Heatons and Reddish U3A

Data Protection and the General Data Protection Regulation 2018

This policy sets out the guidance for members of the Heatons and Reddish U3A in relation to the GDPR regulations of 2018

What is GDPR?

The General Data Protection Regulation (GDPR) is an update to the existing Data Protection Act 1998 (DPA). GDPR will apply in the UK from 25 May 2018 and will replace the DPA.

What are the main changes from the DPA to the GDPR?

The main changes that affect U3As are the requirements relating to processing data and accountability. U3As will also need to evidence how you are complying with the principles of data protection which includes evidencing that members provided **a contractual relationship** via the contractual application forms.

What data do we currently gather?

Heatons & Reddish U3A collect personal data about our members via application and renewal forms. Personal data means any information relating to an identified or identifiable natural person. This includes the information needed for membership purposes such as:

- A member's name.
- Postal address.
- Telephone number/s.
- Email address.
- Photos.
- Videos.
- Articles written by members.

Due to the nature of the work of the Heatons & Reddish U3A it is perfectly legitimate for us to request this information. As long as H&R can substantiate the basis for gathering the information and the members are contracted for obtaining the information then requirements of GDPR for gathering this information are met. Photographs and videos also constitute personal data and **a contractual relationship** will need to be obtained in both taking and displaying photographs/videos of the membership.

Special Categories/disability.

Should personal data in this category need to be recorded e.g. physical or mental health conditions, **Central Office can be contacted for advice if needed. If this additional information is required it will be obtained with the consent of the member who will be informed as to why this information is required and the purpose that it will be used for.**

Data will be held confidentially and only intended for use in the Heatons & Reddish U3A

Data Protection Principles

There are 8 data protection principles that were established under the DPA. For the purpose of this policy the focus is on what Heatons & Reddish U3A needs to do to ensure compliance. Changes affecting the U3A group refer to Processing data and Accountability

Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner.

Requirement

- Inform members as to what their personal information will be used for.
- Inform members as to how their information will be held.
- Gain **a contractual relationship** from members to hold their information.
- Gain **a contractual relationship** from members to communicate with them for different purposes i.e. **renewal**, general U3A information, specific group information.

- Inform members as to how they can withdraw **from the contractual relationship** for their information to be used.

Action by Heatons and Reddish U3A

1. 1. Data is **currently** held on a passworded Microsoft Access database that is held on Microsoft OneDrive. **The database password is known only to the Membership Secretary and the Secretary. When used by either the database is downloaded to the computer of the Membership Secretary. This data has been migrated to Beacon, an approved U3A Trust programme, and will be used for renewals going forward from 8th October 2019. The password is known only to the Membership Secretary and the System Administrator (in this instance the Secretary.) Currently the e-mail addresses are released to the Newsletter Editor as and when required.** Data is shared with the U3A Trust for those members who subscribe to the magazine. Information held by Group Leaders is also confidential. There is no expectation that the H&R U3A needs to gather contractual **relationships** retrospectively but systems need to be implemented for this to go forward. (Application and renewal forms)

2. Gain **a contractual relationship** to hold information at the point at which members provide their details

3.To assist with this, privacy statements have been added to the forms that are in use to recruit members to the H&R U3A.

4. The committee need to review if there are other ways that the H & R U3A is asking members for their information i.e. are group leaders also gathering information.

5. The contractual **relationship** information needs to be refreshed when information changes e.g. at renewal.

6. Retain the documents used to gather **a contractual relationship** as they will constitute the evidence you need to demonstrate compliance. Details will be backed up on computer and back up disk.

7. Ensure that any documents are retained securely.

8. Data to be retained by the Membership Secretary for no longer than 12 months as paper copy and computer back up, except names and year of joining will be kept until the member is no longer in the U3A.

9. Currently the Membership Secretary, **Secretary (Beacon Administrator)** and the Newsletter editor to be the persons who have access to the data.

10. Any queries to the Membership Secretary.

11. The Membership Secretary will take action to remove data and inform the member should they make a complaint and wish to leave the group.

12. To provide a prompt and comprehensive response the Membership Secretary will complete a form about the complaint and give a copy to the member.

Principle 2 – Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Requirement

- Only use members' information for the purposes that they have provided their agreement to.
- Gain additional contractual **relationship** for transferring data outside of the H & R U3A e.g. to a travel company for a trip.

Action by H&R U3A

1. Be specific about what the U3A is going to be using member information for. Information will be used for furthering the activity of the Group. Further use will need **an additional contractual relationship.**

2. Members information is not available for any marketing purposes.

3. Ensure that group leaders are aware of what communications are considered 'appropriate'.

4. Members to be informed that Group Leaders may seek to communicate with Group members by email to facilitate the administration of their group. Addresses held by Leaders should be deleted when a member no longer shows an interest in the group

5. The H&R U3A will be as transparent as possible with how the U3A operates in relation to its communications with members.

Principle 3 – The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.

Requirements

- Limit the information gathered from members to what is needed for membership and accounting purposes.
- Consider and review on an ongoing basis what information the H&R U3A needs and what purpose it is used for.
- When investigating complaints that might require the H&R U3A to request further personal information from a member be sure to record any meetings accurately.

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

Requirements.

Keep up to date and accurate records. Members to be asked to inform the Membership Secretary of any changes in their personal data.

Action by H&R U3A

1. Ask members to keep their information up to date by contacting the membership secretary with updates or changes.
2. If a member does not renew their membership their data will be deleted.
3. Where the H&R U3A needs to retain data for a longer period in order to meet any legal or statutory requirements the relevant member will be informed.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisation measures required by the GDPR in order to safeguard the rights and freedoms of the individuals.

Requirement

Archive or delete information that is no longer required for membership purposes.

Action by H&R U3A.

1. Member information will be retained for 12 months or when a specific situation is resolved.

2. Not use member data for communication purposes beyond the period of their membership unless there is a specific and agreed need.
3. Data is deleted from the data base and paper copies shredded.

Principle 6 – Personal data must be processed in accordance with and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Be aware of what an individual's rights are:

Requirements.

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.

Action by H&R U3A.

1. By following the key principles as detailed within this guidance the H&R U3A should not be infringing the rights of its members.

2. The membership can make a 'subject access request' (a request to view the data that is held on them) to the membership secretary or newsletter editor which will be responded to within 14 days.

3. The Committee to review the policy and practice in relation to data on an ongoing basis.

4. Discuss data protection within the steering committee and provide information for new committee members.

5. Ensure group leaders are aware of expectations in relation to data protection. Provide group leaders with written documentation on data protection.

6. Liaise with National Office if you encounter any issues that the U3A is unsure about or needs further guidance.

7. Discuss data protection at network meetings if the U3A is a network member.

8. Adopt a data protection policy and privacy policy.

Principle 7 – Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Requirements

- Keep personal data and special categories of personal data secure.
- Discuss and agree processing arrangements with any 3rd party suppliers such as venues, travel agents, etc.

Action by H&R U3A.

1. H&R agree that full and partial membership information is restricted to the **Membership Secretary and the Beacon Administrator and when needed by the Newsletter editor. Data information and 3rd Age Magazine info is kept in a secure manner.**

2. The membership Secretary is permitted to process (create, view, change, delete, download) personal data under the guidance of the U3A committee.

3. Members to agree, via a **contractual relationship form**, to information being passed on to a 3rd party and informed as to what information will be passed on.

Principle 8 – Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

Requirements

Members to be informed of any circumstances where information would need to be transferred outside of the EU.

Action by H&R U3A

1. Check whether there are any third party suppliers which the U3A supplies information to who may pass member information to parties outside of the EU.

2. Talk to National Office who will obtain advice if you intend to transfer any personal data outside of the UK and the EU.

Data security and emails

Requirements.

1. Encourage all members with access to the data base to use strong passwords – the recommendation is that these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.

   Avoid sharing password with others. Encourage members not to keep passwords written down somewhere where they can be easily accessed and identified.

2. Avoid leaving PCs, laptops or other devices with sensitive information on them left in such a way that someone else could easily access that information.

3. When sending confidential information by email use password protection.

4. Avoid opening e-mail attachments from an unknown source.

5. Consider purchasing firewall software for committee members PCs, laptops or other devices. This can be purchased and downloaded from the internet.

6. Avoid keeping written records of negative comments about H&R U3A members or suppliers. Where there is an issue between members ensure that any recordings are factual and avoid recording opinion unless directly from an interview. For serious matters, please contact National Office for support.

7. Avoid sending emails that could be considered offensive or discriminatory.

If a PC, laptop or device is stolen or lost that holds a large amount of member information please contact National Office.

Accountability and governance

The GDPR requires organisations to be able to demonstrate that they comply with the data protection principles.

Action by H&R U3A.

1. Review the H& R U3A current policies and data protection practice and record this formally once a year in committee minutes.

2. Add data protection to the agenda of the H&R U3A committee meetings and minute the meetings.

3. Access training for committee members and other data users.

4. Ensure practice is transparent by adopting policies and putting statements regarding privacy on H&R U3A paperwork and the website.

5. Follow through on the things that the policy says H&R U3A will do.

6. Induct new committee members and group convenors in the principles of the GDPR and how they apply in practice.

7. Committee members will stay up to date with guidance and practice within the U3A movement and will seek advice from the Third Age Trust National Office should any uncertainties arise. H&R U3A Committee will review data protection requirements on an ongoing basis as well as reviewing who has access to data and how data is stored and deleted. When Committee Members and Group Leaders relinquish their roles, they will be asked to either pass on data to those who need it and/or delete data.

Breach notification

The GDPR will introduce a duty on all organisations to report certain types of data breaches to the relevant supervisory authority, and in some cases to the individuals affected.

Action by H&R U3A.

On discovering a breach investigate the extent of the breach:

How many members does the breach potentially affect?

- What personal information has been exposed?
- How did the breach occur?

1. Keep a record of actions taken since the breach was discovered and take any immediate actions needed to reduce any further breaches.

2. Contact National Office to discuss whether or not the Information Commissioner's Office needs to be informed of the breach. These will be reviewed on a case by case basis.

3. Report serious breaches i.e. ones that could risk the rights or freedoms of individuals.

4. Be aware of timelines for serious breaches as these need to be reported within 72 hours.

5. Inform members, as required, if there has been a data breach providing them with full information.

As agreed by the committee on 26th September, 2019