaCTSO regarding the security aspects of this incident.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

There has been extensive news coverage across national and local press following.

Sending this form

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday)

BOARD PAPER	
Paper ref:	
Agenda item:	

TO: IPSA Board **DATE:** 19 April 2017

FROM: [redacted]

TEL: [redacted]

SUBJECT: **LESSONS LEARNED FROM THE RESPONSE TO THE RECENT DATA BREACH**

ANNEXES: **A. List of interviewees**

Issue

1. I have conducted a lessons learned exercise in respect of our response to the data breach on 30 March.

Timing

2. For the 27 April Board meeting.

Recommendation

3. That the Board notes the lessons learned and planned actions.

Background

Sequence of events

4. The data breach involved four files of personal information being inadvertently uploaded onto IPSA's old website on 30 March at just after 4.30pm. This included MPs' staff names, their employer, salaries, contractual working hours, special leave arrangements and reward and recognition payments linked to individuals. No bank details, addresses or national insurance numbers were involved. The files remained available for viewing on the website for 4 hours and 50 minutes. We became aware

of the error at 8.20pm, when [redacted] was alerted by an MPs' staff member.[1] The information was removed within an hour of [redacted] being alerted.

5. [redacted] by chance, was still in the office, and alerted [redacted] and a number of other IPSA staff. [redacted] went into the office to help remove the data (unsuccessfully). [redacted] also came in and contacted [redacted][2]. They were able to remove the data by 9.20pm. [redacted] stayed until 3am to try to establish how many times the site had been accessed and by whom. This proved difficult, but Folding Space[3] were able to help on Friday.

6. On Friday 31 March, we met at 10am to agree and plan our response (which was already underway) and again at 3pm to monitor progress and agree future actions. During the day an investigation was conducted and a breach notification form was sent to the Information Commissioner's Office (ICO). Lines to take were produced for IPSA staff and a letter to MPs (as employers of the staff) was sent at 4.20pm, after the full facts had been established. This was also released to the media. After some technical difficulties, the MP support phone lines were extended until 6pm.

7. Over the weekend [redacted] worked on the spreadsheets containing the information so that all affected staff could be identified and communicated with. All staff (with the exception of a few whose letters were held until the following day) received a tailored letter on Wednesday 5 April providing them with information on the type of data that had been revealed in their cases, but not the specific individual details, due to the risk of the letters being opened by the wrong person.

8. MPs were provided with an update on Friday 7 April, and this letter was also made public.

9. News coverage of the data breach was extensive on 31 March, but the story did not run beyond that date.

The lessons learned exercise

10. Between 6 and 11 April, I interviewed 14 people who had been involved in the response to the data breach. They are listed in Annex A. I am grateful to everyone for making time at short notice, and for being very open with me. My findings are described in the following section of this paper.

Findings

11. I have structured this part of the paper as follows:

[1] We were first notified by email at 6.03pm, but that email was sent to a mail box which was unmonitored at that time.

[2] [redacted] provide support on Sharepoint, which is the technical platform used for the old website.

[3] Folding Space is the host supplier for the old website.

- For each of the following periods, what went well and what might have been better:
    - The evening of 30 March.
    - Friday 31 March.
    - 3-7 April.
- Lessons learned.

Evening of 30 March

12. What went well:

- The speed of response to the incident, once we became aware of it. There was an element of good fortune here, because [redacted] was still in the office and [redacted] was in the vicinity, so could return quickly to the office.
- Many commented on [redacted] professionalism and calmness, keeping a clear focus on what needed to be done.
- A number of key individuals (though not all) were alerted to the incident and were able to communicate with others. The [redacted] was alerted in the morning.
- [redacted] was able to contact [redacted], even though we do not have an out-of-hours contract with them. This enabled the data to be taken down.

13. What could have been better:

- A number of people, including the [redacted], and the [redacted] did not find out about the breach until Friday morning[4]. [redacted] may have been able to begin the investigation earlier, had [redacted] known.
- It was not possible for any of the communications team to remove the information remotely. It was fortunate that people were able to come to the office quickly. Even then, it needed [redacted] assistance to remove the data.
- The information could have been removed faster if it had been on the new website. However, the "IPSA for MPs" section of the website was, at that point, still hosted on the old IPSA website. The old website takes some time to "refresh" when changes are made to it.

[4] They were emailed at 9.20pm , but not phoned.

- It was difficult to identify the number of views of the data that had taken place while it was on the website. It was only on Friday that this problem was resolved – at least in terms of identifying IP addresses of users.

Friday 31 March

14. What went well:

- There was a real sense of everyone pulling together and supporting those who had been most directly involved in the data breach.
- Decisions were take quickly and clearly. The two planning/monitoring meetings were instrumental in this and both were very well chaired by [redacted].
- The investigation was prompt and thorough and a report was sent to the ICO on the same day.
- Letters and internal briefing were produced quickly (although not quick enough for some – see para 15) and were well-drafted by the communications team.
- The communications team handled calls from the media highly professionally.
- We were open with MPs and the media about what had happened. In the case of the media, this openness and the professionalism of the communications team may have contributed to the story being relatively short-lived.
- The MP support and payroll teams also handled calls from MPs and MPs' staff professionally and helpfully, even when they did not have all the briefing materials.

15. What could have been better:

- We took a decision not to make the data breach public until the investigation had been concluded and we signed off the contents of the letter to MPs at the 3pm meeting. This enabled us to tell MPs that we had reported the incident to the ICO. The result was that the letter was not sent to MPs until 4.08pm and made available to the media until 4.24pm.
- Some people felt that the letter should have been addressed to MPs' staff rather than the MPs, as it was the former whose information was published. MPs are, however, the employers.
- The MP support phone lines close at 5pm. The operations team were able to get the lines re-opened at 5.30pm and used the communications team phone

line between 5 and 5.30pm to take calls. There were some misunderstandings about whether the opening of the lines could be extended. In the event they were kept open until 6pm. There were no calls between 5.30 and 6pm.

- The full lines to take were not made available to the MP support team until 15 minutes after the letter to MPs had been sent. The lines largely replicated what was in the letter, which the team had, but there was concern about this delay.

- Some members of the operations team felt that they had not been fully informed about the details of the data breach until the afternoon. Had they known earlier, they may have been able to make arrangements with the supplier of the MP support phone line sooner.

- Using the term "data breach" is confusing to people outside IPSA who are not data security experts. A number of people thought IPSA's IT systems had been hacked, including the [redacted], who rang [redacted] to ask for clarification. The communications team had to dispel this notion amongst the media.

3-7 April

16. What went well:

- The payroll team and others met a very challenging deadline of sending letters to all staff affected by close on Wednesday, with the exception of a small number of staff, who had worked for more than one MP, so would have been sent more than one letter.

- The MP support and payroll teams handled a large number of calls and worked well together, after some initial misunderstanding about who was doing what.

- A detailed action plan for data security (which goes wider than measures in response to this particular data breach) was put together quickly by [redacted] and [redacted]. This plan is included in the information which has been provided to the Board.

- The lead taken by the communications team in drafting the letters was appreciated by other colleagues.

- The unity and support developed on the previous Friday was maintained.

17. What could have been better:

- The letter to individual staff members contained a tailored paragraph indicating to each person the type of information on them that had been

inadvertently released (eg, salary, reward and recognition) but not the specific details. They were invited to contact the payroll team if they wished to know the detail. They were asked to provide their National Insurance (NI) number as proof of identity. This meant only payroll could take the calls – and some callers were reluctant to provide their NI numbers. Not surprisingly they took a large number of calls. The reason for the approach taken was to avoid the risk of people other than intended recipient opening the letters. But in retrospect the payroll team would have preferred to have included the detailed information in the letters, although they would have taken longer to produce.

- The payroll team had printed off all the individual letters on Tuesday, when some errors in the text were identified. So they all had to be scrapped and re-printed. The second versions had all been put in their envelopes when it was realised that some staff may receive more than one letter. All the letters had to be arranged in alphabetical order to identify duplicates.

- We do not have pre-printed envelopes marked as "private and confidential", so each one had to be individually stamped.

- There was some disagreement on whether the letter to MPs on Friday was sufficiently detailed[5], although I would say it struck the right balance in the end.

- Two early decisions were taken to mitigate against the risk of sending communications to the wrong MPs or staff members: all emails containing personal information have to be checked by a second person, and the auto-fill address function has been removed from our Outlook. The first decision has not been well-received by staff, partly because it adds a good deal of time to each process when people are already hard-pressed. The second decision has caused less reaction, although it did come out of the blue on a Friday afternoon. The context could have been better communicated, perhaps in advance, particularly when neither measure was directly related to the data breach in question.

- There are not enough people in the office with mail-merge skills, which was essential for the mass mailings.

Lessons learned

18. Inevitably, in an exercise like this, the good points are dealt with quickly in interviews and the problems detailed at more length. This is valuable for learning lessons about how to improve, but we should not forget that everyone worked really well together

[5] For example, whether we should say the data was available for 4 hours, during which time it was accessed, or 4 hours 50 minutes, when it was available. In the end we said both.

in response to the data breach. One interviewee described it as "a textbook exercise" and I believe that description is deserved, notwithstanding some of the issues which arose. There was also a real awareness and sensitivity about the impact that the data breach would have on some MPs' staff members.

19. The data security action plan, which accompanies this paper, outlines a range of measures, many of which were in the pipeline before this data breach occurred. Additionally, I have drawn the following lessons from my interviews:

- Although I was considering the response to the data breach, many people rightly commented on some of the contributory factors towards the breach. While it was human error, a tighter governance of website content may have prevented the data being published. We have, in the past, not insisted in all material being approved by a senior person in communications. In hindsight it is easy to say that we should have. From now on we will be doing so.

- While our response was effective, we do not have all the processes written down, for future reference should another incident of this type ever occur. We will do this. It may also be helpful for key managers to be linked through something like a WhatsApp group, so that we can be sure that everyone who needs to know, does know.

- On reflection, it may be advisable, should another incident occur, to issue an initial communication before the investigation is concluded. People can then be updated in due course, and some actions undertaken earlier. The risk in this is that it will lead to people speculating about the nature of the breach.

- We need to establish greater technical flexibility with regard to the opening times of the phone lines and to make people aware that in a crisis they may need to be available to answer calls (two members of staff did remain behind this time).

- We need to make sure that the people who bear the brunt of answering queries – in payroll and MP support – are fully informed and confident that they are equipped for the task. Other decisions, like the one about the degree of detail in the letter to MPs' staff, should also involve them more closely, even if the ultimate decision is the same.

- We should invest in more stocks of envelopes, including pre-printed ones.

- We need to train more people in skills such as mail merge and putting material on the staging site of the website (prior to final approval).

- More internal communication, setting context, is needed before measures like email checking and the removal of auto-fill are introduced.

- We need to reconsider for what we use the term “data breach”. We used this term in this case, because the ICO calls such incidents a “Data Protection Breach”. But the common interpretation is that it describes hacking of the IT system.

20. Where appropriate, these lessons will be incorporated into the data security action plan.

[redacted]

19 April 2017

ANNEX A – PEOPLE INTERVIEWED BETWEEN 6 AND 11 APRIL

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

[redacted]
Independent Parliamentary Standards Authority (IPSA)
4th Floor, 30 Millbank
London
SW1P 4DU

IPSA
29 MAY 2018

25 May 2018

Case reference: **COM0675411**

Dear [redacted]

I write to inform you that I have now completed my investigation into an incident reported to the Information Commissioner on 3 April 2017, regarding the accidental disclosure of personal data into the public domain.

In summary, it is my understanding that on 30 March 2017, four spreadsheets containing information about MPs' staff members were published on your website. These spreadsheets included data about the staff members' employment, including salaries, contracted hours, working patterns and any special arrangements. In two cases, the disclosures contained sensitive personal data, as there were indicators that the salary for these individuals was being paid out of a disability budget.

When the original case officer wrote to you on 10 April 2017, she set out the details of the Information Commissioner's powers. Based on the information you have provided, we have decided that regulatory action is not appropriate in this case. The reasons for this are set out below.

Our consideration of this case

I have investigated whether the Independent Parliamentary Standards Authority (IPSA) has complied with the requirements of the seventh data protection principle, which states that:

"Appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"

The data in this case is considered to constitute sensitive personal data as defined by the DPA.

The following aggravating factors have been noted:

- The lack of an organised file structure and naming convention means that it is easy to see how this error occurred. There was also a lack of a checking process as to content, prior to it being uploaded; which meant that the opportunity to check and control was not there.

- Lack of process and framework meant that the personal data was placed in a folder with the same name as the main header folder. Inherent protections were not in place.

- The volume and nature of the complaints received by IPSA and the ICO evidences serious distress. It is clear the affected data subjects felt very vulnerable, particularly given the political and security climate at the time of the breach.

- Although IPSA concluded that the level of risk was medium from its own assessment, it was still felt seriousness enough to report to NATsCo, as there were inherent security implications as a result of this breach.

- An early opportunity to detect the incident was missed, when an MP's office emailed IPSA at 18:03 (approximately 90 minutes after the breach), to make them aware the file was accessible online. This email was, however, sent to a mailbox which was not monitored outside of office hours.

- Prior to the incident, there were already reports of employees suffering harassment and threats from constituents. This, combined with the fact that the threat level was at SEVERE at the time of the breach (due to the Westminster attack having taken place 8 days earlier), means there should have been additional safeguards in place to ensure the secure processing of personal data concerning MPs and their staff.

However, we acknowledge the remedial steps taken by IPSA in light of this incident and we have noted the following mitigating factors:

- Sufficient training appears to have been in place at the time of the incident, as both the [redacted] involved were experienced and senior members of staff. Mandatory training was in place, and had been undertaken by the two employees in the 12 months preceding the incident.

- Whilst there was no evidence of a previous policy, IPSA have produced a comprehensive 27 point action plan, including a wide range of measures, which should prevent a further incident of this type from occurring.

Whilst the Commissioner is of the opinion that this incident is significant, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action on this occasion. This breach has caused significant distress to the individuals involved; however, we are also recording that IPSA have responded to the gravity of the situation, and accept that significant remedial measures have been set out by IPSA. Given the seriousness of this incident, we expect IPSA to implement the recommendations as fully as possible in order to prevent any recurrence.

The General Data Protection Regulation (GDPR)

As you will be aware, today marks a new era in Data Protection law as the General Data Protection Regulation (GDPR) takes effect. The ICO expects you to implement any changes required to better protect data subjects' data.

The ICO website contains detailed guidance on what organisations need to do to ensure they are compliant with the new legislation (www.ico.org.uk).

Conclusion

Thank you for reporting this incident. This matter is now closed.

I would point out that any further incidents involving IPSA may lead to this matter being revisited, with enforcement action considered as a result.

Please note that we may make additional enquiries if we become aware of new information that affects the circumstances of the case. Further enquiries may lead to the ICO taking formal regulatory action, as set out in the leaflet.

Further information and guidance relating to data security breach management is available on our website at:

http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Yours sincerely

[redacted]
Lead Case Officer
Information Commissioner's Office
[redacted]

We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue. We will publish information in

accordance with our communicating regulatory activity policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policies-and-procedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

SIRO Assurance Data Breach March 2017

TO: [redacted] **DATE:** 14th June 2018

FROM: [redacted]

SUBJECT: **Assurance and Review of Data Security Action Plan post ICO case closure**

Background

IPSA had a data breach last year resulting in 3500 data subjects having aspects of their working patterns and salaries published, and an ICO investigation was opened. This was reported in the national media.

As a result, IPSA conducted its own investigation to identify the cause and failures and developed a Data Security Action Plan. This was submitted to the ICO in co-operation with their investigation.

In late May 2018, the ICO formally responded to close the case without regulatory action. It did have some comments to make on weaknesses, and stressed the need for completion of remediation actions which IPSA committed to take.

Review

Noting an email sent to [redacted] from [redacted] on 31/5/2018, subject "ICO letter - OFFICIAL:SENSITIVE Conclusion of March 2017 Data Breach" which contained a number of internal actions, one of which was to confirm the implementation and provide assurance of the data security action plan. A number of plan elements were completed quickly, others folded into audit trackers.

The Appendix contains the Data Security Action Plan and comments.

Conclusion

The plan identified a number of improvements, some of which contained the immediate risk, including regular refresh of staff training, and some that would need testing and further planning. Knowledge Management remains a maturing process through 2018 with SMT objectives. The new publication process, which has been working successfully, now needs to be finalised and published.

The [redacted] confirm that most items are complete and all others planned and with team objectives. As the SIRO Group is tasked in information improvements in broader planning, and with IAO/SMT objectives set, this specific plan is recommended to be closed. IPSA should be assured that the commitment to improve has been kept and IPSA is not exposed in this case.

Signed [redacted] June 14th 2018

Appendix A

DATA SECURITY ACTION PLAN (effective date: 27/06/2017)

No.	Action	Owner	Target date	RAG status
	Policy			
1.	Revise data breach policy to make more explicit that IPSA has a zero tolerance approach to staff not following established procedures for handling personal data (any individual data breaches still subject to investigation on facts of each case).	[redacted]	5.4	Complete
2.	Quick review and amendment as necessary of policies on retention, archive, disposal, naming conventions and protective marking of documents.	[redacted]	Draft 9.6 Sign-off 30.6 May 2018	Complete IGF and retention updated through GDPR
3.	Communicate policies and procedures on information management to staff. See also knowledge management actions.	[redacted]	From 28.4 To 29.12	Complete
	Knowledge management			
4.	Audit existing network drives access and set revised access permissions as appropriate.	[redacted]	PMO 30.6 Remainder 31.8 Dec 2018	Interim fixes and changes to sharing
5.	Profile files and folders on team drives and prepare focused lists for Information Asset Owners (IAOs). This involves use of an IT tool that will scan the network drives and allowing Information Asset Owners to see our full estate. It will produce metadata that will be interrogated.	[redacted]	29.9 DEC 2018	Data cleanse commissioned through gdpr
6.	Communication and engagement: issue IAOs with guidance on preparing a plan for retention, archiving, disposal and protective marking of documents in team drives; and run training sessions for them.	[redacted]	30.6 May 2018	Complete
7.	Clear out the 'Common' drive and set it as a transient area where documents can be shared. Anything that is there for more than 30 days will be deleted.	[redacted]	31.10 May 2018	New guidance Complete
8.	IAOs complete team folder plans to ensure that all files and folders on team drives are appropriately marked in accordance with the protective marking scheme and have appropriate access permissions.	IAOs	31.10 DEC 2018	SMT objective
9.	IAOs implement their team folder plans.	IAOs	17.11 DEC 2018	SMT objective
10.	Final review by IAOs in conjunction with folder owners.	IAOs	DEC 2018	As above

11.	Review by Business Technology of effectiveness of implementation of plans.	[redacted]	29.12	Guidance to be issued
	Website			
12.	Put in place new process for checking and approving content before it is published on website (see appendix). Implement governance controls to support evidence and audit requirements, including register of content published, logging what content was checked by whom and when, and approved for publishing by whom and when.	[redacted]	Process defined 21.4 Governance controls 12.5 Final June 2018	Complete
13.	Create standard template to record approvals for publishing content on website, to form part of the auditable register of approvals.	[redacted]	28.4	Complete
14.	Implementation of IT changes required to establish staging site, generate alerts and other technical checks and controls, as part of new process.	[redacted]	Staging site 11.4 Implement software to enable "publish to live" 10.5	Complete
15.	Revise website governance document to reflect new approval process.	[redacted]	28.4	Complete
16.	Communicate process changes to approvers and staff.	[redacted]	28.4	Complete
17.	Review compliance with revised process	?	Ad-hoc	Complete
	Other governance and controls			
18.	Introduce requirement across MP Support and Corporate Services for all external emails to be checked by a second person before they are sent.	[redacted]	5.4	Complete
19.	Remove auto complete from the address field in Outlook.	[redacted]	7.4	Complete
20.	Establish information security group of SIRO plus Information Asset Owners, to strengthen governance of IPSA's information assets in line with best practice, including overseeing knowledge management actions above.	[redacted]	7.4	Complete (first meeting held on 26.4)
21.	Review scope with external suppliers for introducing further technical controls to encourage care by IPSA staff about any release of personal data in contacts with MPs and other stakeholders. [redacted] will be putting in an extra step within CRM to so that people are asked if they are sure they want to send	[redacted]	14.7	Complete

	the email with the subject “nn” to person “nn”. There will also be a delay on all emails going out of CRM of 10 minutes with the option to r stop it in that time. Work will start at the end of this week. Alternative email attachment solutions will be delivered in August.			
22.	Establish clear policy and process for password protecting any file containing personal data which needs to be sent externally.	[redacted]	31.5	Complete
23.	Plan for appointing GDPR compliant Data Protection Officer	[redacted]	30.6	Complete
24.	Ensure that any papers and other corporate data sent to Board members are sent securely via IPSA systems, with support for Board members in making the transition.	[redacted]	28.4	Complete
	Cyber Security			
25.	Subject to separate plan established following external review of compliance with ISO27001. Internal Audit penetration test of effectiveness of defences planned for August 2017.	[redacted]	31.8	Complete
	Training and awareness			
26.	All staff to complete annual online data security training, including in awareness of insider risks.	[redacted]	Invitations 28.4 Complete 12.5	Complete
27.	Run security awareness survey for all IPSA staff.	[redacted]	Invitations 28.4 Complete 12.5	Complete
28.	Invite outside speaker from TNA or other organisation to talk to IPSA staff about best practice in other organisations.	[redacted]	30.6	N/A
	Audit and assurance			
29.	Internal audit (RSM) review of adequacy of action plan	[redacted]	June 2017 tbc	Complete
30.	Cyber security: penetration testing	[redacted]	July 2017	Complete
31.	Internal audit: full review of progress since previous audit.	[redacted]	March 2018	Complete

Website publication approvals process

1. **Content owner** creates content for publication on staging website: internal policy discussions, analysis and clearances. Lead responsibility: **Content owner** within lead team.

2. **Content owner** posts files for publication in temporary holding folder (named "WEBSITE Files for upload") on Common Drive and creates content on staging site. [NEW] (In future all files in the Common Drive will be automatically deleted after 30 days, although the date of implementing this change is subject to general election timing considerations).

3. **First approver** (SMT-level manager from the lead team checks content and/or files and approves or not for publication. [NEW – previous process included approvers but they were generally not managers and not drawn from the lead team]

4. **Second approver** checks content on staging site, with particular regard to any personal data issues, and approves or not for publication. Positive sign-off required, through "Publish to website" functionality [NEW]

5. Content published on website

First approvers: [redacted] (for separate publications process).

Second approvers: [redacted]

Publications process

1. Required information is redacted automatically using the Automated Redaction Tool; then checked by a team member.
2. Redactions are peer reviewed through the refining process by a separate team member.
3. Items which have been identified as security matters, certain expenses outside the scheme or others which do not conform to publication standards are sent to Account Managers to resolve.
4. Redactions are then checked through the SMT-level publication committee.
5. Data checked by individual MPs through a report available on expense@work; MPs prompted by an email which contains no details specific to that MP.
6. An email containing highlights of the data is distributed to IPSA staff.
7. Data is reconciled against previous data and checks are made to ensure items that are not due to be published have been removed.
8. Data is loaded to staging area of website through Eduserv.
9. Further checks made to ensure the loaded data matches what was provided and no hidden data is available. Once these checks are complete the data is loaded to the main site by Eduserv.