South Kesteven Amateur Radio Society

having fun with radio

Data Protection Policy

1. Information held and its use

SKARS may hold the following information on its members, given on membership forms

- Name / Call sign
- Address
- Telephone/Mobile phone numbers
- Email address
- Next of kin details
- Permission to hold personal data

It is for the purpose of administering membership and related to club activities with given consent for the purpose of communication of society activities

The exam secretary also handles information for candidates given on examination forms and/or via electronic communication

- Name/Call sign
- Address
- Telephone
- Email address
- Date of Birth

This is for the purpose of administering exams held by the society, data is sent electronically to the RSGB exam department via email.

2. Storage / Transmission

Membership data is held on paper records (membership forms) in the possession of the society secretary. It is also maintained in an electronic forms of a spreadsheet/database. (Copies of this data may be in possession of the chairman and treasurer for administrative duties).

The officers/committee of the society may communicate information electronically between themselves via email or other secure electronic media (such as Facebook messenger or USB stick).

3. Deletion

Membership expires at the end of February each year for those who have not renewed, all paper and electronic records for expired members should be deleted securely (paper records should be shredded)

Data held for examinations should be deleted and paper records destroyed when the outcome of examinations has been determined and results/call signs issued by the RSGB/Ofcom – for the next stage of licence progression the data should be recollected.

4. Storage of Data

Paper and electronic records should be kept securely whilst in possession of the officers of the society. Computers holding electronic records should be protected by up to date anti-virus and

malware protection.

Electronic communication should be via secure email servers, ideally using a separate account to personal communication. SKARS has secure email accounts under its web hosting for all officials if required. Care should be taken that only those who need the information are in communication/email threads and no attachments should be sent in replies/forwarded messages unless required.

Electronic records that need to be retained should be encrypted using password protection. Electronic records transmitted electronically should be encrypted using password protection.

Officers leaving posts and/or the society should handover all personal information they possess to successors or the committee and destroy any copies in whatever form.

5. Facebook/Social Media/Website/Society Promotion

The information collected and disseminated by social media platforms by members such as Facebook, Twitter, YouTube etc. are governed under their own policies.

Personal information posted by individuals on these platforms is deemed to be in the public domain. Moderators/Administrators of any 'club pages/groups/forums' will endeavour to remove inappropriate data if observed, but SKARS will not be held responsible for data breaches for data posted by individuals using these platforms.

SKARS maintains a website and will post reports and news about club activities on it and other social media accounts (Facebook/Twitter/YouTube etc.) It may identify members in photographs usually by first name and call sign.

The website has a member's only area which members must sign up for using the Wordpress system. The information held is a username and email address.

ACTIONS / POLICY

All data relating to lapsed memberships and examinations should be destroyed, including email communication with personal details attached or included.
All unnecessary backups/copies of electronic records to be destroyed
Officers to ensure secure data keeping practices. Recommend using secure USB memory devices with password protection.