UK Society for Behaviour Analysis

UK-SBA
DATA BREACH
POLICY

Committee responsible:	Membership	**Date approved:**	April 2024
Approved by:	UK-SBA Board	**Date of last review:**	March 2024
Version Number:	1.4	**Date of next review:**	March 2026

TABLE OF CONTENTS

1. Purpose 3
2. Definitions / Types of breach 3
3. Scope 4
4. Reporting an incident 4
5. Containment and recovery 4
6. Notification 5
7. Evaluation and response 6
8. Policy Review 6
9. Contact 6

APPENDIX 1 – Data Breach Report Form 7

1. Purpose

1.1 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across UK-SBA.

1.2 This policy relates to all personal and special categories (sensitive) data held by UK-SBA regardless of format.

1.3 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.4 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, a detrimental effect on service provision, legislative non- compliance, and/or financial costs.

2. Definitions / Types of breach

2.1 'UK-SBA' is an acronym for UK Society for Behaviour Analysis

2.2 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

2.3 An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to UK-SBA's information assets and / or reputation.

2.4 An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record)
- equipment theft or failure
- system failure
- unauthorised use of, access to or modification of data or information systems
- attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- unauthorised disclosure of sensitive / confidential data
- website defacement
- hacking attack
- unforeseen circumstances such as a fire or flood
- human error
- The interception of unprotected workbooks / sheets/ PowerPoint presentations and PDF's
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

2.5 DPO is an acronym for Date Protection Officer

2.6 **ICO** - Information Commissioner's Office, the UK's independent regulator for data protection and information.

2.7 **LIO** is an acronym for Lead Investigating Officer

2.8 **Data Subject** - Person to whom the personal data relates.

3. Scope

3.1 This policy applies to all staff, Directors and members of UK-SBA. This includes temporary, casual or agency staff and contractors, consultants, suppliers, and data processors working for, or on behalf of UK-SBA.

3.2 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4. Reporting an incident

4.1 Any individual who accesses, uses, or manages UK-SBA's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO).

4.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3 The report must include full and accurate details of the incident, including the date and time the breach was discovered; when the breach occurred (dates and times); who is reporting it; a description of the breach; what personal data was involved; how many individuals are involved; what the consequences of the breach were and what action was taken to mitigate it. A Data Breach Report Form should be completed as part of the reporting process (refer to Appendix 1).

4.4 Once Part 1 of the Data Breach Report has been received by the DPO, a Lead Investigative Officer (LIO) will be assigned to liaise with Head of the area affected by the breach, and the Investigative Officer will complete Part 2 of the Data Breach Report Form.

4.5 The DPO will complete Part 3 of the Data Breach Report and advise the relevant stakeholders and authorities as necessary.

4.6 All staff have a responsibility to report any actual or suspected data breach. Staff should be aware that knowingly not reporting a breach may result in UK-SBA's Disciplinary Procedures being instigated. Similarly, any breach of data protection may also result in UK-SBA's Disciplinary Procedures being instigated.

5. Containment and recovery

5.1 The DPO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach and will nominate an appropriate person to take the lead in investigating the breach, as the LIO. The DPO will also ensure the LIO has the necessary resources to investigate the breach.

5.3 The LIO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

5.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

5.5 Advice from experts across UK-SBA may be sought in resolving the incident promptly.

5.6 The LIO, in liaison with the relevant staff will determine the suitable course of action to be taken to ensure a resolution to the incident.

5.7 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

5.8 The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what impact the data loss could have (e.g. what has happened to the data; whether the data could be put to any illegal or inappropriate use)
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

6. Notification

6.1 The LIO and DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, the DPO will notify them within 72 hours of becoming aware of the breach.

6.2 Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation[2];
- whether notification would assist the individual(s) affected (e.g., could they act on the information to mitigate risks?)
- whether notification would help prevent the unauthorised or unlawful use of personal data
- whether there are any legal / contractual notification requirements
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work

6.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed by the LIO or DPO without undue delay. Notification will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks.

Individuals will also be provided with a way in which they can contact UK-SBA for further information or to ask questions on what has occurred.

6.4 The LIO and / or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

6.5 The LIO and or the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

6.6 A record will be kept of any personal data breach, regardless of whether notification was required.

7. Evaluation and response

7.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

7.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

7.3 The review will consider:

- where and how personal data is held and where and how it is stored
- where the biggest risks lie including identifying potential weak points within existing security measures
- whether methods of transmission are secure; sharing minimum amount of data necessary

7.4 The DPO will, with support of relevant staff, agree and implement preventative measures (e.g. changes to systems, policies and procedures, and/or measures to increase staff awareness)

7.5 The DPO will be responsible for ensuring that remedial measures taken are effective.

8. Policy Review

8.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the person responsible for data protection alongside senior managers within UK-SBA.

8.2 This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

8.3 This policy was last reviewed in March 2024.

9. Contact

9.1 Any enquiries in relation to this policy should be directed to UK-SBA Administrator admin@uk-sba.org

APPENDIX 1 – Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please complete Section 1 of this form and email it to the Data Protection:

Section 1: Notification of Data Security Breach	**To be completed by person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen, how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for UK-SBA or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation • Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; • Personal information relating to vulnerable adults and children; • Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; • Spreadsheets of pupil's and client's data, information about individual cases of pupil's and client's discipline or sensitive negotiations which could adversely affect individuals. • Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	To be completed by Data Protection Officer and/or Lead Investigation Officer
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**