Yorkshire and the Humber Region

Data Protection Policy

This Data Protection policy was adopted by the Regional Committee at a meeting on xx/xx/xx
Last reviewed by the committee on xx/xx/xx

Introduction

The YAHR Committee collects data from members of its member U3As.
It is the Committee's intention to comply with the new Data Protection Act coming in to force in May 2018. This is the act which gives force to the European General Data Protection Regulation (GDPR).
All committee members should read this policy and confirm they have done so to our secretary.

Definitions

Data Controller
This is the organisation not an individual. In our case it is the Regional Committee. The data controller determines what data to collect, how it is processed and what it is used for.

Data Processors
These are organisations that process data on behalf of the Data Controller. Processing includes the storage of data so if we were to use online storage like Google they become one of our data processors.

Data Protection Officer
There is no formal requirement to have one but the Committee has appointed one of its members to be so. Their role is to be aware of how we process and use members' data and ensure we do not breach our policy for data protection. They also make sure that the committee reviews our policy and its implementation at least once a year.

Our Policy

Legitimate Interest v Consent
We do not have to ask for individual's consent to contact them when it is in our legitimate interest to do so. But first we need to assess what our legitimate interests are. To do this we need to (a) identify our interests, (b) check that they are necessary and (c) balance them against the "rights and freedoms" of the individual.

a) Our constitution tells us that our objectives include developing the educational, cultural and social interest of the U3A movement in the Region and encouraging joint activities including events such as Summer Schools, Study Days, Seminars or Conferences. In order to do this we need to communicate our activities to our member U3As and their members.

b) Our only practical way of communicating is by asking individuals for their email address, storing it on a database and using it to tell them about our activities.

c) Would a member reasonably expect us to use their data in this way? Yes, because they have already expressed an interest in our activities by attending a seminar or requesting news or sending us their email address when they become chair or secretary of their U3A. We tell them that we will use their information in this way in our

Privacy Policy and at the point when they provide their email address.
Does the processing of their data in this way impinge on their rights and freedoms?
No, but when we email people we should always give them an opportunity to unsubscribe.

Note that we should not pass individual's email addresses on to any other organisation including our member U3As. If we thought it necessary to do this we would need to ask individuals for their explicit consent.

Evidence of members engaging with our legitimate interests
We need to record where and when individuals provide their data to us so that we have evidence of these circumstance.

Putting our policy into practice
Our flyers which advertise our activities should inform members how we plan to use their email address i.e. use it to tell them about future activities.
The forms on our website which we use to collect members' data should do the same.

Processing - External
The organisations that we use are:-
Airtable to store data that we collect in forms on our website
Mailchimp to send out mass emails

A risk assessment of these organisations is contained in Appendix B

Volunteers with access to these applications are listed in Appendix C

Processing - Internal
Our admin secretary maintains lists of members who have registered for events.
These lists are deleted within two months of the event.
Our secretary also maintains a list of chairs & secretaries of U3As in our region.
Our website manager maintains a list of members who have registered for events or have asked to receive news from YAHR.

See Appendix C for risk assessment.

Notification of a Breach
Should we learn that there has been a breach in security we will inform the National Office as soon as possible and take their advice before informing members that might be affected or the Information Commissioners Office. The latter should be informed within 3 days.

Retention of Data
Every 2 years we will email everyone who has been on our mailing list for more than 2 years asking them to sign up again if they continue to wish to hear from us. That way we will never have anyone on our list who we have not heard from for more than 2 years.

Moving Data by Email
On the rare occasions when lists are moved from one volunteer to another they should be in an encrypted spreadsheet.

Sending personal emails
When sending emails to 10 or more people we should use the "Bcc" facility so that the email list is not broadcast to everyone on the list.

Personal Details on our website

We should not publish any personal contact details on our website unless the individual has given their explicit consent; e.g. our admin secretary's address for correspondence.

Scam Emails

Committee members should be aware that role based email addresses are openly available on our website. This means that scammers can send an email from chair@yahrU3A.co.uk to treasurer@yahrU3A.co.uk requesting the treasurer to transfer money.

Appendix A

Yorkshire & the Humber Region Committee

Privacy Policy

Introduction
This privacy notice sets out the way we process your information and how we use it. We will refer to this policy when we ask you for your consent. The Data Controller is the YAHR Regional Committee and is subject to the General Data Protection Regulation when it takes effect on May 25th 2018.

How we collect your information
We collect your personal information in three ways:-

- When you register to attend one of our events
- When you complete a form on our website requesting news of our activities
- When you, as chair or secretary of your U3A, tell us that you have taken up this role

Information we collect

- Your name and for some activities your postal address
- Your email address
- The U3A that you belong to
- Your role in this U3A as appropriate
- Any special dietary or access requirements

How we use your personal information
We process your information for our legitimate interests in fulfilling our objectives as laid down by our constitution. These include developing the educational, cultural and social interest of the U3A movement in the Region and encouraging joint activities including events such as Summer Schools, Study Days, Seminars or Conferences. You have the right to object to this processing if you wish and to do so contact our secretary - see below.

We use your information in the following ways:-

- If you are the chair or secretary of your U3A we use it to send you information for distribution to other members of your committee and members of your U3A.
- To send you information about events that we have arranged or any activity that we judge to be of interest to you as a U3A member.
- In the case of special dietary and access requirements we use the information when we arrange catering and access to events.

Sharing your information with others
We do not share your information with any other organisations other than our data processors. These are:

Airtable to store data that we collect in the forms on our website
Mailchimp to send out mass emails

We have made a risk assessment of these organisations and are satisfied that the risk of a security breach is low.

How long is your information kept
Every 2 years we will email you and ask you to sign up again if you wish to continue to hear from us.

Your Rights
You have the right to ask us, in writing, for a copy of all the personal data held about you. (This is known as a "subject access request"). You should write to:-

YAHR Secretary, 361 Bricknell Ave, Hull, HU5 4TN

If you do this you should include your telephone number so we can verify your identity.

You can also ask us to delete all the information we hold about you and you can make this request by email to secretary@yahrU3A.co.uk or in writing to the address above.

Updating and amending your personal information
If your information needs amending you should inform our secretary via secretary@yahrU3A.co.uk

Contacting us about your data
If you have any queries about the use of your data please contact our secretary as above.

This Privacy Policy was last updated on 28th March 2018

Appendix B

Security Assessment of External Processors

We are satisfied that the two external organisations we use to process members' data have good security practices and therefore pose a low risk to the security of members' data. We have based this judgement on the statements that they have made on their websites.

Airtable

Airtable make this statement on their website*:-

> Maintaining the security and privacy of our customers' data is our utmost concern at Airtable -- our success and credibility depend on it. All data you enter into Airtable remains yours, and we are committed to ensuring that your data is not seen by anyone who should not see it. Airtable's data is encrypted both when it is sent to and from our servers, as well as when it is at rest. To protect your content in transit, Airtable uses 256-bit SSL/TLS encryption. At rest, Airtable content is protected using 256-bit AES encryption.
>
> Airtable's production data is regularly backed up to a separate, isolated location and all backups are encrypted. You also have the option to manually back up your bases by exporting individual tables as CSV files or by retrieving your data via the Airtable API.

**Airtable - Support/Policies and Guidelines/Airtable Security Practices*

MailChimp

MailChimp make the following statements on their website*:-

Data Center Security
MailChimp delivers more than 20 billion emails a month for millions of users. We use multiple MTAs, placed in different world-class data centers, around the US.
Our data centers manage physical security 24/7 with biometric scanners, and the usual high tech stuff that data centers always brag about.

Protection from Data Loss, Corruption
All large account databases are kept separate and dedicated to prevent corruption and overlap. Smaller and free user accounts** are placed into the same large database for speed. As accounts grow in list size, they are migrated into their own distinct databases. Account data is mirrored and backed up regularly off site.

**The is the case for YAHR data

Application Level Security

- MailChimp account passwords are hashed. Our own staff can't even view them. If you lose your password, it can't be retrieved—it must be reset.
- All login pages (from our website and mobile website) pass data via SSL.
- The entire MailChimp application is encrypted with SSL.
- Login pages have brute force protection.
- Logins via the MailChimp API have brute force protection.
- We perform regular security penetration tests, using different vendors. The tests involve high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.

Internal Protocol & Education

- All new employees on teams that have access to customer data (such as tech support and our engineers) undergo criminal history and credit background checks prior to employment.
- *The Art of Deception*, by Kevin Mitnick, is required reading for all new employees. *Fatal System Error*, by Joseph Menn, is extra credit.
- All employees sign a Privacy Safeguard Agreement outlining their responsibility in protecting customer data.
- All new employees are given security guidelines for using social media, including information about social engineering.

**https://mailchimp.com/about/security/*

Appendix C

Internal Processing - Security Assessment

Our admin secretary maintains lists of members who have registered for events on her laptop. These lists are deleted within two months of the event.
Our secretary permanently maintains a list of chairs and secretaries of all the U3As in our region.

Our website manager maintains a list of members who have registered for events or have asked to receive news from YAHR. This list is stored on a desk-top PC. It was noted that this PC was rarely connected to the internet and was not used for handling emails on a daily basis.

Both these processes are assessed as low risk.

Permission to access data stored on-line

Airtable

The website manager has administrative control over this application.
The admin secretary has read only access.

Mailchimp

The website manager has administrative control over this application.
No other volunteers have access.