Fincomp Services Limited
Data Breach Policy

Introduction

Fincomp Services Limited ("us" or "we") take our responsibilities with regard to the management of the requirements of the Data Protection Act 1998 very seriously. This document provides the policy framework for an effective response in respect of any confirmed or suspected data breach.

1. Purpose

The purpose of this policy is to standardise our response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated;
- incidents are dealt with in a timely manner and normal operations restored;
- incidents are recorded and documented;
- the impact of the incident is understood, and action is taken to prevent further damage;
- the Information Commissioner's Office (ICO) and data subjects are informed as required in more serious cases;
- incidents are reviewed, and lessons learned.

2. Scope

This policy applies to all information, regardless of format, and is applicable to all Information Users.

3. Policy

3.1 Information User Responsibilities

All Information Users are responsible for reporting actual, suspected, threatened or potential data breaches and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

In any situation where an Information User is uncertain whether an incident constitutes a data breach, they must report it to the Chief Information Officer (CIO) for evaluation.

If there are IT issues, such as the security of the network being compromised, the CIO should be informed immediately so that remedial action can be taken, and any potential data breach identified.

3.2 CIO Responsibilities
The CIO will be responsible for overseeing management of all data breaches in accordance with the Data Breach Management Plan, outlined in section 3.4. Suitable further delegation may be appropriate in some circumstances.

The CIO must maintain documentation on data breaches, their nature and remedial action taken to ensure appropriate oversight in the types and frequency of confirmed breaches for management and reporting purposes.

3.3 Reporting a Breach
Confirmed or suspected data breaches should be reported promptly to the CIO at 020 8099 7301, email: cio@fincomp.co.uk. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

The Incident Report Form (see **Appendix 1**) should be completed as part of the reporting process. Once a data breach has been reported an initial assessment (see **Appendix 2**) will be made to evaluate the incident severity of the breach.

After evaluation, we must notify the ICO if the breach is likely to result in a risk to the freedoms and rights of natural persons. Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made without undue delay and within 72 hours of us becoming aware of it. If we fail to do this, we must explain the reason for the delay.

A report to the ICO must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of the CIO, likely consequences of the breach and action taken.

3.4 Data Breach Management Plan
Our response to any reported data breach will involve the following four elements:

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the data breach checklist (see **Appendix 3**). An activity log (see **Appendix 4**) recording the timeline of the incident management should also be completed.

Note: This reflects current guidance from the ICO, which is likely to change.

4. Related policies, standards and guidelines

ICO guidance on data breaches can be read here.

5. Terms and definitions

An Information User is anyone (including staff, visitors and third-party data processors) who process data on our behalf.

A data breach is a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

A data breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy;
- Data posted, emailed or faxed to the incorrect recipient;
- Loss or theft of equipment on which data is stored;
- Inappropriate sharing or dissemination;
- Staff accessing information to which they are not entitled;
- Hacking, malware, data corruption;
- Information is obtained by deception or “blagging”;
- Equipment failure, fire or flood;
- Unescorted visitors accessing data;
- Non-secure disposal of data.

6. Enforcement

Any Information User found to have violated this policy may be subject to disciplinary action or other appropriate sanctions.

Appendix 1: Data Breach Reporting Template

Part A: To be completed by the person reporting the incident	
Date incident was discovered:	
Date(s) of incident:	
Name of person reporting incident:	
Contact details of person reporting incident:	Email: Phone: Address:
Brief description of incident or details of the information lost:	
Classification of data breached (refer to section 4.3.2 of the **Information Security Policy**)	☐ Public ☐ Internal ☐ Confidential ☐ Highly Confidential
No. of Data Subject 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:	
Part B: To be completed by the Chief Information Officer	
Received by:	
On (date):	

Appendix 2: Evaluation of Incident Severity

The severity of the incident evaluated based upon the following criteria:

High Criticality: Major Incident

• Highly Confidential/Confidential Data
• Breach involves Personal Data more than 1000 individuals
• External third-party data involved
• Significant or irreversible consequences
• Incident may not yet be contained
• Immediate response required regardless of whether it is contained or not
• Requires significant response beyond normal operating procedures
• External parties must be notified:
  ○ Information Commissioner's Office (ICO)
  ○ Individuals Impacted

Moderate Criticality: Serious Incident
• Confidential Data • Breach involves Personal Data of more than 100 individuals • Not contained within Fincomp • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does not require immediate response
Low Criticality: Minor Incident
• Internal or Confidential Data • Breach involves Personal Data of a small number of individuals • Risk to Fincomp low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident does not require immediate response <u>Examples:</u> • Email sent to wrong recipient • Loss of encrypted mobile device

Appendix 3: Data Breach Checklists

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Evaluate the severity of the breach and determine if any Personal Data is involved.	See **Appendix 2**
2	Identify the cause of the breach and whether the breach has been contained?	Establish what steps can or need to be taken to contain the breach from further data loss.
3	Ensure that any possibility of further data loss is removed or mitigated as far as possible.	This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
5	Where appropriate, inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
6	Ensure all key actions and decisions are logged and recorded on the timeline.	
B	**Assessment of Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
7	What type and volume of data is involved?	Data Classification/volume of individual data etc
8	How sensitive is the data?	Sensitive Personal Data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).
9	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
10	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.

11	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-ups
12	How many individuals' Personal Data are affected by breach?	
13	Who are the individuals whose data has been compromised?	Staff, clients or suppliers?
14	What could the data tell a third-party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
15	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?
16	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
17	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.
C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
18	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
19	Can notification help Fincomp meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.

20	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
21	If a large number of people are affected, or there are very serious consequences, inform the ICO.	Contact and liaise with the Director of Legal Services or the Governance and Information Compliance Team.
22	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".
23	Consider whom to notify, what you will tell them and how you will communicate the message.	• There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. • Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. • When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. • Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
24	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of Personal Data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of Personal Data. Guidance available from here.
25	Consider, as necessary, the need to notify any third-parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.
D	**Evaluation and Response**	**To evaluate the effectiveness of the University's response to the breach.**
26	Establish where any present or future risks lie.	

27	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
28	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
29	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.

Appendix 4: Timeline of Incident Management

Date	Time	Activity	Decision	Authority