ipsa
Independent Parliamentary Standards Authority

Subject:	**Data Breach Policy**
Owner:	**SIRO (Alastair Bridges)**
Sponsors:	**Senior Management Team**
Date:	**April 2018**
Version:	**V2.0**
Changes:	**V1.8 inclusion of Data Protection Officer, increased advice and clarity** **V2.0 insert for Security Incidents (SI), para 1 and 2, link change**

Scope of this policy

1. **Security Incidents** (SI) involve wrongful handling or disclosure of information and can give rise **Data Breaches** where personal data is involved. Although this policy concentrates on personal data breaches, the policy equally applies to SIs, including containment, investigation, improvements and lessons.

2. Personal data breaches may occur as an error (in operation, or judgement) where the result has been the wrongful disclosure, or loss of private personal data. The primary focus is on personal data, although most of the same considerations apply to other sensitive data, for example containing commercially sensitive information. **See the Appendix for Data Protection related definitions and obligations.**

3. Much of the information we deal with is sensitive and it is essential that all IPSA staff take special care to ensure it is handled correctly in compliance with our procedures and legal obligations. IPSA information is generally classified as OFFICIAL, and may be OFFICIAL SENSITIVE and where necessary protective marking should be obvious and supplied with handling instructions. IPSA will consider disciplinary action where instructions for handling personal data are not followed. Malicious intent and actions will be treated accordingly.

4. Most data breaches under consideration here are likely to be human error incidents, where personal information belonging to one or more MPs or members of MPs' staff is sent to someone else or published by mistake. However, all breaches, whether staff related or system related (automatic, poor design, malfunction or failure), including redaction, will use this policy.

5. The procedures outlined below cover:

- Action to be taken to contain the incident in the event of a data breach.
- Decision on whether the Information Commissioner's Office (ICO) should be notified, and then following reporting ICO producedures in a timely manner.
- Actions to investigate the breach, and short and longer term mitigation. In particular to accurately capture the incident and record the log entries.
- Action to be taken in respect of the individual(s) responsible for the breach.

Legal context and IPSA's code of conduct

6. IPSA, like all bodies holding personal information, has a legal duty to observe the Data Protection Principles, from the Data Protection Act 1998 (DPA), and the GDPR (see Appendix) due mid 2018. Data must be processed *fairly* and *lawfully*, and the seventh principle deals with the question of data security:

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

7. All staff must comply with the principles of data protection law, and the common law duty of confidentiality.

Actions to be taken in the event of a data breach

8. When any member of staff becomes aware that personal information has inadvertently been sent to the wrong person, he or she must inform:

- Their Line manager and the Data Protection Officer.
- In their absence, the SIRO, a Director or the senior manager present.
- Failure to notify immediately on discovery significantly increases risk and exposure for IPSA and may result in disciplinary procedings.

9. Staff should seek advice (see 8 above) before taking any remedial action.

10. The Data Protection Officer, or another individual nominated by the Senior Information Risk Owner (SIRO), will carry out an initial investigation of the data incident to establish the time line, facts and scale and inform the SIRO, and other Directors, on whether a data breach has occurred and any recommendations. This investigation should ordinarily be undertaken within 24 hours of being informed of the data incident. It should include an initial assessment of the risks to the individual(s) affected.

11. Manage the incident using the CARE approach:

- Contain – immediate actions to prevent further disclosure or damage
- Assess – to pause and plan by considering the scale of the breach
- Respond – putting the planning into action having considered the options
- Evaluate – to reflect and report on the success of the actions and consider next steps or further more assertive action.

12. The line manager of the member of staff who has committed a data breach should carry out the following actions as soon as practical and authorised:

- Consider if the Communication Manager should be informed in the event the incident may become public knowledge or available to the media, who will also consider briefing the Minister for Data Protection (Dept. DCMS).

- Contact whoever received the information by mistake and ask them either to return or delete it, depending on which is appropriate. They should also be requested to confirm that this has happened. Has it been further disclosed?

- Inform by email the people whose personal data has been sent to the wrong destination, and offer to speak to them personally. (They are referred to as "data subjects" below, as shorthand). The email should contain:

    - The line manager's name and contact details.
    - Estimated time of breach, a summary, information type disclosed
    - The measures that have been, or will be taken to retrieve the information, with a commitment (a) to inform them when this has happened, and (b) to keep them informed of any developments.

13. The Data Protection Officer should then conduct a full investigation of the data breach and report the findings to the SIRO and other Directors within a week of the initial investigation. The findings should include the following:

- A full description of the nature, cause, and timing of the data breach.
- Identification of the data subject(s) affected, and controllers/processors.
- Assessment of the risks to the individuals concerned.
- The cause(s), process failures, of the breach and the individual(s) responsible.
- Remedial action already taken, future actions to be taken, and timescales.
- A recommendation as to whether the ICO needs to be informed.

14. Common Questions to address, and which will likely be asked by the ICO:

- Was the individual sufficiently trained, and had they completed the Civil Service Learning cource on Information Management?

- Was prescribed procedure followed? Is that process functional?
- What checks took place to support success of the process?

15. HR should be kept informed of all developments, so that they can advise the lead investigator and provide support to staff involved in the incident.

16. If the recipient who received the information by mistake has not responded within 48 hours, they should be contacted again. Check by email and phone, and log attempts. This cycle should be repeated until a resolution is reached.

Severity of the data breach

17. While all data breaches are a matter of concern, some will have a more severe impact on the data subject. The ICO employs the terms *damage* and *distress*.

18. Potential damage to the data subject takes three main forms:

- *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, itinerary or other information which is relevant to a person's security (for example detailed travel arrangements for Northern Ireland MPs) is misplaced. This includes home security arrangements.

- *Reputational*, if information which could be misused by the media, political opponents, or other individuals, goes astray.

19. The ICO defines substantial distress as being "a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation, strong dislike, or a feeling that the [data] processing is morally abhorrent". Clearly, any of the categories of damage above could cause considerable distress. But there are other losses of data that could cause distress or detriment (disadvantage).

20. As a guideline, we can regard there as being three levels of severity. These definitions are **internal only** – they do not come from official sources - although they are informed by the ICO's guidance on damage and distress.

- LOW RISK - IRRITATION/ INCONVENIENCE. This is where some inconvenience or irritation may be caused to the data subject, but there is no significant damage or distress caused. For example, this could be when an email about arrangements for a meeting are sent to the wrong person.

- MEDIUM RISK - DISTRESS THAT DOES NOT POTENTIALLY CAUSE SERIOUS DAMAGE. An example here could be the sending of salary details to the wrong person. This may cause significant distress to the member of staff, but unless it is accompanied by payment details (bank account details for example), it will not cause material damage to the data subject.

- HIGH RISK - SERIOUS DAMAGE. Any misplacing of information that causes financial or security risk to the data subject, or significant reputational risk - confidential correspondence about MPs' pay might be an example – should be regarded as potentially causing serious damage to the data subject.

Deciding whether the ICO should be notified

21. A recommendation on whether the ICO should be notified will be made by the Data Protection Officer to the SIRO. They will consult the Chief Executive and other Directors before notifying the ICO. This recommendation will be based on the sensitivity, scale, risks of the breach.

22. If the initial investigation of the data breach indicates a significant and serious breach, then the Data Protection Officer, Head of IT and SIRO may recommend that the ICO is informed immediately of the breach and any immediate measures to be taken. This will then be followed up with details of the full measures to be taken to address the breach and prevent the same thing happening again after the detailed investigation has taken place. In any event, notification to the ICO must be within 72 hours of discovery.

23. Except in these urgent circumstances, a decision will be deferred until after the full investigation has been completed, subject to the above.

24. Where there is potentially distress but not damage, a judgement will need to be made about the likely significance of the distress. If there is doubt, then the default position should be to notify the ICO, but to make clear what is considered to be the severity.

25. If there is likely to be inconvenience or irritation, but not damage or significant distress, then there may be no need to inform the ICO, although a record should still be kept. Consider non-reporting decisions with considerable care, as investigation and fines to IPSA, as well as having the confidence of MPs rests on good judgement and timely co-operation.

HR action to be taken with the individual responsible for the breach

26. The IPSA Disciplinary Policy refers to breaches and serious breaches of confidentiality, security and negligence which leads to loss of data (including failure to apply procedures) being disciplinary matters, potentially amounting to gross misconduct. If there are signs of intention, this may give rise to criminal charges under the Data Protection Act and Computer Misuse Act.

27. Any loss of personal data - which includes information which would not normally be published being sent to the wrong person - is considered a very serious matter, and may result in a review of conduct and guidance.

28. HR **must** be involved throughout to guide the disciplinary process, although the line manager is responsible for chairing disciplinary meetings and making decisions about sanctions to be imposed. HR will advise if the Police should be involved if there are indications that there was intention to breach or disclose information unlawfully. HR will also lay out the rights of the individual.

29. This disciplinary process should be followed for data breaches, but the severity and impact of the breach should also be taken account, and the actions below applied where necessary.

- If serious damage could be caused to the data subject, then the outcome of the resultant disciplinary process should be a written warning for the individual concerned.

- If distress could be caused to the data subject (within the medium risk category in paragraph 19 above), then a verbal or written warning should be issued, with the decision as to which of these is appropriate taking account of the impact of the data loss and any mitigating circumstances.

- If the breach is only likely to cause some inconvenience or irritation then the line manager should discuss the matter with the responsible individual, and agree how to avoid it happening again; but there will be no need, first time around, for a verbal warning.

30. If a verbal warning or more is required, then the line manager and the responsible individual should agree measures to ensure that a recurrence is avoided. This should constitute a personal performance objective for the individual. Their training should be evaluated and corrected as required.

Keeping a central record of data breaches and disciplinary measures

31. It is the responsibility of the Data Protection Officer to lead the investigation and report on data breaches. He or she will also be the main point of contact for the ICO, and will maintain a central record of all data breaches. Records of any disciplinary measures will be held by HR.

Appendix – Data protection, ICO, and GDPR guidance

Introduction: http://ec.europa.eu/justice/data-protection/reform/index_en.htm
Full: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

General Data Protection Regulation (GDPR) Articles and recitals

http://www.privacy-regulation.eu/en/4.htm - Definitions:

'*personal data*' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'*controller*' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'*processor*' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'*recipient*' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by [them] shall be in compliance with the […] data protection rules according to the purposes of the processing;

'*personal data breach*' **means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed**;

http://www.privacy-regulation.eu/en/33.htm - "Notification of a personal data breach to the supervisory authority (ICO)"

http://www.privacy-regulation.eu/en/r85.htm - risk of harm and notification

http://www.privacy-regulation.eu/en/r87.htm - establish confirmation of breach and fact of notification to the supervisory authority (ICO) without “undue delay”

http://www.privacy-regulation.eu/en/34.htm - "Communication of a personal data breach to the data subject"

http://www.privacy-regulation.eu/en/r86.htm - notify subjects, but also consideration of balance given of further harm to subject versus risk of further breaches in the circumstances

ICO Guidance:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf