THE UNIVERSITY OF THE THIRD AGE

Southwell U3A

Policy and procedure for using email

Email is an easy and convenient method of communicating with U3A members. However, a member's email address is personal data and is subject to our U3A's privacy policy and the general data protection regulations (GDPR). The use, storage and sharing of members' email addresses must be in line with our U3A's privacy policy and with GDPR. Our privacy policy states that we will not normally store a member's personal data for more than 12 months after they leave our U3A and accordingly, this time limit applies to stored emails or any other material that contains the member's personal data – in this context, their email address.

GDPR is for the protection of an individual's privacy. It applies to 'data controllers' – in our case, the committee/trustees, and to 'data processors' – those who are storing and using personal information on behalf of a controller; in our case all those who are involved with managing and running all the various aspects of our U3A.

To comply with our privacy policy and GDPR, you must follow the procedures set out below when sending emails to other U3A members and in managing stored emails. This applies to emails to individual members, committees, groups and members going on a trip or holiday.

Preferred method - Beacon

The preferred method for sending emails to U3A members is to use the U3A Beacon administration system. The sender only compiles one message and each recipient receives a personalised email. No email addresses are shared and no data is stored on your computer or other digital device. This avoids the need to manage personal data stored on your computer or other digital device, in particular making sure it is deleted when it is no longer needed. You can track delivery and whether the email has been opened through Beacon.

Alternative methods

If you choose not to use Beacon and prefer to send emails from your computer or other digital device, you should use one of the two methods below. In either case, the digital device must be password-protected. And you should ensure that the settings of your device do not lead to data being inadvertently shared through cloud storage, or features such as Homegroup in Windows 7 or Sharing Options in Windows 10 and some Linux systems. If other persons have access to that 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.

A. Blind copy emails

Where there is no need to share member's email addresses within a group/committee, the recipients' email addresses should be listed as blind copies ('Bcc'). This ensures that email addresses are not inadvertently shared within a group/committee or with other U3A members.

However, bear in mind that the copy of the email stored as a sent item on your device will list the email addresses of the recipients and will need to be managed in accordance with our privacy policy.

B. 'Open' emails

If running your group/committee/trip/holiday needs the members to be able to contact each other, i.e. for transport purposes, 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 the member's confirmation securely, whether it be on paper or electronically.

Once you have that confirmation, the recipient's email addresses can be listed in the normal way. Again, bear in mind that the copy of the email stored as a sent item on your device will list the email addresses of the recipients and will need to be managed in accordance with our privacy policy.

Deleting personal data from a computer or other digital device

To comply with our privacy policy and GDPR, a member's personal data must be deleted when it is no longer needed. Most commonly, this will be when a member leaves a group or a committee, or once a trip or holiday is finished. And the overreaching requirement to delete personal data within 12 months of the member leaving the U3A also applies.

If a member leaves a group or committee and the only reason you stored and used their email address was for U3A purposes, you must delete it. If you hold any other personal data related to the leaver, it must also be deleted/destroyed. This includes data stored in any back-ups. And the same applies if a group leader or committee chair is the leaver – data that was only stored and used for U3A purposes must be deleted.

But you do not need to delete the leaver's email address if you have a lawful reason unconnected with the U3A to retain it. This may be because you are friends and have agreed to use email to communicate with each other; or it may be that you are lawfully storing and using the leaver's email address because you are members of another organisation that is subject to GDPR.

If you had obtained the member's consent to share their email address, you should retain that consent for 12 months after the member has left the group before destroying it – or pass the consents onto the new group leader/committee chair where the leader or chair is leaving.

To minimise the risk of personal data being inadvertently shared, it is good practice for a group leader or committee chair to ask other group/committee members to delete the leaver's email address from their records; and the leaver to delete any group/committee member email addresses that they hold (unless those concerned have a lawful reason to retain the email address as above).

For the avoidance of doubt, 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

From a practical perspective, the most important thing is that the leaver does not receive any further communication once they have left the group or committee. So you should delete the leaver's email address from your address book/contacts list immediately – or if using Beacon to send emails, remove the member from the list of members on Beacon, if the membership secretary has not already done this.

But you do not need to immediately trawl through your sent items to find and delete old emails that contain the leaver's email address. Instead, if you adopt a practice of only retaining emails sent on U3A business for a maximum period of 12 months, this will ensure your records comply with our privacy policy. Habitually deleting U3A emails more than 12 months old avoids the need for a specific exercise when member leaves a group or committee.

Managing stored emails

Deleting stored emails as described above should reduce the risk of personal data being inadvertently shared. If you have cause to forward on a stored email, be aware that the body of the forwarded message may contain personal data or other sensitive personal data, 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 on and delete any personal data or other sensitive material from it.

August 2018