UKRA Data Retention Policy

Background

In order to provide an efficient and accurate service to members, the United Kingdom Rocketry Association (UKRA) maintains an increasing proportion of its information about members in electronic formats. In keeping with the principles of the Data Protection Act 1998, UKRA is required to have a policy on how this information is maintained and used.

New UKRA members and those renewing membership with UKRA need to be aware of UKRA's data retention policy when joining UKRA/ renewing UKRA membership. Details of the policy will be made available through UKRA publications and posted on the UKRA web site.

Use of Data

Data held by UKRA on present and former members is held and used primarily to support UKRA's functions.

- Data is required to ensure members have valid membership and suitable insurance.
- Information on membership, both current and former, is required in case of any current or retrospective insurance claims or criminal investigation.
- Details of the certification status of lapsed members will be held should they wish to recommence rocketry actives in the future.

Data Policy

1. The UKRA data retention policy aims to comply with the principles of the Data Protection Act 1998, listed at the end of this document.

2. Member data will be held primarily on a private database. Data held on local devices will be password protected and destroyed when no longer required. Access to member data will be restricted to only those who have a legitimate need for UKRA to fulfil its obligations.

3. Limited data will be available to associated individuals and organisations as required from time to time for UKRA to fulfil its functions. Any hard copy extracts will be marked 'Confidential' and will be destroyed when no longer required.

4. In the event of an enquiry from a legal body investigating possible criminal activity, or for the purpose of excluding the involvement of UKRA members in any such activity, UKRA is only required to divulge information if it believes there is legitimate reason to do so. In such an event UKRA will attempt to contact any members concerned and ask for their permission to release information. If UKRA does not believe that the legal body has sufficient grounds to justify divulging member information that legal body can apply to a court for the authority to compel UKRA to release the requested information, as stated in the relevant schedule of the Data Protect Act 1998. In the event of such an authority from a court or equivalent body, UKRA will release the information requested.

5. Member data will not be given, sold or exchanged with third parties for marketing purposes or other such commercial endeavours

6. Individuals and organisations with access to member data have a legal obligation to protect it against loss or theft. Should there be a loss or theft of data, the 'Guidance on data security breach management' from the Information Commissioner's Office shall be followed without delay.

7. Members can submit a Data Access Request at any time by emailing membership@ukra.org.uk

4 March 2013

Principles of the Data Protection Act 1998

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Complete versions of the act and relevant schedules can be found at;

http://www.legislation.gov.uk/ukpga/1998/29/contents

Further information is available through the Information Commissioner's office;

http://www.ico.gov.uk/