Data Breach Recovery Action Plan

The Lambourn Junction Community Interest Company
The Blue House
Station Road
Lambourn
RG17 8PH

Initial Response:

1. Designate a Response Team:
   - Identify key individuals from the volunteer pool to form a Data Breach Response Team, including a team leader, IT specialist (if available), and a communications representative.

2. Assessment of Breach:
   - Investigate and assess the nature and scope of the data breach.
   - Identify the types of data compromised and potential impact on individuals.

3. Containment:
   - Isolate affected systems or areas to prevent further unauthorized access.
   - Change passwords and credentials for compromised accounts.

Notification:

4. Legal Obligations:
   - Consult relevant data protection laws and regulations to determine the necessity and timeline for reporting the breach to regulatory authorities.

5. Communication Plan:
   - Develop a communication strategy for notifying affected individuals, volunteers, and stakeholders.
   - Clearly articulate the steps being taken to address the breach and prevent future incidents.

Recovery:

6. System Remediation:
   - Work with IT volunteers to implement security patches, updates, and necessary improvements to prevent a recurrence.
   - Conduct a thorough security audit to identify and address vulnerabilities.

7. Data Restoration:
   - Restore affected data from secure backups.
   - Verify the integrity of restored data and ensure its accuracy.

Evaluation:

8. Post-Incident Review:
   - Conduct a comprehensive review of the incident, including the response process and effectiveness.
   - Identify lessons learned and areas for improvement in policies and procedures.

9. Training and Awareness:
   - Provide additional training to volunteers on data protection practices and security awareness.
   - Reinforce the importance of reporting any suspicious activities promptly.

Prevention:

10. Policy and Procedure Enhancement:
    - Review and update data protection policies and procedures.
    - Implement additional safeguards to prevent similar breaches in the future.

11. Regular Audits:
    - Schedule regular security audits and vulnerability assessments.
    - Monitor systems for any unusual or suspicious activities.

Communication:

12. Public Relations:
    - Work with the communications representative to rebuild trust with the community.
    - Share information on enhanced security measures being implemented.

13. External Communication:
    - Keep regulatory authorities, if applicable, updated on the progress of recovery efforts.
    - Maintain transparency in external communications while ensuring compliance with legal requirements.

Document Control

- Owner: Data Protection Officer
- Procedure approved on: 8 December 2023
- Next review date: 7 December 2024

Change Control

- 2023-12 - Procedure Published