GDPR: what does it mean for Surrey Association Officers?

GDPR applies to ALL Personal Data, however it is stored. "Personal" data is anything that, on its own or with other information, relates to an identified living individual. Personal data you hold as a private individual, such as your personal address book, is not covered. But any Personal Data you obtain from the Surrey Association IS covered, even if you were to copy it to your personal address book.

This short Guide applies to anyone collecting or using personal data about our Members, including visitors e.g., to a training course. It is not a complete guide to GDPR law – see https://ico.org.uk for more details.

The Surrey Association holds Personal Data about our Members:

- Name and contact details;
- Membership information, such as date joined, type of membership, subscription payments, tower and district affiliation, opt-in to various email lists;
- Optionally, demographic information such as age, gender, ringing ability.

The Surrey Association has a Privacy Policy, which lays out how we deal with the personal data we (and you, on our behalf) hold about our members (and others, such as contacts). If you are dealing with personal data on behalf of the Surrey Association, you must know what it says, and act accordingly. The full Policy, and supporting documentation, is on our website at: https://www.surreybellringers.org.uk/about-us/rules-and-policies/gdpr/

Personal Data must be acquired fairly, kept secure (against loss as well as unauthorised access), kept up-to-date, used only for the purpose it was originally collected for, and disposed of securely and promptly when no longer required for that purpose.

"Data subjects" (the persons to whom the data relates) have "subject access" rights. The General Secretary is responsible for responding to "subject access requests", and should you receive such a request you must forward it to the General Secretary. You may be required to respond to the General Secretary about data you hold in response to such a request.

Some simple Do's and Don'ts:

- Do refer to our data system MemberMojo whenever you need data about a member, complete your task, and delete the data from your possession. This ensures you use up to date Personal Data and reduces the risk of a security breach.
- Do email members using the MemberMojo email groups – use the Notices groups for Association business, the Network groups for your personal ringing interests. See the email guidelines at https://www.surreybellringers.org.uk/about-us/rules-and-policies/use-of-email-groups/
- Do use BCC when emailing if not using the MemberMojo groups – e.g. to attendees at an event
- Do avoid making any local copies of Personal Data from the Association. If unavoidable, e.g. for an Officer you work closely with, preferably keep the information separately (e.g. in a second contact folder) or mark the information in your address book with "Surrey Association" (e.g. in the Company field or with a #tag) so you can easily find and delete it when no longer needed or in response to a Data Access Request
- Do ensure locally held data is secure – password protected account used only by you, encrypted hard drive, etc.
- Do delete locally held data as soon as it is no longer needed – e.g. when you leave your role or when the event for which it was gathered is over. Do not keep it "in case it might be useful"!
- Do delete any email containing personal data, after processing it as required (e.g. updating MemberMojo)
- Do regularly check any local data to ensure it is still needed (delete if not) and accurate

- Don’t use data held by the Surrey Association for your personal purposes
- Don’t share data held by the Surrey Association with anyone, including other ringers, other than as explicitly covered in our Privacy Policy. Refer requestors to publicly available data (e.g. the website) rather than answering directly, or offer to pass on the request.
- Do treat data for under-18s and vulnerable adults with especial care.
- Do treat Safeguarding as more important than Data Protection. If in any doubt, consult the Safeguarding Officer and the Data Protection Compliance Officer
- Don’t ever email one-to-one to an under-18 or vulnerable adult. Always copy another adult such as parent, guardian, carer, or another Association Officer such as Master, General Secretary or Safeguarding Officer. If you receive a one-to-one email from an under-18 or vulnerable adult, always immediately reply copying such an adult.
- Do immediately report any suspected or actual leak of personal data to the General Secretary.