Reigate Squash Club

Data breach response plan

Background

Reigate Squash Club ("the Club") is committed to protecting members' personal data. This document sets out how the Club will deal with any potential data breaches.

What is a data breach?

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by the Club or those organisations who process personal data on behalf of the Club;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

What to do when a personal data breach may have occurred

When a security incident takes place, either the Chairman or Honorary Secretary must be informed promptly. If, for some reason, this is not possible then a Management Committee member must instead be informed, who must make a written note of the conversation and its date and submit it to the Chairman or Honorary Secretary.

The Chairman or Honorary Secretary will quickly establish whether, in their view, a personal data breach has occurred.

Actions where a personal data breach has occurred

If it is deemed that a personal data breach has occurred, then the Chairman or Honorary Secretary will establish a group to take the matter forwards (the "Investigating Committee") which will be formed of two or more members of the Management Committee (which may include the Chairman or Honorary Secretary themselves).

When a personal data breach has occurred, the Investigating Committee will establish the likelihood and severity of the resulting risk to members' rights and freedoms.

If it is unlikely that there is a risk to members' rights and freedoms, then the Club will not be required to report the personal data breach. However, the decisions and the justifications for it will be documented and retained by the Honorary Secretary.

If it is likely that there is a risk to members' rights and freedoms, then the Club will notify the Information Commissioner's Office ("ICO"). The ICO should be notified of a personal data breach within 72 hours of becoming aware of it, even if the Investigating Committee has not yet obtained all of the details. Further information will be submitted by the Investigating Committee as soon as possible. If the Investigating Committee knows that it will not be able to provide full details within 72 hours, it will look to explain the delay to the ICO and confirm when it expects to submit more information.

The following information will be given to the ICO about a personal data breach:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of a member of the Investigating Committee from whom more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach.

Informing the affected individuals

The Investigating Committee will inform, without undue delay, the affected individuals about the personal data breach when it is likely to result in a high risk to their rights and freedoms. Advice will also be provided to help the affected individuals protect themselves from the effects of the personal data breach.

The nature of the personal data breach will be described in clear and plain language including (at least) the following:

- the name and contact details of a member of the Investigating Committee from whom more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Documentation

The Investigating Committee will document all actions taken in relation to the personal data breach, even if it does not need to be reported. Such documentation will be retained by the Honorary Secretary.

Reigate Squash Club, December 2019