HILLINGDON U3A DATA PROTECTION

Introduction

On 25th May 2018 a new General Data Protection regulation came into operation in addition to the Data Protection Act already enacted.
The Hillingdon University of the Third Age (HU3A) is committed to a policy of protecting the rights and privacy of members. We acknowledge the importance of keeping members' personal information safe and secure at all times. This is how we comply with the new regulation.

Transparency

Under the Data Protection Act the data held by HU3A is defined as Standard Personal Data. The level of security must be good and proportionate to the data kept by Hillingdon U3A. To carry out the work of HU3A members are asked to provide their contact details when they join.

Membership Administrator

The Membership Data is managed by the Membership Administrator who controls access to this database and provides it to members and agents where necessary. The Administrator is the only person with the authority and access to change a member's personal details.
Members must request in writing or by email to authorise changes to their Personal Data.
By supplying an e-mail address they agree to their name and e-mail address being transferred to Mailchimp for the delivery of HU3A communications.
By requesting a posted Newsletter they agree to their name and address being passed to ProntaPrint for the distribution of the Newsletter.

Physical Data Security

Backup copies of the Membership Data are taken regularly for security reasons and retained at the home of the Membership Administrator. This may involve keeping data under lock and key. A further copy is created during system closure which is uploaded to the cloud, making it available to other members and the IT team in the event of emergencies. All this data is encrypted to prevent unauthorised access should it fall into the wrong hands.

Control over Access

The committee will maintain and review the list of those Committee members who have permission to view, modify or download the information necessary to their function. Access will also be given to IT Group members who send mass emails to all members and handle distribution queries. It is HU3A policy that no third party will have access to our membership data base.

Personal email addresses will not be made available for the general public to view on our website. Committee and other functions can be contacted by members and non-members via the website at https://u3asites.org.uk/hillingdon/contact

Notification to Members

This policy is available on our website and notification of its existence was sent to all members in May 2018, and is sent to all new members. Any review of the document is notified to members in the Newsletter. If members have any objections they must be sent in writing to the secretary.

Personal Data Misuse

As stated above, the level of security must be good and proportionate to the data kept, and it will be stored in an encrypted form to protect against unauthorised access or processing, to avoid causing damage or distress to individuals. If a member feels that their data has been misused, they can complain to the Information Compliance Officer (ICO).

Table of Data Held on Each File or List

Data Item	***Main***	***Comm***	***GMR***	*MailChimp*	*Prontaprint*	***TAM***	***Website***
Membership Number	*x*	*x*	*x*	*x*	*x*		*x*
Name	*x*	*x*	*x*	*x*	*x*	*x*	*x*
Address	*x*	*x*			*x*	*x*	
Telephone Nos.	*x*	*x*					
Email Address	*x*	*x*	*x*	*x*			
Newsletter Type	*x*	*x*					
Renewal/Join Date	*x*	*x*					
Gift Aid (y or n)	*x*						
Security used							
Encrypted	*x*						
Password Controlled		*x*	*x*	*x*	*x*	*x*	*x*

What Do We Hold?

The description of data held in the Main (Membership) File is shown in column 1 and is indicated by an x in column 2. This is the main file and the source of all extracts and lists which are necessary for the management of further activities and the distribution of communication material.

The items of data held on these extracts and lists is indicated by an x in the columns in the table.

The final rows in the table show the security method used for each of these files

Who Sees What?

This section describes access rules and structures of the data files.

Committee - Approved Committee Members will receive an electronic list of all current members each month. Committee Members who have access to this list cannot copy or email personal details to anyone else.

Group Membership Register (GMR) The name, telephone number and email address of members within an Interest Group is known to the Group Leader and held in the Group Membership Register. This is necessary for Risk and Fire safety purposes and attendance recording. The contact details are required in order for the Group Leader to contact members for dissemination of relevant Group information. They must not be made available to other group members.

MailChimp - This is our 'tool' for the transmission of electronic information such as quarterly ***Newsletter, monthly Bulletin, and the occasional important message. It will be kept up to date with email addresses for each member who has provided one.***

Prontaprint - This is a file of addresses for all members who have chosen to receive a paper Newsletter. A single combined record is produced for members living at the same address.

Third Age Matters (TAM) - A file, similar in format to that for Prontaprint, is prepared and loaded directly onto the Third Age Trust system which distributes TAM. An address record is sent for ALL members, consolidated by address where necessary.

Website - A file of current members is prepared and made available to Group Leaders to check currency of membership. The file is password controlled and the password is emailed to Group Leaders and Subject Area Supervisors (SAS).

Lapsed Member Data

On leaving Hillingdon U3A a member's data will be retained for no longer than 12 months. This helps to cope more efficiently with the member re-joining within that period. The Inland Revenue insist that Gift Aid lists are retained for 7 years which is adhered to by the Treasurer.

Group Leaders

The Group Leader has a responsibility to exercise due care to provide only information that is relevant to all Group members, and to avoid promotion of direct commercial offers from third parties. Where possible, when sending an email, the sender should use the bcc facility which will conceal email addresses from the other recipients.