Royal Highland Yacht Club

Data Breach Policy

Data Breach Policy

1. About this Policy

1.1 The Royal Highland Yacht Club takes the security of its members' personal data seriously. We are committed to keeping members' personal data safe and will comply with the General Data Protection Regulations (GDPR) 2018 when dealing with members' personal data.

1.2 We take every care to protect members' personal data from incidents (either accidentally or deliberately).

1.3 Any compromise of personal information could result in harm to individual(s) and/or reputational damage, potentially resulting in detrimental effect on Club operation, legislative non-compliance and/or financial cost.

2. Purpose & Scope

2.1 The Royal Highland Yacht Club has in place policies and procedures designed to protect the security of members' personal data.

2.2 This policy includes the procedure to be followed to ensure a consistent and effective approach in managing data breach and information security incidents. This policy relates to all personal data held by the Club, irrespective of format, and applies to all Club members of all categories.

2.3 The purpose of this policy is to define how the Club will contain any breaches, minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3. Definitions & Types of Breach

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

3.2 For the purpose of this policy, an incident is an event or action which may compromise the confidentiality, integrity or availability of data (or systems on which it is held), either accidentally or deliberately, and has caused or has the potential to cause damage to the Club's information assets and / or reputation.

3.3 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, 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 the Club's computer system(s)
- unauthorised disclosure of sensitive / confidential data

- website defacement
- hacking attack
- unforeseen circumstances such as a fire or flood
- human error.

4. Reporting an Incident

4.1 Any individual who accesses, uses or manages the Club's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (vice-commodore@rhyc.org.uk) and/or the Club Secretary (secretary@rhyc.org.uk).

4.2 Any incident must be reported as soon as practicable.

4.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved (if known). A Data Breach Reporting Form should be completed as part of the reporting process (see Appendix A).

5. Containment & Recovery

5.1 The Club's Data Protection Officer (DPO) will firstly determine if the breach is still occurring, and what steps need to be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the DPO to establish the severity of the breach and whether there is anything that can be done to recover any losses and limit the damage the breach could cause. The DPO will establish who may need to be notified as part of the initial containment and will inform Police Scotland, where appropriate.

5.3 The DPO will determine the suitable course of action to be taken to ensure a resolution to the incident. Any recommended action will be recorded on the reporting form.

6. Investigation & Risk Assessment

6.1 The DPO will immediately undertake an investigation and, wherever possible, within 24 hours of the breach being discovered / reported.

6.2 The DPO 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.

6.3 The investigation will need to consider the following:

- the type of data involved
- its sensitivity
- the protections are in place
- 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.

Royal Highland Yacht Club

Data Breach Policy

7. Notification

7.1 The DPO, in consultation with other flag officers, will establish whether the Information Commissioner's Office (ICO) will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

7.2 Every incident will be assessed on a case by case basis; however, the following will be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation
- 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.

7.3 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 Club's DPO without undue delay. The DPO will consider notifying third parties such as Police Scotland, the Club's insurers and/or banks where illegal activity is known or is believed to have occurred, and/or where there is a risk that illegal activity might occur in the future.

7.4 The Club will keep a record of any personal data breach, regardless of whether notification was required.

8. Evaluation & Response

8.1 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 the Club's policies and procedures should be undertaken. 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.

8.2 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
- implementing changes to the Club's data breach policy and reporting requirements.

8.3 If deemed necessary, a report recommending any changes to systems, policies and procedures will be laid before the Club's management committee for consideration.

9. Policy Review

9.1 The above policy and procedures will be reviewed from time to time.

Royal Highland Yacht Club

Data Breach Policy

Royal Highland Yacht Club

Data Breach Policy

APPENDIX 1

Royal Highland Yacht Club

Data Breach Policy

Royal Highland Yacht Club

Data Breach Policy

DATA BREACH REPORTING FORM

If you discover a personal data security breach, please notify the Club's Data Protection Officer (DPO) and/or Club Secretary as soon as practicable.

Notification	Date(s) of breach:	
	Date incident was discovered:	
	Name of person reporting the incident:	
	Contact details of person reporting the incident:	
Details of Breach	Brief description of security breach: *(Do not include any detailed personal data here)*	
	How did the incident occur?	
	Number of data subjects affected (if known):	
	Are the affected individuals aware that the incident has occurred?	
Containment	Brief description of any action since breach was discovered:	
	Brief description of any action to prevent a recurrence of the incident:	

For Club Data Protection Officer Use Only:	
Report received by:	
Date:	
Action:	
Date:	