Reviewed 5th January 2020
By Holly Roberts

Data Breach Policy 2020

Introduction
Owl Live utilises various information systems and holds of data / information which may include personal or confidential information (for its own use and that of clients) and also non-personal information which could be sensitive or commercial, for instance financial data. Care should be taken to protect these information assets from incidents (either accidentally or deliberately) that could compromise their security. In the event of a data breach or an information security incident, it is vital that appropriate actions are taken to minimise associated risks.

Purpose
The purpose of this policy is to set out the procedure that should be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

Responsibilities
All users of information assets are required to familiarise themselves and comply with this policy. All individuals who access, use or manage the information are responsible for reporting data breach and information security incidents immediately to the data controllers (Antony Greenberg and Holly Roberts).

Compliance
Owl Live has an obligation to comply with relevant statutory, legal and contractual requirements. The Data Breach and Information Security Incident Policy is part of the Information Security suite of policies, designed to ensure data breach and information security incidents are reported promptly and managed properly to mitigate any risks to the confidentiality, integrity and availability of information and information systems. Failure to adhere to this policy will be addressed by necessary disciplinary actions in accordance with the Owl Live Disciplinary Procedures, and relevant contractor and third party contractual clauses relating to non-conformance with the Information Security Policy and related policies.

Definition of an incident
An incident in the context of this policy is an event which has caused or has the potential to cause damage to information assets or reputation. Examples are;

- Accidental loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick).
- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- Unauthorised disclosure of sensitive or confidential information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee)
- Compromised user account (e.g. accidental disclosure of user login details through phishing)
- Failed or successful attempts to gain unauthorised access to information or information systems
- Equipment failure
- Malware infection
- Disruption to or denial of IT services

Reporting an incident
Data breach and information security incidents should be reported immediately to the data controllers (Antony Greenberg or Holly Roberts), as the primary point of contact. The report should include full and accurate details of the incident, including who is reporting the incident, what type of incident it is, if the data relates to people, and how many people are involved. Owl Live will keep logged and store all information

Investigation and Risk Assessment
Depending on the type of incident, the data controllers will instigate the relevant incident management team or inform the relevant individual to investigate the incident. An investigation will be started within 24 hours of the incident being discovered, where possible. The investigation will establish the nature of the incident, the type of data involved, and where personal data is involved, who the subjects are and how many personal records were breached. The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be performed as to what might be the consequences of the incident, for instance whether harm could come to individuals or whether data access or IT services could become disrupted or unavailable.

Containment and Recovery
The incident management team or relevant individuals will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment. Appropriate steps will be taken to recover system or data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords. Advice from experts may be sought in resolving the incident promptly and appropriately.

Notification
The data controllers will make a decision to inform any external organisation, such as the police or other appropriate regulatory body.
If the breach involves a client's data, they will be immediately informed and consulted to ensure the client's policies are also adhered to. If a breach involving personal data has occurred, the Information Commissioner's Office may be informed based on the extent of the breach. Individuals whose personal data have been affected by the incident will be notified to enable them take steps to protect themselves, and where users of information assets have been affected, users will be notified. The notice will include a description of the breach and the steps taken to mitigate the risks.

Review
Once the incident is contained, a thorough review of the event will be undertaken by the relevant team or individual and reported to the data controllers. The report will detail the root cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement. Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.