Data Protection Policy

Original Policy by **Bindesh Majithia**

Updated
June 2026

The United Synagogue

Contents

US Data Protection Policy

Introduction

The United Synagogue (the Charity) processes personal data relating to members, employees, volunteers, and other individuals in the course of its activities. The Charity is committed to handling personal data lawfully, fairly, securely, and transparently, in accordance with applicable UK data protection legislation and good practice.

Purpose and Objectives

The purpose of this policy is to set out the Charity's approach to the lawful, fair, and secure processing of personal data and to provide a framework for compliance with UK data protection legislation across the organisation.

- To define the principles and standards that apply to the processing of personal data across the Charity.
- To clarify the responsibilities of employees, volunteers and others who handle personal data on the Charity's behalf.
- To support the protection, confidentiality, integrity, and appropriate retention of personal data.
- To promote compliance with data protection requirements and good practice throughout the organisation.

Scope

This policy applies to all employees, volunteers, office holders, committee members, and trustees, and to any other individuals who process personal data on behalf of the Charity. It applies to personal data held in any format, including electronic records, paper files, emails, images, and other recorded information.

Legal Framework

This policy is informed by the following legislation and regulatory guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications 2003 (PECR)
- Data (Use and Access) Act 2025
- Guidance and statutory codes issued by the Information Commissioner's Office (ICO)

Associated Policies

This policy should be read alongside the following related policies and procedures:

- Data Retention Policy
- Confidentiality Policy
- WhatsApp for Business Use Policy
- Information Security Policy
- Remote Working Policy

Data Protection Principles

The Charity will process personal data in accordance with the UK GDPR principles and reflect them in its day-to-day practices and procedures.

1. Personal data will be processed lawfully, fairly, and transparently.
2. Personal data will be collected for specified, explicit and legitimate purposes and not Processed incompatibly with those purposes.
3. Personal data will be adequate, relevant, and limited to what is necessary.
4. Personal data will be accurate and, where necessary, kept up to date.
5. Personal data will be kept no longer than necessary.
6. Personal data will be processed securely using appropriate technical and organisational measures.
7. The Charity will be responsible for, and able to demonstrate, compliance with these principles.

Our Commitment

The Charity is committed to protecting personal data and maintaining appropriate standards of confidentiality, integrity, and security. It will process personal data lawfully, transparently and in accordance with legal requirements.

The Charity will communicate clearly about the use of personal data and take appropriate organisational and technical measures to support compliance across the organisation.

Data Protection Processes

To support compliance, the Charity will:

- Maintain appropriate organisational and technical measures to protect personal data.
- Ensure appropriate controls, governance, and oversight of processing.
- Put in place written arrangements with third parties processing personal data on the Charity's behalf.
- Limit access to personal data to those who need it for authorised purposes.
- Require personal data to be handled only through approved Charity systems and processes.
- Provide appropriate guidance, training, and awareness to those handling personal data on the Charity's behalf.

Accountability and Governance

The Charity is responsible for, and must be able to demonstrate, compliance with UK data protection legislation. It will maintain appropriate governance, policies, records, and oversight to support and evidence compliance.

- Maintain records of processing and supporting documentation where required.
- Keep relevant policies, procedures, and contracts under review.
- Ensure compliance responsibilities are clearly allocated and supervised.
- Involve the Data Protection Officer where appropriate.
- Review and update data protection measures as activities, risks, systems, and legal obligations change.

Special Category and Criminal Offence Data

Where the Charity processes special category or criminal offence data, it will identify and document the lawful basis and any additional condition required by law, and apply safeguards appropriate to the sensitivity of the data and the risks to individuals.

This may include enhanced access, confidentiality and retention controls, staff guidance and training, and any additional documentation required under the Data Protection Act 2018, including an appropriate policy document where applicable.

Privacy by Design and Data Protection Impact Assessments

The Charity will apply data protection by design and by default when introducing, reviewing, or changing activities involving personal data. Privacy considerations must be addressed at the earliest practicable stage and throughout the activity lifecycle.

The Charity will carry out a Data Protection Impact Assessment where processing is likely to result in a high risk to individuals' rights and freedoms, and keep such assessments under review where appropriate. The Data Protection Officer will be consulted in accordance with the Charity's internal arrangements.

International Transfers

The Charity will only make a restricted transfer of personal data outside the United Kingdom, where permitted by law, and subject to an appropriate transfer mechanism, such as adequacy regulations, appropriate safeguards, or a lawful exception.

Where required, the Charity will assess the transfer and keep relevant safeguards under review.

Direct Marketing and PECR

Where the Charity carries out direct marketing by email, text, or other electronic communication, it will do so in accordance with UK data protection legislation and the Privacy and Electronic Communications Regulations 2003. The Charity will use consent, soft opt-in, or another lawful route only where the legal requirements are met.

The Charity will provide clear marketing choices, respect opt-outs and objections, and maintain appropriate suppression arrangements where an individual has asked not to receive further marketing communications.

Data Sharing

The Charity may share personal data where necessary, proportionate, and lawful for its activities or obligations. Any sharing will be carried out in accordance with UK data protection legislation, the Charity's privacy information and, where relevant, applicable data sharing or processing arrangements.
Where the Charity shares personal data, it will provide appropriate information about:

- The identity of the Charity and, where relevant, the parties with whom data is shared.
- The purpose for which personal data is shared.
- The lawful basis and, where applicable, any additional condition relied on for the sharing.

The Charity will ensure that appropriate written agreements or other contractual measures are in place, where personal data is shared or processed by third parties on its behalf, and keep them under review. Decisions to share personal data must be justifiable, documented where appropriate, and consistent with the Charity's legal and regulatory obligations. Where the Charity determines the purposes and means of processing, it acts as controller and retains overall responsibility for the protection of the personal data concerned.

Exemptions

In limited circumstances, the Charity may rely on an exemption from particular data protection rights or obligations where permitted by the Data Protection Act 2018 and applicable law. Any reliance on an exemption will be considered case by case, justified and documented where appropriate, and applied only as far as necessary. This may include disclosures or restrictions for the prevention or detection of crime, the apprehension or prosecution of offenders, or compliance with a legal obligation.

Data Retention

Personal data will be retained only as long as necessary for the purpose for which it was processed, in accordance with the Charity's retention schedule, legal obligations and operational requirements. This applies to data held in electronic and paper records.

Individuals may, in certain circumstances, have the right to request erasure of their personal data. This right is not absolute and may apply where:

- The personal data is no longer necessary for the purpose for which it was collected or processed.
- The individual withdraws consent and there is no other lawful basis for processing.
- The individual objects to processing and there are no overriding lawful grounds to continue.
- The personal data has been processed unlawfully.
- Erasure is required to comply with a legal obligation.

Where appropriate, the Charity may retain limited information on a suppression list to record that an individual has asked not to be contacted or that certain processing should stop.

The Charity's Data Retention Policy and retention schedule set out retention periods, rationale, and disposal arrangements for the main categories of personal data it holds.

Disposal of Data

When personal data or confidential information is no longer required and the retention period has expired, it must be disposed of securely in accordance with the Charity's retention schedule and approved procedures.

- Paper records containing personal data must be shredded, confidentially destroyed, or otherwise securely disposed of, to prevent reconstruction or unauthorised access.
- Electronic records must be permanently deleted or destroyed using appropriate technical measures so that the information cannot be recovered, unless restricted storage is still required for lawful or technical reasons.
- Devices, storage media and hard copy records awaiting disposal, must be kept securely and access restricted, until destruction takes place.

- Where disposal is carried out by a third party, the Charity will take appropriate steps to ensure the service is secure and confidential.

Individual Rights

Individuals may have rights in relation to their personal data, including rights to be informed, access, rectification, erasure, restriction, objection and, where applicable, data portability and rights relating to automated decision-making. The Charity will recognise and respond to those rights in accordance with applicable law and its internal procedures.

Right of Access to Personal Data: Subject Access Requests (SARs)

Individuals have the right to obtain confirmation as to whether the Charity processes their personal data and, where it does, to receive a copy of that data together with the information required by law. Subject Access Requests should be directed to the Data Protection Officer at dpo@theus.org.uk.

Requests may be made in writing or verbally and do not need to use a particular form. The Charity may ask for information needed to confirm the requester's identity, clarify the request where reasonably necessary, or confirm authority where a request is made on behalf of another individual.

- The Charity will normally respond without undue delay and within one month of receiving the request and any information reasonably required to process it.
- Where clarification is reasonably required to identify the information requested, the Charity may seek it before completing its response.
- Searches carried out in response to a request will be reasonable and proportionate.
- there is normally no fee for making a subject access request.
- The Charity may refuse to act on a request, or charge a reasonable fee, only where the request is manifestly unfounded or excessive, in accordance with applicable law.

Where a request is made by a third party, the Charity will require evidence that the third party is authorised to act on the individual's behalf, unless another lawful basis for disclosure applies.

Complaints

Individuals may raise a data protection complaint with the Charity if they consider that their personal data has been handled in breach of data protection law. The Charity will facilitate and handle complaints in accordance with legal requirements and internal procedures.

The Charity will acknowledge complaints within the applicable period, investigate and respond without undue delay, and inform the complainant of the outcome. Individuals will also be informed of their right to complain to the Information Commissioner's Office.

Data Breaches

A personal data breach is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Charity will take appropriate steps to identify, contain, assess, investigate, document, and respond to suspected and actual breaches in accordance with law and internal procedures.

In the event of a suspected or confirmed personal data breach, the Charity will:

- Report incidents internally without delay and escalate them for assessment.
- Take appropriate steps to contain the breach, mitigate harm, and investigate the circumstances.
- Keep an internal record of the breach, including the facts, effects and remedial action taken.
- Notify the Information Commissioner's Office without undue delay and, where required, within 72 hours of becoming aware of the breach.
- Inform affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.
- Review the incident and take steps to reduce the risk of recurrence.

Employees, volunteers, and others acting on the Charity's behalf must report suspected personal data breaches promptly, and comply with the Charity's breach management procedures. Failure to do so may be addressed under disciplinary or other appropriate internal procedures.

Where a breach involves a third-party processing personal data on the Charity's behalf, the Charity will take appropriate contractual and operational steps in accordance with the relevant agreement and applicable law.

Review

This policy will be reviewed every two years, or sooner if required, to ensure it remains current, effective, and compliant with law and good practice.