



Southwell u3a Email Policy

Email is a convenient method of communicating with u3a members. However, a member's email address is personal data and is therefore subject to Southwell u3a's Privacy Policy and the general data protection regulations (GDPR).

Our Privacy Policy states that we will not normally store a member's personal data for more than 12 months after they leave Southwell u3a and accordingly, this time limit applies to stored emails or any other material that contains the member's personal data, including their email address. GDPR is for the protection of an individual's privacy.

The email policy applies to:

- 'Data controllers'; defined as the committee and trustees
- 'Data processors'; defined as anyone who stores and uses personal information on behalf of a data controller. This includes all members involved in managing and running all aspects of Southwell u3a.

GDPR and personal data

Email addresses provided in connection with an individual's membership of Southwell u3a may only be used for the following purposes:

- To provide u3a activities and services to members.
- For administration, planning and management of our Southwell u3a.
- To communicate with members about group activities.
- To monitor, develop and improve the provision of our u3a activities.

If you are a u3a group leader, to ensure you remain GDPR compliant:

- Do not share group members' email addresses (or other personal data) with other members of your group(s) without written consent.
- Any members' data you store and use may only be used for the furtherance of your role within the u3a.
- All personal data must be deleted within 12 months of the member leaving the u3a.

Email management

When sending emails to other u3a members, and when managing stored emails please follow the procedures set out below. This applies to emails to individual members, committees, groups, and members going on a u3a trip or holiday.

Beacon (preferred method)

- Using the u3a Beacon administration system means that the sender only compiles one message and each recipient receives a personalised email. No email addresses are shared. Since no data is stored on your computer or other digital device there is no need to 'manage' personal data or delete it when it is no longer needed. You can track delivery and whether the email has been opened through Beacon.

- If you wish to communicate with members privately, please use a personal email address. Using Beacon solely for u3a matters mitigates the risk of accidental disclosure of personal data.

Alternative methods

If you choose not to use Beacon, please use one of the two methods below. Whichever you choose, the digital device you use must be password protected. If other persons have access to your device, u3a members' email addresses and any other personal data held must be stored in a separate password protected file, and not in an address book or contacts' list that is available to all users.

Blind copy emails

- Where there is no need to share member's email addresses within a group or committee, the recipients' email addresses should be listed as blind copies ('Bcc'). This ensures that email addresses are not inadvertently shared.
- Please note that the copy of the email stored as a 'sent item' on your device will list the email addresses of the recipients. It will need to be managed in accordance with the privacy policy.

Open emails

- If you need members to be able to contact each other as part of running your group/committee/trip/holiday, you must obtain documentary confirmation (an email is acceptable) from each group member that they agree to their email address being shared with other members of the group, stored on group members' devices and used for group communications.
- You must retain each member's confirmation securely in accordance with our Privacy Policy.
- Please remember that the copy of the email stored as a sent item on your device will list the email addresses of the recipients. It must be managed in accordance with our Privacy Policy.

Deleting personal data from a computer or other digital device

A member's personal data must be deleted or destroyed when it is no longer needed for u3a purposes; this includes data stored in any back-ups. Most commonly, personal data needs to be deleted when a member leaves a group or a committee, or once a trip or holiday is finished.

You do not need to delete the leaver's email address if you have a lawful reason, unconnected with the u3a, to retain it. Lawful reasons may be because:

- you are friends and have agreed to use email to communicate with each other
- you are lawfully storing and using the leaver's email address because you are both members of another organisation that is subject to GDPR.

Consents

- If you obtained the member's consent to share their email address, you should retain that consent for 12 months after the member has left before destroying it.
- If you leave or change your role, consents must be passed to your successor.
- To minimise the risk of personal data being inadvertently shared, it is good practice for an outgoing leader to ask other group and committee members to delete their address

from all records. Additionally, the leaver should delete any group or committee member email addresses that they hold (unless there is a lawful reason to retain).

- It is not necessary for a group leader/committee chair to chase up and confirm that members have made the deletions.

Deleting personal data in practice

To prevent the leaver from receiving communication once they have left the group or committee, delete the leaver's email address from your address book and contacts list.

If using Beacon to send emails, remove the member from the list of group members, or ask the Beacon administrator to do so if you do not have permission to change the information on Beacon.

If you only retain u3a emails for a maximum period of 12 months, you do not need to check your Sent Items to delete old emails that contain the leaver's email address.

Managing stored emails

If you have cause to forward a stored email, be aware that the body of the forwarded message may contain personal data or other sensitive personal information, such as political or religious opinions, which are also subject to GDPR. It is therefore good practice to always check the content of an email you intend to forward and to delete any personal data or other sensitive material from it.

October 2024