

Regents Canoe Club Risk Assessment – Club Security (Site, Financial and Data Security)

Assessment to follow the 5 step process as recommended by the HSE and set out below. Further information can be found online: <http://www.hse.gov.uk/risk/controlling-risks.htm>

- 1) Identify any hazards
- 2) Decide who might be harmed and how
- 3) Evaluate the risk and decide on precautions
- 4) Record your findings
- 5) Review and update as necessary

Assessment undertaken: June 2019

Signed: Kate Balderson

Post: Chair

Next review due: June 2020

Significant Hazards	People at risk from identified hazards	Precautions taken to minimise the risk
Site security: Theft of club equipment or cash	Risk to club as a whole	<p>No cash to be held on site at Graham Street</p> <p>Cash transactions to be as limited as possible. Wherever possible transactions to be made by card payment. Cash should only be accepted for guest members on Mondays (on Thursdays Equipment Officer is present and can take payment) or for social events.</p> <p>All cupboards, boxes and boat cage to be locked at the end of every session, as well as changing rooms, project room and barge</p> <p>Members who have hired equipment to be made aware that they may be held responsible for replacement costs if equipment is stolen through carelessness while in their possession. All members to be asked to use a boat lock while boats are stored on cars. Boat locks to be made available for members to borrow for free on request.</p>
Site security: Misuse / loss of club keys	Keyholders	<p>Incoming committee to agree designated members who will be keyholders for the year</p> <p>Keys should not routinely be given to members who are not dedicated keyholders. This may be necessary on exceptional occasions (e.g. all keyholders on the Alps trip) and if necessary clear arrangements for key handover and return should be made</p> <p>No additional keys to be cut without agreement from full RCC Committee and IBC</p>
Financial security: Online fraud – phishing, hacking etc	Committee members, especially treasurer	<p>Payment Approval Process to be followed before any online payment from the club accounts is made. This is documented elsewhere but involves</p> <ul style="list-style-type: none"> - Receipt of a formal invoice - Verification that the invoice is genuine and that payment details are correct (either with company who has issued it or with member who is arranging for the payment). Verification to be

		<p>made by a means other than email</p> <ul style="list-style-type: none"> - Additional confirmation that payment can be made by one of two other designated committee members (usually Chair and Secretary). Confirmation to be made by a means other than email <p>Only the Treasurer to make payments from club account</p>
<p>Data security: Loss of members personal data</p>	<p>All users</p>	<p>Committee to maintain a ROPA to record what data is held on members, why it is required, where it is stored, how long it will be retained and how it can be deleted if a member requests this</p> <p>All sensitive personal data to be held on a password protected database (currently Webcollect). Access to this database to be limited to the Membership secretary, Secretary and Chair only.</p> <p>All members to be required to confirm that they have read the Privacy Notice. New members to be given the opportunity to read this before joining. Existing members to confirm that they have read it when they renew their membership each year.</p> <p>Privacy notice to be reviewed by the Committee each year and updated as necessary.</p>