



Halton u3a

Data Protection & Privacy Policy



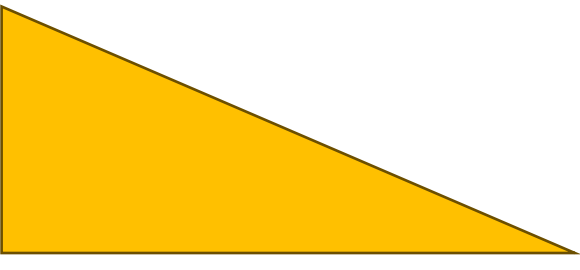
Halton u3a

Doc Hu3a 004 – Data Protection & Privacy

Version: 01

Implemented: 13.07.2026

Review Date: July 2028



Contents

1.	Introduction	2
2.	Aims	2
3.	Scope.....	2
4.	Data Principles	2
4.1	Principle 1- Lawfulness, Fairness and Transparency.....	2
4.2	Principle 2- Purpose Limitation.....	3
4.3	Principle 3 – Data Minimisation.....	4
4.4	Principle 4 – Accuracy	4
4.5	Principle 5-Storage Limitation.....	4
4.6	Principle 6- Integrity and Confidentiality (Security).....	4
4.7	Accountability- Compliance	5
5.	Subject Access Request.....	5
6.	Responsibilities	6
6.1	Trustees	6
6.2	Group Leaders	6
7.	Responding to Data Breaches	7
7.1	Action to take in the event of a data breach.....	7
8.	Definitions -Glossary of Terms	7
9.	Further Information and Training	8



1. Introduction

Data protection legislation controls how personal information is used by organisations. In the UK, data protection is governed by the UK General Data Protection Regulation (UK-GDPR), which is the European Union's (EU's) data protection law and the Data Protection Act 2018, which tailors GDPR principles to address specific UK needs and law.

Everyone who is responsible for using personal data has to follow strict rules, known as 'data protection principles' to fulfil the rights and reasonable expectations of individuals to privacy and to also ensure that personal data, e.g. information that could identify, or is related to the identity of an individual, is managed appropriately.

Halton u3a obtains, uses, stores and otherwise processes personal data relating to former, current and potential members and therefore, Halton u3a takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously.

This policy sets out how the organisation manages those responsibilities.

2. Aims

The main aim of the Halton u3a Data Protection & Privacy policy is to outline the requirements of the current data protection and privacy legislation and to advise how to manage those requirements effectively. Therefore, the policy seeks to offer appropriate guidance to:

- Ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- To provide clarity regarding responsibilities in respect to data protection
- Provide guidance on the collection, storage and management of personal data and the steps to take to in the event of a data breach
- Outline the rights of individuals with respect to data held about them

3. Scope

This Policy applies to the Trustees (The Halton u3a Committee), group leaders and others processing personal data on behalf of Halton u3a; and applies to all personal data processed on behalf of Halton u3a, regardless of the location where that personal data is stored (e.g. on a committee member's / group leader's own device).

4. Data Principles

The General Data Protection Regulation (UK GDPR) identifies 7 key data protection principles:

4.1 Principle 1- Lawfulness, Fairness and Transparency

'Personal data shall be processed lawfully, fairly and in a transparent manner, ensuring individuals understand how their data is used.'



Halton u3a requests personal information from members and potential members for membership applications, for sending communications regarding members' involvement with the u3a and for emergency health and safety requirements regarding group activities. This information includes:

- Name
- Home / email address
- Age
- Telephone number
- Emergency contact and telephone number
- Medical information required in the case of an emergency, when the member may be unconscious and unable to personally advise a medical practitioner / paramedic, for example allergies, diabetic, pace maker, blood thinning medication etc. (Please see section 4.3)
- Consent to allow an application for Gift Aid, where appropriate

Members will be informed as to why the information is being requested and what the information will be used for. The lawful basis for obtaining member information is due to the legitimate interest and contractual relationship that the u3a has with individual members.

In addition, where appropriate, members will be asked to provide consent for specific processing purposes such as the taking of photographs and the use of resulting images, for example in any promotional material, such as leaflets.

Halton u3a will ensure that members' information is managed in such a way as to not infringe an individual members' rights which include:

- 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 (enabling the data subject to obtain and reuse their data for different services.)
- The right to object

4.2 Principle 2- Purpose Limitation

'Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.'

Personal information is used by Halton u3a:

- For administration, planning and the management of Halton u3a, including communicating with members about their membership and /or renewal of their membership
- To contact members by email, telephone and post to advise them of u3a activities or communicate about specific issues that may have arisen during the course of their membership
- By group leaders to communicate with members about specific group activities
- To monitor, develop and improve provision of our u3a activities
- To apply for 'Gift Aid' and to maintain the required related records
- To facilitate delivery of the Halton u3a newsletter and other Halton u3a communications
- In order to receive the national u3a newsletter, member information will be provided to the distribution company that sends out the Trust publication – 'u3a Matters'. Therefore, members will be informed and have a choice as to whether or not they wish to receive the publication.



4.3 Principle 3 – Data Minimisation

‘The collection of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’.

The collection of personal data by Halton u3a is obtained via membership forms, both from initial registration and subsequent renewals. It is deemed that the provision of data for membership purposes, which forms a contract between Halton u3a and the member, implies that consent has been given to store such data and use it to communicate appropriately.

Members of Halton u3a will usually only be asked to provide information that is relevant for membership purposes. However, where additional information may be requested, when undertaking group activities, such as health related information and next of kin information, this 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.

4.4 Principle 4 – Accuracy

‘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, having regard to the purposes for which they are processed, is, once identified, erased or rectified without delay.’

Members will be informed to let the membership secretary know if any of their personal information changes. In addition, on an annual basis, the membership renewal process will provide an opportunity for members to inform Halton u3a as to any changes in their personal information.

4.5 Principle 5-Storage Limitation

‘Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.’

In most instances membership information will not be stored for longer than 12 months after membership ceases. However, exceptions to this include maintaining records relating to Gift Aid declarations, which in line with HMRC regulations must be kept for six years after the end of the year or accounting period that includes the last donation to which they relate, or at least 12 months after a claim is made for the last donation to which the declaration relates, if this is later. (Note: This may include gift aid claim related records relating to previous members whose membership has now lapsed and therefore must remain on the database for up to six years.)

Further exceptions include where there may be legal or insurance related circumstances that require information to be held for longer whilst these are investigated or resolved.

4.6 Principle 6- Integrity and Confidentiality (Security)

Appropriate security measures must be in place to protect personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Trustees have a responsibility to ensure that data is both securely held and processed. This will include:

- Committee members using strong passwords
- Committee members not sharing passwords
- Restricting access of sharing member information to those on the Committee who need to communicate with members on a regular basis
- Using password protection on laptops and PCs that contain personal information
- Using password protection, a membership database or secure cloud systems when sharing data between committee members and/or group conveners



- Paying for firewall security to be put onto Committee Members' laptops or other devices.

Halton u3a has a range of security safeguards in place to protect personal information against loss or theft, unauthorised access, disclosure or modification. This includes holding membership information on our password protected membership management system 'Beacon,' with access to the system by Committee members and group leaders being strongly restricted.

4.7 Accountability- Compliance

'The data controller is responsible for complying with the principles and must be able to demonstrate compliance.'

As the data controller, Halton u3a is responsible for demonstrating compliance with all the above principles, including maintaining appropriate documentation and processes.

Where consent is required for a specific purpose, then evidence of this consent (either electronic or paper) will be obtained and retained securely.

The Halton u3a Committee will ensure that:

- That new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role
- That group leaders are made aware of their responsibilities in relation to the data they hold and process
- Committee members stay up to date with guidance and practice via appropriate training
- Access rights to view personal data is reviewed on an appropriate regular basis
- 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
- If a committee member or group leader dies who holds Halton u3a data on a dedicated laptop or similar, then the next of kin should be approached to retrieve the equipment and related data as soon as possible.

5. Subject Access Request

In accordance with the GDPR, a data subject is entitled to be given a description of the types of their personal data being processed by an organisation, how the personal data was acquired, how and why it is being processed, how it will be disposed of, and if applicable, who it is shared with. (The term 'processed' in this context is very broad and includes all uses and storage means.)

Members of Halton u3a are therefore entitled to request access to the information that is held about them by Halton u3a, which should be received in the form of a written request to the Membership Secretary.

A member also has a right to see the actual data held.

On receipt of the request, the request will be formally acknowledged and dealt with expediently (the legislation requires that information should generally be provided within one month) unless there are exceptional circumstances as to why the request cannot be granted.

The processing of a Data Subject Access Request must not result in the disclosure of personal data relating to another individual. Therefore, in circumstances where personal data is mixed with other non-relevant personal data, the non-relevant personal data must be permanently redacted prior to disclosing the records.

Halton u3a will provide a written response detailing all information held on the member and a record shall be kept of the date of the request and the date of the response.



The response should include the provision of advice for the member on how to contact the Information Commissioner's Office for advice or to make a complaint, if they remain concerned about how Halton u3a is handling their personal data.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113

6. Responsibilities

As the Data Controller, Halton u3a is responsible for establishing appropriate policies and procedures in order to comply with data protection law.

6.1 Trustees

The Trustees of Halton u3a will comply with their duty under data protection legislation to:

- Keep up to date with current data protection law
- Advise group leaders of obligations under GDPR
- Provide appropriate training for group leaders
- Monitor compliance with all aspects of the 7 key principles of GDPR
- To cooperate with and act as the contact point for the Information Commissioner's Office
- Ensure that no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party

Where external companies are used to process personal data on behalf of Halton u3a, responsibility for the security and appropriate use of that data remains with the u3a. Therefore, where a third-party data processor is used, a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data.

6.2 Group Leaders

Group Leaders, should:

- Understand their responsibilities under GDPR and keep up to date with current data protection law
- Ensure that personal data that they deal with is collected, stored, processed and managed in accordance with the 7 principles of GDPR
- Ensure that any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Trustees.
- Seek clarification from the Trustees, where there is uncertainty regarding a data protection matter
- That any data breaches are reported immediately to the Trustees



7. Responding to Data Breaches

The GDPR requires that any personal data breach, that poses a risk to the rights and freedoms of the data subject, is reported to the Information Commissioner's Office (ICO).

Where the personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

7.1 Action to take in the event of a data breach

In the event of a data breach, action will be taken to minimise the harm, which includes ensuring that all Halton u3a committee members are made aware that a breach has taken place and how the breach occurred.

The Committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches.

The Chair of Halton u3a will contact National Office as soon as possible after the breach has occurred to notify of the breach. A discussion will take place between the Chair and National Office as to the seriousness of the breach, action to be taken and, where necessary, the Information Commissioner's Office would be notified.

The Committee shall also contact the relevant u3a members to inform them of the data breach and actions taken to resolve the breach.

Where a u3a member feels that there has been a breach by the u3a, a committee member will ask the member to provide an outline of the breach.

If the initial contact is by telephone, the committee member will ask the u3a member to follow this up with an email or a letter detailing their concern. The alleged breach will then be investigated by members of the committee who are not in any way implicated in the breach.

Where the committee needs support or if the breach is serious, they should notify National Office. The u3a member should also be informed that they can report their concerns to National Office if they don't feel satisfied with the response from the u3a. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome

8. Definitions-Glossary of Terms

Definitions in respect of words or phrases which are not explained in further detail within the main body of the document.

Data Controller:

The person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the GDPR. Halton u3a is the Data Controller of all personal data relating to it and used delivering education and training and leisure events and all other purposes connected with it including business purposes.



Data Subject:

A living, identified or identifiable individual about whom Halton u3a holds personal data.

Personal Data:

Any information identifying a data subject or information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers that Halton u3a possesses or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach:

Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission

Processing or Process:

Any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

9. Further Information and Training

- Additional information around Data Protection and the related responsibilities for committee members and group leaders is available on the national u3a website <https://www.u3a.org.uk/members-area/support>
- In addition Halton u3a will offer appropriate induction and training around Data Protection to Committee Members and Group Leaders.

	Doc Hu3a 004 – Data Protection & Privacy Policy		Halton u3a
Version	Description of changes	Date	
1.0	Policy ratified and adopted by Halton u3a Committee	13.07.2026	

