# Worcester Society of Artists
# Data Protection Procedures

21/08/2020

1. All personal data held by the Worcestershire Society of Artists (the Society) must be identified and a Schedule prepared.

2. The Schedule must document:
a. the type of data held
b. the details of the data held
c. how the data is collected
d. how the data is stored
e. what the data is used for
f. when the data is destroyed

3. Personal data must only be collected, stored, used and destroyed in accordance with the Schedule.

4. Consent must be obtained before any personal data can be held or used by the Branch. Giving an 'opt out' facility is not sufficient. The consent must be recorded.

5. Individuals can request that the Branch deletes their personal data. If the individual is a Member then their membership will be terminated.

6. Personal data must only be made available to members of the Committee or others, as defined in the Schedule, who need access to carry out their role or duties.

7. When sending e-mails to Members or other interested parties the latest list of e-mail addresses from the appropriate spreadsheet must be used as the data is frequently updated.

8. Any e-mails sent to all Members, must be sent via worcesterarts@googlegroups.com which by default does not show the e-mail addresses of recipients. Emails sent to selected groups of members (eg attendees/ exhibitors at an event) must be blind copied (Bcc), rather than sent or copied (Cc), to the distribution list so that the e-mail addresses are not revealed to recipients. Care must also be taken when forwarding an existing e-mail chain that e-mail addresses and other personal details are not revealed to the recipients**. This constraint does not apply to e-mails sent solely between members of the Committee.**

9. Any suspected or actual breaches of the Policy or Procedures must be reported immediately to the Data Protection Lead or, in their absence, to another Committee member. They will investigate and decide on any remedial or preventative actions to be taken and also report any non-trivial data loss to the Information Commissioner's Office within 72 hours of becoming aware of an actual data loss. All suspected or actual breaches will also be discussed and minuted at the next Committee meeting.

10. When someone joins the Committee they must confirm by e-mail to the Data Protection Lead that:
a. they have read the Policy and Procedures and will abide by them, and
b. agree that when they leave the Committee they will carry out the actions listed in paragraph 11.

11. When someone leaves the Committee they must:
a. pass any personal data they alone hold to another Committee member, and then
b. destroy all personal data they hold. Electronic data (e-mails, documents and spreadsheets) should be deleted and then further deleted from the recycle bin or deleted items. Such data must also be deleted from any data backups if possible. Any paper documents should be confidentially destroyed or returned to the Committee.

c. Confirm by e-mail to the Data Protection Lead that they have carried out the actions in a) and b) above.