Privacy Policy

Original Policy by **Mark Shear**
Drafted by **Bindesh Majithia**

Updated
February 2026

The United Synagogue

Contents

Data Controller 2
Registered office 2
Contact 2
Scope 2
Legal Framework 2
Associated Policies 2
Data Collected 2
Use of Personal Data (purposes and legal bases) 3
Core Activities 3
Communications and Marketing 4
Legitimate Interests (when used) 4
Special-category data (e.g. religion, health) 4
Sharing Data (recipients and categories) 4
International Transfer of Data 4
Data Retention 5
Data Subject Rights 5
Exercising Your Rights As a Data Subject 5
Providing Personal Data 5
Cookies And Similar Technologies (PECR) 5
Children's Data 6
Security 6
Links to Other Websites 6
Review and Changes to Policy 6

US Privacy Policy

Data Controller

The data controller is **The United Synagogue** ("US"), a registered charity in England & Wales (Charity No**. 242552)**.

Registered office

305 Ballards Lane, North Finchley, London N12 8GB.

Contact

Data Protection Officer (DPO): Bindesh Majithia
Email: dpo@theus.org.uk
Address: DPO, The United Synagogue, 305 Ballards Lane, London N12 8GB
ICO: ico.org.uk

Scope

This policy sets out how we use and handle personal data when you interact with our websites and digital services, apply for or hold membership, participate in events and programmes (including youth/education), donate, volunteer, use our sites/facilities, or otherwise engage with us. It is drafted to meet the transparency requirements of Articles 12–14 UK GDPR and reflects updates arising from the Data Use and Access Act 2025 (DUAA) and PECR.

Legal Framework

Our approach is compliant with all prevailing UK legislation and guidelines, including, UK GDPR, Data Protection Act 2018, Data Use and Access Act 2025, and the Privacy and Electronic Communications Regulations 2003 (PECR).

Associated Policies

This policy, together with the Confidentiality Policy, Data Protection Policy, and Data Retention Policy, detail the Charity's comprehensive approach in this area.

Data Collected

We may process identity/contact details, membership and lifecycle data, education/youth data, event bookings, donations and Gift Aid, volunteer/safeguarding data, CCTV/visitor logs, technical website data, and correspondence.

Depending on the interaction, we may process:

- **Identity and contact** (e.g., name, addresses, emails, phone numbers).
- **Household/membership** information and lifecycle details relevant to our religious/communal services.
- **Education/youth** participation data (including parental contacts and, where necessary, medical/dietary info for trip safety).
- **Event bookings and payments** (including transaction identifiers via payment providers).
- **Donations and Gift Aid** records.

- **Volunteer and safeguarding** data (e.g., references, DBS where roles require).
- **Site security** data such as visitor logs and **CCTV** images.
- **Technical/usage** data from our websites and apps (including cookies/analytics—see Cookies section).
- **Correspondence and feedback** (e.g., enquiries, surveys, complaints, subject access requests).

We may also receive data from other sources (e.g., DBS services, referees, third party platforms you use to engage with us, or from public sources). Where we receive data from sources other than you, we provide the information required by UK GDPR Article 14 unless an exemption applies.

Use of Personal Data (purposes and legal bases)

UK law requires us to explain each **purpose** and the **lawful basis** we rely on; the ICO expects a clear link between purposes and bases. Where we process **special-category data** (e.g., data revealing religious beliefs or health data), we also identify an **Article 9** condition (and where needed, a **DPA 2018 Schedule 1** condition).

Core Activities

Purpose	Examples of data	Lawful basis (UK GDPR Art. 6)	Special category / DPA 2018 condition (if applicable)
Membership administration & community support	Identity, contact, household, lifecycle	**Contract** (providing membership services); **Legitimate interests** (running our charity and communicating with members)	**Art. 9(2)(d)** not-for-profit with religious aim (appropriate safeguards)
Religious lifecycle services	Identity, lifecycle, family	**Contract**; **Legal obligation** (record-keeping); **Legitimate interests**	**Art. 9(2)(d)**; **Art. 9(2)(f)** legal claims where relevant
Education & youth programmes (incl.	Participant details, emergency contacts; medical/dietary where necessary	**Contract**; **Legitimate interests**; **Vital interests** (emergency)	**Art. 9(2)(a) consent** for optional medical/dietary; **Art. 9(2)(c)** vital interests; **Sch.1 DPA** safeguarding where relevant
Events & ticketing	Booking details, payments	**Contract**	—
Donor relations & Gift Aid	Donation details, Gift Aid	**Legitimate interests** (stewardship); **Legal obligation** (HMRC)	—
Volunteer management & safeguarding	Identity, references, DBS	**Legitimate interests**; **Legal obligation**	**Sch.1 DPA** safeguarding; **Art. 9(2)(g)** substantial

Communications and Marketing

- **Service communications** (e.g., membership updates; event info for bookings you made): **Contract** / **Legitimate interests**.
- **Newsletters, community updates, and fundraising appeals:** We rely on **consent** or (where permitted) **legitimate interests** with an opt-out, in line with **PECR** rules for electronic marketing. You can opt out at any time.

Legitimate Interests (when used)

We use **legitimate interests** to operate a UK charity safely and effectively, for example, stewarding relationships, ensuring physical and information security, and internal reporting, while balancing those interests against your rights in a documented assessment. You can object to processing based on legitimate interests.

Special-category data (e.g. religion, health)

We only process special-category data where an **Article 9** condition applies (for us, commonly **Art. 9(2)(d)** not-for-profit with a religious aim, **vital interests**, **legal claims**, or **substantial public interest** for safeguarding). Where **DPA 2018 Schedule 1** applies, we maintain an **Appropriate Policy Document**.

Sharing Data (recipients and categories)

We share personal data only, when necessary, under contract and confidentiality, with:

- **IT, hosting, and cloud service providers** (e.g., productivity suites, CRMs, forms, web platforms)
- **Payment processors and banks**; **mailing/SMS providers** and print houses.
- **Insurers, auditors, professional advisers**, and regulators.
- **Partner communal bodies** involved in programmes you choose.
- **Local authorities, police, courts** where legally required.

International Transfer of Data

Some suppliers may process data **outside the UK**. Where this happens, we use one of:

- a **UK adequacy regulation** (including the UK-US "data bridge" where applicable); or
- the **ICO's International Data Transfer Agreement (IDTA)** or **UK Addendum** to the EU SCCs, plus a **Transfer Risk Assessment (TRA)**.

We follow the ICO's updated (2026) guidance using a **three-step test** to determine whether a restricted transfer occurs and apply appropriate safeguards and roles/responsibilities accordingly.

We use UK adequacy regulations or IDTA/UK Addendum with Transfer Risk Assessments under ICO's 2026 guidance.

Data Retention

We keep personal data **only for as long as necessary** for each purpose, then delete or anonymise in line with our retention schedule. For example:

- **Membership records**: see Data Retention Policy
- **Donations & Gift Aid**: see Data Retention Policy
- **Event bookings**: see Data Retention Policy
- **Safeguarding/incident data**: as required by law or guidance.
- **CCTV**: typically, **up to 30 days** unless needed longer for an investigation.

We will state a fixed period where possible; where not, we state the **criteria** used. We regularly review and document our schedule as part of accountability under UK GDPR (and DUAA's emphasis on transparent retention practices). This

Data Subject Rights

You have the rights to **access**, **rectification**, **erasure**, **restriction**, **objection**, and **data portability** (for data you provided to us, processed by automated means under consent or contract). Where we rely on **consent**, you can **withdraw consent at any time**, without affecting processing already carried out. For **direct marketing**, you can opt out at any time.

These rights are set out in detail within our Data Protection Policy.

Exercising Your Rights as a Data Subject

Contact **dpo@theus.org.uk**. We will respond to all requests within statutory timeframes and may request proof of identity to safeguard individual privacy and data.

Providing Personal Data

We will tell you when providing personal data is **statutory or contractual**, or **necessary to enter into a contract** (e.g., membership, event registration). If you do not provide required information, we may be unable to provide the relevant service.

Cookies And Similar Technologies (PECR)

Our websites use **cookies** and similar technologies. We use **essential** cookies to make the site work and, where required, ask for your **consent** for **non-essential** cookies (e.g., analytics/advertising). You can change your preferences at any time via our cookie banner/preferences centre.

DUAA 2025 changes to PECR: DUAA increased potential fines under PECR (aligning them with UK GDPR) and introduced limited relaxations for certain **non-essential cookies used for performance or service improvement**, which in some cases **may not require consent**. We will continue to obtain consent for analytics/marketing cookies unless an exemption clearly applies and will keep our banner and policy under review as ICO updates guidance.

Children's Data

Where we process children's data (e.g., education/youth programmes), we present information in plain language, obtain appropriate **consents** where required, and take particular care with **medical/dietary** and safeguarding information. Our notices and consent mechanisms follow ICO expectations for clarity and fairness for children.

Security

We apply technical and organisational measures appropriate to the risks (e.g., access controls, encryption in transit where applicable, staff training, due diligence on processors, incident handling).

Links to Other Websites

Our websites may link to other sites. We are not responsible for their content or privacy practices. You should review their privacy notices.

Review and Changes to Policy

This policy will be reviewed every two years to ensure it remains appropriate, valid, and compliant with current laws and best practices.

We may update this document to reflect changes in our processing or in the law (including **DUAA** developments and **ICO guidance**). We will post updates here and, where appropriate, notify you via email or on-site banners.