Maghull & Lydiate U3A

# Data Protection & Privacy Policy

## Introduction

Maghull & Lydiate U3A Committee collects data from all new and existing members and therefore has a legal obligation to comply with the new UK Data Protection Act[1], which came into force in May 2018. This is the act which encompasses the European General Data Protection Regulations (GDPR). We must also ensure that all data collected and stored within the U3A is managed correctly. Ensuring that personal data is accurate and up to date. It 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, theft, destruction or damage, using appropriate technical or organisational measures with integrity and confidentiality.

## Definitions

### Data Controller

This is the organisation not an individual. In our case it is the Maghull & Lydiate U3A 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 such as 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.

### Accountability Principle

GDPR introduces an accountability principle that requires U3As to be able to demonstrate compliance with the data protection principles. The principles refer to a 'Data Controller' (*see earlier definition*). However, when managing groups, group leaders will assume joint responsibility with the Committee for how data is processed and managed.

## Our Policy

### Legitimate Interest v Consent

We do not have to ask for an individual's consent to process their data or 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 full Legitimate Interest

[1] https://ico.org.uk/for-organisations/data-protection-act-2018/

Assessment has been carried out and is available to view on request.

a) Our constitution tells us that the objects of our organisation include "the advancement of education and, in particular, the education of older people...". We do this by offering membership of our organisation.

b) It is in our legitimate interest to collect and store personal information from our members **in order to provide the services associated with this membership.**

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 becoming a member of the 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 information. Does the processing of their data in this way impinge on their rights and freedoms? No, but when we email people with information/news **we should always give them an opportunity to unsubscribe**. Note that we should not pass individuals' email addresses on to any other organisation or other members. If we thought it necessary to do this we would need to ask individuals for their explicit consent**. When we provide personal information to third parties we will always seek 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 circumstances.

## Putting our policy into practice

The forms which we use to collect members' data, members' requests, etc. inform members how we plan to use their personal data. **This information is also contained within our Privacy Policy. Please refer to Appendix A.**

## Processing - External

The organisations that we provide information to are (currently):

- The Third Age Trust and its distributors to enable them to deliver their Trust Magazines.
- HMRC, who have a right to receive personal information regarding Gift Aid subscribers.

**A risk assessment of these organisations is contained in Appendix B**

## Processing - Internal

- Our membership manager and team operate the system for registering new members and renewal of annual membership.
- Our database manager maintains and manages the list of members' details.
- Our website manager maintains a list of members who have registered for various access rights to the website.
- A group leader may request information to assist in the management of the group.
- All members have a responsibility to manage theirs and other members' data correctly.
- From 2019, anyone wishing to obtain a copy of the membership database will be required to request a copy in writing to the Data Protection Officer, giving the reason for the request.

**Please refer to Appendix C for the Internal Processing 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. We will take their advice before informing members that might be affected or the Information Commissioners Office (ICO). The latter should always be notified within 3 days.
**Please refer to Appendix E - What Constitutes a Data Breach?**

## Retention of Data

- Lapsed members' details will be removed from that year's renewal database in June.
- Members' information required by HMRC will be retained for seven years.
- Members' details required for legal reasons such as an insurance claim, complaint, etc. will be retained until the process is complete but may need to be held indefinitely.
- Financial documents will be retained for at least seven years.
- AGM reports, annual accounts and minutes should be retained for the life of the association.
- Committee meeting minutes should be permanently retained but, where it is difficult or impractical to do so, a minimum of six years is recommended.
- Committee members and group leaders who hold information will delete or return all files and documents when relinquishing their roles.

## Committee Members and Group Leaders Responsibilities

**Please refer to Appendix F for further information.**

## Moving Data by Email

On the rare occasions when lists are moved from one volunteer to another they must be in a password-protected document.

## Sending Emails

When sending emails to four or more people we should use the "Bcc" facility so that the email list is not broadcast to everyone on the list. **Please refer to Appendix F - GDPR – Committee/Group Leaders' Responsibilities, for further guidance.** Don't give out members' data without their consent.

## 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. group leaders' contact details etc.

## Scam Emails

Committee members should be aware that scammers can send an email from what appears to be a legitimate email address requesting members' details or the treasurer to transfer money. Always physically check that the intended recipient is legitimate.

**≈≈≈≈≈ END ≈≈≈≈≈**

# Appendix A

# 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 specific consent, or use your data in our legitimate interest. The Data Controller is the Maghull & Lydiate U3A committee and, when necessary group leaders. All members are subject to the General Data Protection Regulations which are encompassed within the UK Data Protection Act, which came into effect on 25th May 2018.

### How we collect your information

We collect your personal information in three ways:-

- When you register to become a member or when you renew your membership.
- When you complete a website request.
- When you provide information to a group leader to assist in the management of the group.

### Information we collect:

- Your name and postal address
- Your email address
- Your phone number(s)
- Your role in this U3A as appropriate
- Your Gift Aid preference
- If you wish to receive The Third Age Trust magazines
- If you wish to be included within U3A photographs

### 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 interests of the U3A movement in the area. You have the right to object to any of this processing if you wish, and to do so, please refer to **Your Rights** section, below.

### We use your information in the following ways:

- The administration of membership;
- To tell members about the activities they can take part in;
- To inform members generally about the activities of our U3A and the wider U3A movement;
- To provide notice of our AGM;
- When a member has expressed an interest in joining a group, provide group leaders with individual member's contact details for the purposes of inviting them to join the group;
- When necessary, to provide group leaders with their groups' contact details.

### Sharing your information with others

We do not regularly share your information with any other organisations other than our data

processors. These are:

- The Third Age Trust and its magazine distributors.
- HM Revenue & Customs (Gift Aid claims).

Due to the nature of these organisations we are satisfied that the risk of a security breach is low.

We will also, from time to time, provide information to the likes of venues, travel agents, data managers, printers, etc. Those responsible for obtaining/providing these services will undertake individual risk assessments at that time to ensure that third party processors are GDPR compliant.

**Holidays, Short Breaks and Overnight Stays** - Members going on a holiday will always be asked to carry with them, clear and up to date personal and medical details, including next of kin for use in the case of an emergency. **This is the responsibility of the individual concerned** (further information is contained within item 7 of Appendix F (iii) of the Group Leaders' Handbook). No information will be retained by the U3A. Travel agents may request next of kin details. For expediency, group leaders may collect this data to pass directly to the travel agent. Once again no data will be retained by the U3A.

**Group Day Trips -** All U3A members will be provided with a Next of Kin section on the back of membership cards from 2019 **(which must be filled in)**, for members to carry with them, negating the need for the U3A to obtain, store or process this type of data.

The U3A requests all members to inform the person identified as their next of kin, that they are using their details as described above.

## How long is your information retained?

Lapsed members' who do not renew their membership by June will be removed from that year's database. Members' information required by HMRC will be retained for seven years. Members' details required for legal reasons such as an insurance claim, complaint, etc. will be retained until the process is complete but may be retained indefinitely for legal reasons.

## Your Rights **(Please refer to Appendix D for a list of 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"). To do this, you should contact the U3A either:

- by ***EMAIL*** to ***mandlu3a@gmail.com*** for the attention of the Data Protection Officer. If you do this you should include your telephone number so we can verify your identity.
- or ***IN PERSON*** by visiting the Coffee Morning and speaking to a Committee Member.

You can also ask us to delete some or all of the information we hold about you and you can make this request by contacting the U3A, either by ***EMAIL*** to ***mandlu3a@gmail.com*** for the attention of the Data Protection Officer, or ***IN PERSON*** by visiting the Coffee Morning and completing a Data Removal Form available from the Membership Desk.

***PLEASE NOTE: If you request us not to store or process your contact details (Name & Address) we will be unable to offer you any of the services provided by Maghull & Lydiate U3A.***

**Updating and amending your personal information**

If your information needs amending you should inform us, using one of the above methods.

***If you have any queries about the use of your data, please talk to our Data Protection Officer using one of the above contact methods.***

## Policy Review

This policy and its implementation will be reviewed at least annually and whenever there are any legislative changes or amendments to guidance issued by relevant statutory bodies.

***This Policy was adopted by Committee on:*** 12th MARCH 2019***.***

# Appendix B

## Security Assessment of External Processors

We are satisfied that HMRC 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 website.

The information obtained from The Third Age Trust was a little less clear as their privacy policy mainly relates to their websites and we only have a verbal response to the question regarding the Trust magazine distributor. On the basis of the information provided we must assume that they also have good security practices and therefore pose a low risk to the security of our members' data.

---

## HM Customs & Revenue[2]:

HMRC is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you in accordance with data protection law, including the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018

**Data protection principles**

We'll comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and kept up to date.
5. Kept in a form that identifies you for only as long as necessary for the purposes we have told you about.
6. Kept securely.

## The Third Age Trust[3]:

**Our first question:** "Unfortunately I can only find the privacy policy relating [primarily] to your websites online. I would be grateful if you could provide me with the data protection & privacy policies for the Trust, not including the website".

***Their answer was:*** *"Our privacy statement is on the website – possibly updated since you last asked". N.B.: the privacy statement has not been updated since we last asked.*

---

[2] https://www.gov.uk/government/publications/data-protection-act-dpa-information-hm-revenue-and-customs-hold-about-you/data-protection-act-dpa-information-hm-revenue-and-customs-hold-about-you

[3] https://u3a.org.uk/privacy-policy

**Our second question:** "With regard to the distribution of the Trust's magazines, can you tell me if an assessment of the distributor's compliance with GDPR has been undertaken and if so, could a copy of the assessment be made available".
***Their answer was:*** *"We have ensured that they are GDPR compliant but this didn't constitute a written assessment".*

# Appendix C

## Internal Processing - Security Assessment

Our database manager maintains lists of members who have registered or renewed their annual registration. Lapsed members' data is removed from the main database in June of that year.

Our committee secretary permanently maintains a list of committee members and officer responsibilities, their names (only) are displayed on the MBC notice board.

Our website manager maintains a list of members who have registered for various levels of access to the website.

Our newsletter editor maintains a list of members who may wish to contribute to the newsletter.

The data review confirmed that group leaders generally maintain (using various methods) contact details relating to their individual groups, although a small number of anomalies have been identified (detailed later in this section).

Members who manage holiday groups, overnight stays and day trips temporarily manage booking/contact details which are deleted at the end of a trip. From membership renewal in 2019 members' next of kin details will be located on the reverse of membership cards. Members must be reminded to carry their card with them at all times when engaging in holidays, overnight stays and day trips. No next of kin details will be retained by M&L U3A.

Various officers, such as Group Support, the Welfare Officer and Holiday Group Leaders also require the use of the database to allow them to undertake their duties.

All of these processes are assessed as low risk, apart from the anomalies referred to below.

As a result of the data review, it has been identified that several group leaders have a mixture of new and old copies of the membership database. From 2019, in line with Head Office recommendations, to improve data security, access to the full database by members will be restricted on a strictly need-to-know basis.

# Appendix D

## The list of a Data Subjects Rights

GDPR requires organisations to be aware of individuals' rights which are:

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

# Appendix E

## What Constitutes a Data Breach?

A personal data breach is about more than just losing personal data. It means a breach of security which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Some of the ways you could suffer a breach are:

- Weak/stolen credentials e.g. passwords;
- Lost/stolen computing devices ***(including memory sticks)***, containing personal data;
- Systems and application vulnerabilities;
- Malware attacks;
- Insider threats;
- User error;
- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Sending personal data without consent ***(someone asks you for a friend's contact details)***;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

Cyber-crime and hackers present an ever-present threat to organisations. While effectively ensuring your defences against these types of attacks is critical, many data breaches are caused by human error. **Loss of paperwork, data sent to the wrong recipients, insecure disposal of hardware, loss of unencrypted devices and failure to redact names are all avoidable.**

# Appendix F

## DATA PROTECTION – COMMITTEE MEMBERS & GROUP LEADERS RESPONSIBILITIES

Maghull & Lydiate U3A Committee collects data from all new and existing members and therefore has a legal obligation to comply with the new UK Data Protection Act[4], which came into force in May 2018. This is the act which encompasses the European General Data Protection Regulations (GDPR). We must also ensure that all data collected and stored within the U3A is managed correctly. Ensure that personal data is accurate and up to date. It 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, theft, destruction or damage, using appropriate technical or organisational measures.

**GDPR also requires organisations to be aware of individual's rights which are:**

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

**Accountability Principle**

GDPR introduces an accountability principle that requires U3As to be able to demonstrate compliance with the data protection principles. **The principle refers to a 'data controller' however, group leaders will assume joint responsibility with committee members for how data is collected, processed and managed.**

**To ensure compliance, please make sure you follow these guidelines:**

- Although we do not have to ask for an individual's consent to process their data or contact them when it is in our legitimate interest to do so, **please note,** we should not pass individuals' details to any other organisation or other members. If we thought it necessary to do this we would need to ask individuals for their explicit consent**. When we provide personal information to third parties *(who could be within the U3A)* we will always seek explicit consent.**
- Consent forms will be securely stored for evidential purposes, as we may be required to provide proof of compliance.
- All information must be stored securely and used for membership purposes only:
  - To communicate with U3A member on U3A business;
  - To send general information about The Third Age Trust;
  - To ensure that data is being used for membership purposes only, as detailed above;
  - That only data pertaining to U3A business is collected and stored, i.e. only collect relevant information.
- Consider who within the U3A needs access to the full membership information and restrict access to only those who need it.
- Only share data with group leaders for those groups that someone is a member of.
- Inform members where information is to be passed to a third party such as venues, travel

[4] *https://ico.org.uk/for-organisations/data-protection-act-2018/*

agents, data managers, printers etc. and ensure that third party processors manage data securely and are GDPR compliant.

- Ensure consent is obtained from members for photographs taken during U3A events which may be used on the U3A website, newsletter or literature. Should any member not consent to the future use of the photograph ask that member to step aside from the photograph?

**Data Security and Emails**

- Ensure you use strong passwords – the recommendation is that these are long (at least eight characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters such as the asterisk or currency symbols.
- Do not share passwords. You should not keep passwords written down somewhere where they can be easily accessed and identified.
- Do not leave PCs with sensitive information on them in such a way that someone else could easily access that information.
- Please do not send confidential information by email. It is generally accepted that email is similar to sending an old type postcard, in that everyone can read it. If you need to send confidential information to someone there are a number of other methods that can be used, such as file transfer via OneDrive or Dropbox, password a document and then send via email or you could just use Royal Mail.
- Do not open e-mail attachments from an unknown source.
- **All electronic equipment used by members to store and/or process personal data must have suitable and up-to-date security measures/software installed, activated and in permanent operation.**
- Avoid keeping written records of negative comments about 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, group leaders should consider contacting Group Support, and committee members the Chair, for advice.
- Avoid sending emails that could be considered offensive or discriminatory.
- Avoid sharing email addresses or personal information via email without permission.
- If a laptop that holds a large amount of member information is stolen or lost, the committee should be informed immediately.
- **For security and privacy reasons, you MUST use the blind carbon copy (Bcc) feature when sending an email message to a group of people**. In addition, using the Bcc: field to conceal email addresses also acts as an anti-spam measure.
- **When sending emails to several group leaders please ensure that your email goes to group support for them to send out**, this will ensure that the email is only received by current group leaders. This also improves security and privacy and helps reduce unwanted emails being received by members who are no longer group leaders.

**Committee members and group leaders who hold information must delete or return all files and documents when relinquishing their roles.**

| **DOCUMENT CONTROL TABLE** | | | |
|---|---|---|---|
| **Document Title** | Data Protection and Privacy Policy | | |
| **Version Number** | V1F | **Status** | Final |
| **Originator's Name** | Tony Dodd | **Position** | Data Protection Officer |
| **Committee/Sub Committee** | GDPR Sub Committee | | |
| **Master Document Controller** | Linda Simms/Tony Dodd | | |
| **Date Approved** | 12 March 2019 | **Approved by** | Committee |
| **Date Effective** | 12 March 2019 | **Next Review Due** | 12 March 2020 |

| **REVISION HISTORY** | | | |
|---|---|---|---|
| **Version** | **Date** | **Author** | **Notes** |
| v0.1D | 20 September 2018 | Tony Dodd | First draft. |
| V0.2D | 24 September 2018 | Tony Dodd | Second draft, incorporating suggestions, additions and to correct a number of grammatical errors. |
| V0.3D | 25 October 2018 | Tony Dodd | Third draft, additional information included in the Introduction, Privacy Policy & Appendices. |
| V0.4D | 03 February 2019 | Tony Dodd | Fourth draft, includes the internal data processing – security assessment and revised committee member & group leaders' responsibilities. To incorporate various suggestions. |
| V1F | 12 March 2019 | Tony Dodd | Document approved by Committee |