Data Protection Policy

1. Introduction

This is the Data Protection Policy of the Saxon Shore u3a. It should be read in tandem with the Saxon Shore u3a's Privacy Policy.

It is reviewed on a regular basis by the the Committee to ensure that the Saxon Shore u3a remains compliant.

The word ‘Committee’ in this policy refers to the Committee of the Saxon Shore u3a.

The word ‘Members’ in this policy refers to members of the Saxon Shore u3a

The word ‘Trust’ in this policy refers to The Third Age Trust.

2. Policy

2.1 Scope of the policy

This policy applies to the work of the Saxon Shore u3a for membership purposes. It sets out principles and guidance for the protection of personal data when it is collected, processed, stored and managed by the Saxon Shore u3a.

This policy applies to any and all databases, systems, portals, applications and devices on which personal data is stored or shared, and to all media types, file types and formats, both digital and hard copy.

Although not mentioned explicitly, the policy applies to all parties the u3a receives or processes personal data for. For example, emergency contacts.

2.2 Why this policy exists

The work of the Saxon Shore u3a must comply with UK data protection legislation and regulations, including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy gives direction on the application of data protection legislation and regulations. It aims to ensure that the Saxon Shore u3a:

- complies with data protection law and regulations and follows good practice
- protects the rights of members.
- is open about how it collects, processes, stores and manages personal data
- protects itself from the risks of a data breach.
- has the guidance to implement appropriate and effective data protection operational measures.

2.3 General guidelines for Committee members and Group Facilitators

- The only people able to access personal data covered by this policy should be those who need to communicate with or provide a service to members.
- Saxon Shore u3a will provide induction training to Committee members and Group Facilitators to help them understand their responsibilities when handling data.
- Committee members and Group Facilitators should keep all data secure by taking sensible precautions (at home and in public) and following the guidelines in this policy and in Trust guidance materials.
- Strong passwords must be used and should never be shared.
- Personal data should not be shared outside of the u3a unless with prior consent and/or for specific and agreed reasons.
- Member data should be kept up-to-date and accurate.
- Additional support is available from the Trust where uncertainties or incidents regarding data protection arise.

2.4 Data protection principles

The General Data Protection Regulation identifies key data protection principles:

- Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner;
- Principle 2 - Personal data must 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;
- Principle 3 - 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;
- 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 are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Principle 5 - 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. 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 organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- Principle 6 - 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.

2.5 Lawful, fair and transparent data processing

- The Saxon Shore u3a requests personal data from potential members and members for membership applications, for sending communications and other reasons regarding the planning and operational management of the u3a.
- Members will be told why personal data is being requested and what it will be used for.
- The lawful bases for obtaining member information are legitimate interests, contract and consent. Please refer to our Privacy Policy for further details.
- In addition, members will be asked to provide consent for specific processing purposes. Members will be informed who they need to contact should they wish to withdraw their consent. Such requests will be acted upon promptly and the member will be informed when the action has been taken.
- More detail can be found in Saxon Shore u3a's Privacy Policy.

2.6 Processed for specified, explicit and legitimate purposes

Members will be informed how their personal data will be used and the Committee will seek to ensure that personal data is not used inappropriately.

Appropriate use of personal data provided by members includes:

- Communicating with members about Saxon Shore u3a events and activities.
- Group Facilitators communicating with their group members about specific group activities.
- Providing personal data to the distribution company that sends out the Trust publication – *u3a Matters*. Members will have a choice as to whether or not they wish to receive the publication.
- Providing members with information about Trust events and activities
- Communicating with members about their membership and/or renewal of their membership.
- Communicating with members about specific issues that may have arisen during the course of their membership.
- Using emergency contact details in the event of an emergency.
- Enabling the u3a's efficient operation, financial management and development.

Saxon Shore u3a will ensure that Group Facilitators are made aware of what would be considered appropriate and inappropriate use of personal data. Inappropriate use of personal data includes:

- Sending members marketing and/or promotional materials from external service providers.
- Sharing personal data outside of the u3a unless with prior consent and/or for specific and agreed reasons.

Saxon Shore u3a will ensure that personal data is managed in such a way as to not infringe an individual member's 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
- The right to object

2.7 Adequate, Relevant and Limited Data Processing

Members will only be asked to provide personal data that is relevant for membership purposes. This will include:

- Name
- Postal address
- Email address
- Telephone numbers
- Emergency contact details (optional)

Where additional personal data may be required such as health related data (where relevant) or to investigate a complaint, this will be obtained with the consent of the member who will be informed why this data is required and the purpose for which it will be used.

Saxon Shore u3a has completed a legitimate interest assessment for the collection and use of emergency contact details. This assessment will be kept under review and will be refreshed if there is a significant change in how or why emergency contact data will be used. Members will be made aware that the assessment has been refreshed.

2.8 Photographs

- Photographs in which individuals are recognisable are classified as personal data.
- Where group photographs are being taken, members will be asked to step out of shot if they do not wish to be in the photograph. Otherwise consent will be obtained from members in order for photographs to be taken and members will be informed as to where photographs will be displayed.
- Should a member wish at any time to rescind their consent and to have their photograph removed then they should contact the Committee to advise that they no longer wish their photograph to be displayed.

2.9 Accuracy of data and keeping data up-to-date

- Saxon Shore u3a has a responsibility to ensure that personal data is accurate and kept up-to-date.
- Members should be regularly reminded to inform the Membership Secretary of any changes. This could be done via the membership renewal process, as part of other communications or when this policy is changed.

2.10 Accountability and governance

- The Committee is responsible for ensuring that the Saxon Shore u3a remains compliant with data protection law, regulations and good practice and can evidence that it does.
- All Committee members have joint responsibility for data protection.

- Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely.
- The Committee will ensure that new members joining the Committee are provided with induction training to data protection requirements and legislation to help them understand their responsibilities when handling data.
- Saxon Shore u3a will also ensure that Group Facilitators and other persons approved by the Committee are made aware of their responsibilities in relation to the personal data they hold and process.
- Committee members will stay up to date with guidance and practice within the u3a movement and in Trust guidance materials, and will seek advice from the National Office should any uncertainties arise. Detailed guidance on all aspects of data protection is also available from the Information Commissioner's Office (ico.org.uk).
- The Committee will review data protection requirements and compliance 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 Facilitators relinquish their roles, they will be asked to either pass on data to those who need it and/or delete or otherwise dispose of data securely. Such data could be held both digitally and on hard copy.

2.11 Secure Processing

Committee members and Group Facilitators have a responsibility to ensure that data is both securely held and processed by taking sensible precautions and following the guidelines in this policy. This will include:

- Using the Trust's Beacon membership management system to securely process and store personal data.
- Restricting access to personal data to those on the Committee, Group Facilitators and persons approved by the Committee, each with access at an appropriate level for their role or the reason why they were granted access.
- Using strong password protection on laptops, tablets, PCs and other devices that contain personal data and not sharing passwords.
- Using password protection, the Beacon system or secure applications, portals or systems when sharing data between Committee members and/or Group Facilitators.
- Any person with access to personal data must ensure that they have installed, and keep up-to-date, recognised firewall security and virus protection software on all devices used to access personal data.
- Deleting personal data when it is no longer required for its original purpose, in line with the Committee's data retention policy. This applies wherever and however that data is stored. Hard copy documents must be securely shredded.
- Where appropriate, using encryption or password protection when sharing data externally. For example, when sending sensitive data via email.
- Ensuring members' permission is obtained for sharing relevant contact details where a Committee or interest group matter is discussed via email or messaging application (e.g. WhatsApp).

2.12 Subject Access Request

- Members are entitled to obtain a copy of their personal data that is held by Saxon Shore u3a.
- The request needs to be made in writing to the Membership Secretary of Saxon Shore u3a. On receipt, 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.
- With support from the National Office, Saxon Shore u3a will provide a written response detailing all personal data held on the member.
- A record will be kept of the request and the response.

2.13 Data Breach Notification

- Were a data breach to occur, action will be taken to minimise the harm. This will include ensuring that all Committee members are made aware that a breach has taken place and how the breach occurred.
- The Committee will seek to rectify the cause of the breach as soon as possible to prevent any further breaches.
- The Chair of Saxon Shore u3a will contact the National Office of the breach as soon as possible after it occurs. 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 will also contact the relevant members to inform them of the data breach and actions taken to resolve the breach.
- Where a member feels that there has been a breach by the u3a, a Committee member will ask them to provide an outline of the breach. If the initial contact is by telephone, the Committee member will ask for 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.
- The member should also be informed that they can report their concerns to the National Office if they are not satisfied with the response from the u3a.
- Breach matters will be subject to a full investigation, records will be kept and all those involved will be notified of the outcome.

3. Changes to our Data Protection Policy

This Data Protection Policy is available on our website. This policy may change from time to time. Members will be informed via the newsletter and the monthly meetings when any material changes are made to Saxon Shore u3a's policies and procedures.

4. Adoption and Review

This policy was adopted on: 18th May 2026
Policy review date: 18th May 2027 (or earlier, should a need arise, e.g. a change in legislation, regulations or technology)