# DATA BREACH RESPONSE PLAN

## 1. Introduction & Purpose

This plan outlines the procedures to be followed in the event of a data breach at Move More Move Well. Its purpose is to ensure a swift, effective, and compliant response to minimise harm to individuals and the studio, and to meet our obligations under the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018.

### What is a Data Breach?

A data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This could include:

- Loss or theft of client lists (digital or physical)
- Unauthorised access to client booking systems
- Accidental emailing of client details to the wrong person
- Cyber-attack (e.g., ransomware)
- Lost or stolen devices (laptops, phones, USB drives) containing client data

## 2. Roles and Responsibilities

At Move More Move Well, Dawn Fazackerley-King is the Studio owner and Data Protection Lead. This person is ultimately responsible for overseeing the entire response, reporting to the ICO if necessary, and communicating with affected individuals. Andrew King provides Technical Support.

## 3. Breach Detection & Assessment

How to detect a breach:

- Alerts from software/security systems
- Reports from staff or clients (e.g., "I received an email not meant for me")
- Suspicious activity on systems (e.g., unusual logins, file access)
- Physical loss of documents or devices

**Initial Steps:**

1. Confirm the Breach: As soon as a potential breach is suspected, the DPL must be informed immediately.
2. Gather Information:
    - What happened? (e.g., lost laptop, email sent to wrong person, system hacked)
    - When did it happen? (Date and time discovered, estimated time of breach)
    - Where did it happen?
    - What type of data is involved? (e.g., names, contact details, health information, payment details)
    - How many individuals are affected? (Estimate initially)
    - What is the potential impact on individuals? (e.g., financial loss, reputational damage, discrimination)
    - Who discovered it?

**4. Containment & Remediation**

The goal is to stop the breach and prevent further damage.

1. Isolate the Source:
    - Take affected systems offline.
    - Change passwords for compromised accounts.
    - Revoke access for compromised users.
    - Disable external connections if suspicious activity is detected.
    - If a physical device is lost/stolen, remotely wipe it if possible.
2. Mitigate Harm:
    - Retrieve lost data/devices if possible.
    - Delete incorrectly sent emails.
    - Fix vulnerabilities that led to the breach (e.g., patch software, improve security settings).
    - Implement stronger security measures (e.g., multi-factor authentication).
3. Preserve Evidence: Do not delete logs or other information that could be useful for investigation.

**5. Risk Assessment & Notification Decision**

This is crucial for GDPR compliance.

- Assess the Risk to Individuals: The DPL, in consultation with technical support, will assess the likelihood and severity of harm to the affected individuals. Consider:

    - Type of data: Sensitive data (health, financial) carries higher risk.
    - Volume of data: More data means higher risk.
    - Vulnerability of individuals: Children or those with specific health conditions might be more vulnerable.
    - Circumstances of the breach: Was the data encrypted? Was it publicly exposed?
    - Mitigation measures taken: Have steps been taken to reduce the risk?

- Decision Points:

    - ICO Notification: Is the breach likely to result in a risk to the rights and freedoms of individuals? If YES, the ICO *must* be notified within 72 hours of becoming aware of the breach.
        - Use the ICO's online breach reporting form: https://ico.org.uk/for-organisations/report-a-breach/
    - Individual Notification: Is the breach likely to result in a high risk to the rights and freedoms of individuals? If YES, affected individuals *must* be notified without undue delay.

**6. Notification Process**

A. Notification to the Information Commissioner's Office (ICO)

- When: Within 72 hours of becoming aware of the breach, *if* it meets the risk threshold.
- Who: The DPL is responsible for this.
- What to include (as much as known within 72 hours):
    - The nature of the personal data breach including categories and approximate number of data subjects and personal data records concerned.[2]
    - The name and contact details of the[3] DPL or other contact point.
    - Description of the likely consequences of the personal data breach.
    - Description of the measures taken or proposed to be taken[4] to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[5]
- Remember: You can update the ICO with more information as your investigation progresses.

**B. Notification to Affected Individuals**

- When: Without undue delay, *if* it meets the 'high risk' threshold.
- Who: The Communications Lead/DPL.

- How: Via the most appropriate and secure method (e.g., email, letter, phone call if highly sensitive). Avoid public statements before individuals are directly informed, unless absolutely necessary.
- What to include:
    - Clearly and concisely describe the breach.
    - Explain the nature of the data involved.
    - Explain the likely consequences.
    - Advise them on steps they can take to protect themselves (e.g., change passwords, monitor bank statements, be wary of phishing).
    - Provide contact details for further information (e.g., DPL email/phone).
    - Explain measures the studio has taken or proposes to take.
    - Assure them of the studio's commitment to data security.

**7. Post-Breach Review & Improvement**

Once the immediate crisis is over, learn from the incident.

1. Full Investigation: Conduct a thorough review to understand:
    - Root cause of the breach.
    - Effectiveness of the response plan.
    - Any weaknesses in security measures.
2. Documentation: Maintain a detailed record of the breach, including:
    - When it occurred and was discovered.
    - What happened.
    - Who was affected.
    - Steps taken to contain and mitigate.
    - Notifications made (ICO, individuals).
    - Lessons learned.
3. Implement Improvements:
    - Update security policies and procedures.
    - Provide additional staff training on data protection and security.
    - Invest in new security technologies if necessary.
    - Review and update this Data Breach Response Plan regularly.

**8. Key Contact Information**

- Data Protection Lead: Dawn Fazackerley-King 07899 716920 email: movemoremovewell@hotmail.com
- Technical Support: Andrew King 07966 377110
- ICO Contact: 0303 123 1113 (ICO Helpline) - https://ico.org.uk/

Date: June 9, 2025
Prepared by: Dawn Fazackerley-King, Studio Owner and Data Protection Lead