Guidelines for handling Personal Data under GDPR.

- All those responsible for handling & storing data should be familiar with our Privacy Policy.
- All data should be stored securely. If in paper form it should be in a locked cabinet. If in electronic form it should **not** be stored on a shared/public computer. It should be stored on a dedicated, password protected computer. Sensitive data will be additionally password protected.
- All data should be reviewed regularly (at least once per year) to ensure it is accurate and that we are not holding unnecessary data.
- Data no longer required should be deleted/shredded.
- Any data we hold should not be shared with third parties.
- Any emails sent out to circulation lists should use BCC. No one should be able to 'Reply All' to our mailings. This excludes groups which have previously consented to share email addresses for the convenience of communication, for example the Management Committee and Trustees.
- All general emailing should include the option to Unsubscribe with clear instructions as to how to do so.
  Example wording: *If you no longer wish to receive news updates from DACYP please reply to this email and mark 'Unsubscribe'. Thank you.*