Data Protection Policy

1. Ensure that the Secretary knows what personal data we hold, where we hold it and why we hold it. Ensure that any that is no longer required is destroyed.
2. Ensure that everyone is aware of the risks of identity theft and financial loss if personal data is lost or stolen.
3. No personal data shall be shared with third parties without the individual's express consent.
4. All devices handling third party personal data shall be password protected.
5. The circulated membership list shall be restricted to: name, email address, preferred phone number and emergency contact name and phone number. Any member not wishing to share these details (other than emergency contact details) must let the Treasurer know. Members must delete/destroy superseded membership lists when asked to do so.
6. Financial records shall be held securely by the Treasurer at home, applying the usual home security measures required by insurers. Correspondence, minutes, etc. containing personal data shall be held similarly by the Secretary at home.
7. Access to the mailing list of patrons shall be restricted to those needing to use it. The electronic list shall be password protected at all times and any paper records shall be held as in paragraph 6. Emails shall refer to the privacy policy on the website and include an opt-out clause. No emails shall reveal the identities of other recipients.
8. Financial records (but not the accounts prepared from them) shall be destroyed after 7 years. Booking details shall be destroyed when payment has been received and tickets have been issued. Duplicate copies of minutes and correspondence shall be destroyed after 3 years. Emails shall be reviewed at least twice a year and be deleted if no longer required. Members shall be reminded annually of their responsibility to delete records in accordance with this policy.
9. Any person ceasing to serve on the committee shall surrender, destroy or delete all documents they hold which contain personal data, unless it is also held for their personal, domestic or recreational purposes, or the individual has consented to share it or it is in the public domain.
10. The destruction of paper records containing personal data shall be by shredding.
11. All Subject Access Requests should be referred immediately to the Secretary, who will be responsible for verifying the identity of the applicant, determining what information has to be supplied (see www.ico.org.uk) and ensuring that a reply is sent within 30 days.
12. Any data breach should be reported immediately to the Secretary, who will decide if it should be reported to the ICO.
13. The NODA Privacy Policies relating to Patrons and Members/Supporters (adapted as necessary) shall be displayed on the website.
14. This policy shall be displayed on the society's website.