WEST LONDON SYNAGOGUE OF BRITISH JEWS

ק"ק שער ציון

UPPER BERKELEY STREET

A CONSTITUENT OF THE MOVEMENT FOR REFORM JUDAISM

Privacy Policy

General Data Protection Regulations (GDPR)

PRIVACY POLICY - General Data Protection Regulations (GDPR)

Policy
Everyone has rights with regards to the way in which their personal data is handled. During the course of our activities we collect, store and process personal data about our membership, friends and other contacts, suppliers and other third parties, as well as our employees and other workers, and we recognise that the correct and lawful treatment of this data will maintain confidence in our organisation and will assist us to achieve success in our business operations.

Employees and other individuals who handle personal data within our organisation are obliged to comply with this policy when processing personal data on our behalf**.**

About this policy
Personal data which is held on a computer or other electronic device, and in some cases in paper files, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the "DPA") and other regulations. As from 25th May 2018 the DPA will be replaced by the EU General Data Protection Regulation ("GDPR"), supplemented by UK legislation currently going through Parliament ("New DPA"). These laws are together referred to in this policy document as the "Data Protection Legislation".

The Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

This policy sets out the basis on which we process any personal data that we collect from data subjects or other sources outside of our organisation.
(For the ways in which we process personal data about our own employees and other workers, there is a separate policy for Internal use: "Processing Employee Data")

This policy does not form part of any employee's contract of employment and may be amended at any time. Nevertheless, any breach of this policy may result in disciplinary action, as well as possible personal liability.

This policy has been approved by The WLS Executive Director, Stewart Sether. It sets out rules on data protection and the legal conditions that must be satisfied when we collect, handle, process, store and transfer personal data.

Should you have any queries, issues, concerns or problems however in relation to this Privacy Policy please contact either of our Data Protection Co-Ordinators:
Ros Clapham: ros.clapham@wls.org.uk, tel: 0207 535 0266 (tues & thurs)
Adi Ben-Naim: adi.ben-naim@wls.org.uk, tel: 0207 535 0275 (mon-fri)

Please contact Stewart Sether (Executive Director), the WLS Data Protection Lead should you have any concerns that Data Protection Legislation or this Privacy Policy or is not being complied with:
email: stewart.sether@wls.org.uk
tel: 0207 535 0268

Definition of data protection terms
Data is information which is stored electronically, on a computer or other device, or in certain paper-based filing systems.

Data subjects include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified, directly or indirectly, from that data (or from that data and other information in our possession), in particular by reference to an identifier such as a name, an identification number, location data or an online identifier. Personal data can be factual (for example, a name, address, email address or date of birth or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person) or it can be an opinion about that person, their actions and behaviour.

Data Controllers are the people who or organisations which determine the purposes and means of processing personal data. They are responsible for establishing practices and policies in line with the Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes other than (for example) where we process data in the context of providing services to a third party who is the data controller, in which case we will be a data processor.

Data Users are those of our employees or other workers whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data Processors include any person or organisation (other than a data user) that processes personal data on our behalf and on our instructions. Data processors will include suppliers that handle personal data on our behalf.

Data Processing is any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or destruction of the data.

Sensitive Personal Data (referred to under the GDPR as "special categories of personal data") includes information revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as data concerning a person's health or sex life or sexual orientation. Sensitive personal data can only be processed with the explicit consent of the person concerned. Under the DPA, sensitive personal data also includes information about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Under the GDPR and the New DPA, similar conditions apply to processing of personal data about criminal convictions and offences or related security measures.
Third country means a country outside the European Union (or the EEA).

Data Protection Principles
Data controllers are responsible for ensuring and demonstrating that data processing is performed in accordance with the requirements of the Data Protection Legislation ("Data Protection Principles").
These provide that personal data must be:

- processed fairly and lawfully and in a transparent manner (see Fair & Lawful Processing below)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;

- kept in a form which permits identification of data subjects for no longer than necessary for the purpose;
- 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.

In addition, personal data must not be:

- transferred to people or organisations situated in countries without adequate protection for personal data.

When processing personal data as the data controller in the course of our business, we will ensure that those requirements are met, and all Data Users must therefore take account of the contents of this policy document.

Fair and lawful processing

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation.

These include, among other things, where:

- the data subject has given consent to the processing,
- or the processing is necessary for the performance of a contract with the data subject,
- or the processing is necessary for the compliance with a legal obligation to which the data controller is subject
- or the processing is necessary for the legitimate interests of the data controller or a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data).

When Sensitive Personal Data (see page 4) is being processed (including personal data about criminal convictions etc), additional conditions must also be met.

Data Subject's Consent

It is important to note that when this is relied on as a lawful basis for processing, the consent has to be:

- freely given
- specific
- informed
- unambiguous
- consent requires some form of clear affirmative action
- silence, pre-ticked boxes or inactivity does not constitute consent
- if the data subject's consent is given in a context which also concerns other matters, the request for consent must be presented so it is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language
- consent must be verifiable
- individuals have a right to withdraw their consent at any time, as easily as they gave it.

Personal Data we may collect and process

In the course of our business, we may collect and process Personal Data, a sample of which is set out in the attached Schedule.

This may include:

- data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise)
- data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only:

- process personal data of the types and for the specific purposes set out in the attached Schedule
- or for any other purposes specifically permitted by the Data Protection Legislation.

We will also ensure that:

- our processing is based on the lawful basis set out by the Data Protection Legislation
- is not retained for longer than the period set out there
- personal data is not transferred to third parties other than those specified in the Schedule.

Notifying Data Subjects

1. **If we collect personal data directly from data subjects, we must inform them of:**
    - our identity and contact details
    - the purpose or purposes for which we intend to process that personal data, as well as our legal basis for doing so
    - where we are processing the personal data on the basis of legitimate interests, what those interests are
    - the third parties, or categories of third parties, if any, with which we will share or to which we will disclose that personal data
    - if we intend to transfer the personal data to a Third Country, the adequacy (or otherwise) of the data protection laws there, and safeguards to be used to protect the personal data (and how the data subject can access these safeguards).

2. **In addition, the following information must also be provided at the time of collection, where this is necessary in order to ensure fair and transparent processing:**
    - the period for which the personal data will be stored, or how that period will be calculated
    - the individual's right of right of access to, and rectification or erasure of the data
    - where processing is based on the individual's consent, their right to withdraw consent for processing their data
    - the individual's right to lodge a complaint with a supervisory authority
    - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract (and the possible consequences of failure to provide the data)
    - where applicable, the existence of automated decision-making
    - any further processing of the data that is intended for any other purpose.

If we receive personal data about a data subject from other sources, we must provide the data subject with the information at 1. and 2. above (as soon as possible and at the latest within one month) together with:

- the categories of personal data concerned
- the source from which the personal data originated, and if applicable, whether it came from publicly accessible sources.

The information provision requirements at 1. and 2. above will not apply where the data subject already has the information, or the provision of such information proves impossible or would involve a disproportionate effort, in which case we must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Rights of Data Subjects

Data subjects have certain enforceable rights under the Data Protection Legislation, including

- the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed
- and, if so, access to the personal data, plus a copy of the personal data undergoing processing
- information on their personal data as to:
    - the purposes of the processing
    - the categories of personal data concerned
    - the recipients or categories of recipient of the data
    - the envisaged period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period
    - where the personal data are not collected from the data subject, any available information as to their source
    - where personal data are transferred to a third country, the safeguards relating to the transfer

In addition, the data subject has the following rights:

- the right of rectification: to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her and (taking into account the purposes of the processing)
- the right to have incomplete personal data completed
- the right of erasure: to obtain from the controller the erasure of personal data concerning him or her without undue delay, where:
    - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
    - the processing is based on the data subject's consent, and the data subject withdraws consent (and there is no other legal basis for processing)
    - the processing is based on it being necessary for the legitimate interests of the data controller or a third party, and the data subject objects to the processing, unless the controller demonstrates that the processing is based on compelling legitimate grounds which override the interests, rights and freedoms of the data subject, or is for the establishment, exercise or defence of legal claims
    - the processing is for the purpose of direct marketing, and the data subject objects to the processing (including profiling)
- the right of restriction: to obtain from the controller restriction of processing where the data is inaccurate, unlawfully processed, no longer required except for the establishment, exercise or defence of legal claims, or pending the verification whether the legitimate grounds of the controller override those of the data subject
- the right of portability: to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and to transmit the data to another controller, where the processing is based on consent or carried out by automated means
- the right to object: to object to processing based on the controller's legitimate interests, where these are outweighed by the interests, rights and freedoms of the data subject, unless the processing is required for the establishment, exercise or defence of legal claims
- the right not to be subject to a decision based solely on automated processing, including profiling

Manner of processing

In order to ensure that we comply with the Data Protection Legislation, we need to implement appropriate technical and organisational measures to ensure and to be able to demonstrate compliance, and to maintain a record of our processing activities.

The practical implications of this include ensuring that:

- we only collect personal data to the extent that it is required for the specific purpose notified to the data subject
- we check the accuracy of any personal data at the point of collection and at regular intervals afterwards, and take all reasonable steps to destroy or amend inaccurate or out-of-date data

- we do not keep personal data longer than is necessary for the purpose or purposes for which they were collected, and take all reasonable steps to destroy, or erase from our systems, all data which is no longer required
- we process all personal data in line with data subjects' rights.

In addition we will:

- adopt appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement the data protection principles, including data minimization
- implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed ("protection by design and by default")
- where processing (in particular, when using new technologies) is likely to result in a high risk to the rights and freedoms of individuals, carry out an impact assessment of the data processing implications prior to the processing and, where necessary, consult the supervisory authority (the Information Commissioner's Office)

- Where processing is to be carried out on our behalf by a data processor we must ensure that:
    - the processor provides sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of the Data Protection Legislation and ensures the protection of the rights of the data subjects
    - the processing is governed by a written contract that sets out (amongst other things) the:
        - subject-matter and duration of the processing
        - the nature and purpose of the processing
        - the type of personal data and categories of data subjects
        - the obligations and rights of our organisation as data controller.

Data security

We will take appropriate security measures against unauthorised or unlawful processing of personal data, and against the accidental loss of, destruction or damage to, personal data, using appropriate technical or organisational measures.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality:

- Means that only people who are authorised to use the data can access i
- When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:
    - We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
    - We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.
    - ***Employees must not allow themselves to be bullied into disclosing personal information.*** For assistance in difficult situations employees will refer the request to their own Departmental Manager (or in their absence, Stewart Sether, the Executive Director)

Integrity: means that personal data should be accurate and suitable for the purpose for which it is processed

Availability: means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the company's central computer system instead of individual PCs.

Security: The following measures will be adhered to:

- **Entry controls:** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal:** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- **Equipment:** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

- **Passwords:** These must not be shared or disclosed to anyone else
- **Encryption:** This should be used wherever it is available and appropriate
- **Back-ups.** Regular back-ups must be taken of the information on the computer system and kept in a separate place, so that if you lose your computers, you don't lose the information.

Dealing with Subject Access requests
Data subjects may make a formal request for information we hold about them, this request must be made in writing. Any employees or workers who receive a written request will immediately forward it to Stewart Sether, the Executive Director. (Under the GDPR, we must usually provide information pursuant to a subject access request free of charge and within one month of the request)

ANY ACTUAL OR SUSPECTED BREACH OF DATA SECURITY, OR THIS POLICY, MUST BE REPORTED IMMEDIATELY to:
Stewart Sether, the Executive Director: stewart.sether@wls.org.uk
Data breaches will be handled in line with our Data Breach Policy.

(Data subjects also have the right to lodge a complaint with the supervisory authority, which is the Information Commissioners Office: www.ico.org.uk, tel:0303 123 1113)

Transferring personal data to a country outside the EEA
We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The data subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms (this includes countries in respect of which a finding of adequacy has been made, and also transfers to entities in the USA that participate in the US-EU Privacy Shield)
- The transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights. This may include what are known as "binding corporate rules", or where standard data protection clauses in an approved form have been adopted
- Subject to the requirements in clause above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Disclosure and sharing of personal information
We may:

- share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006, where this is necessary for certain reasons, or we have legitimate interest in doing so which are not outweighed by the interests, rights and freedoms of the data subject.
- disclose personal data we hold to third parties, on the basis of our legitimate interests in the event that:
    - we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets
    - we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets
    - we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply

any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

Changes to this policy
We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email

Please read the following Schedule, of our Data Processing Activities, listed by department.

Schedule of Data Processing Activities - West London Synagogue (by department)

IT AND HEALTH & SAFETY DEPT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Staff/Volunteers	**User IT Profiles**	User set-up System Access (restricted rights only limited to need to perform job function) User deletion	To enable Data Subject IT profile set-up and restricted system access.	The data subject has given consent to the processing and the processing is necessary for the legitimate interests of the data controller and necessary for the performance of a contract with the data subject	Internal: to IT Manager External: to Optima IT	For the duration of the Data Subjects required IT access
Staff	**Names & telephone numbers of staff**	Staff contact in the event of an Emergency or Disaster Recovery situation	To enable staff to be contacted in an emergency situation by WLS. (by the IT Mgr/Exec. Director/ Security Co-ordinator)	The data subject has given consent to the processing and the processing is necessary for the legitimate interests of the data controller (employment & associated duty of care) and is necessary for the performance of an employment contract with the data subject	Internal: IT Manager	For the duration of the Data Subjects employment
	Telephone numbers only of staff				External: Txtlocal Ltd. (the company WLS use to quickly send text messages to staff in the event of an emergency/disaster recovery situation) that we need to communicate with all members of staff quickly staff mobile numbers only, not names)	

Non-Members, Members & Staff/Volunteers	**Accident Log Detail** **Name, address, nature of Accident**	Information is filed in ring binders and stored in a locked filing cabinet in office. Softcopies stored on the secured WLS Network	For internal use and to keep records of first aid & accident log	the data subject has given consent to the processing and and the processing is necessary for the compliance with a legal obligation to which the data controller is subject	Internal only (unless access requested by external party such as the HSE during an H&S inspection visit)	6 years
	CCTV Signs are up advising that CCTV is in use	Live video feed for monitoring and recording of visitors to the building	For security purposes	the processing is necessary for the legitimate interests of the data controller & on occasion may be necessary for the compliance with a legal obligation to which the data controller is subject	Internal: Security Staff & IT Manager External: CST	After 30 days

HUMAN RESOURCES DEPT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Employees/ Workers/Volunteers	Name Address Telephone number Date of Birth Personal email address, work email address, Salary Benefits Bank details National insurance number Passport, visa, nationality Medical disclosure Student loan information, court deductions, Pension Gender Vehicle registration number Childcare vouchers, Employment references Disciplinary/capability records, Employee correspondence References	Information held on personnel files and payroll spreadsheets (electronic) and in archive boxes and paper personnel files for use in payroll and employee management.	Storage of historic and current personal and employment documentation of employees, paper copies of current employment documentation	This processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of employees in the field of their employment. It is necessary for the performance of a contract to which the data subject is party.	Internal: Within HR & selected details provided to the Finance Director in a password protected file (Sum instruction, Bank Details & Name) to enable payments of Earnings/Expenses. External: Outsourced payroll HMRC, relevant detail only to Organisations dealing with Childcare Vouchers, Student Loans & Disclosure Barring Service checking, Insurance companies relevant to employee insurance, Employment Lawyers for Employment Law advice, Auditors for Accounts & HR Home Office	For 6 years or if longer, for the duration of the Working/Volunteering relationship
	Employment/education history	Used for assessment decision of the Data Subjects' suitability to perform a WLS role DBS Check for child &/or vulnerable adult contact. Certificates/details held in locked paper and password protected personnel files and		The processing is necessary for the purposes of performing or exercising obligations or rights of WLS as the employer	(Dept Line Mgrs receive Employment/Education history purely to enable their effective participation in the WLS recruitment process)	
	Special Categories of Personal Data: Disclosure Barring check (to which the Data Subject has given consent to process) & disclosure result of any criminal conviction		Storage of historic and current personal and employment documentation of employees,	The processing is necessary for the purposes of performing or exercising obligations or	Internal: within HR & & DBS outcome update (but not conviction details) provided to the relevant employing Manager within WLS.	3 years

		employee/DBS status spreadsheets on WLS network	paper copies of current employment documentation.	rights of WLS as the employer or the data subject under employment law, and the law relating to social protection and WLS has an appropriate policy in place.		
FINANCE DEPARTMENT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Members (Adults, Religion school students, Child members Major donors)	Name Address Telephone number Date of Birth Gender Next of Kin information Personal email address, work email address. Bank details, copy of cheques, forms with credit/ debit card details only for payment processing of Membership Fees payments & donation requests from the Data Subject including High Holy Days Appeal forms received.	Information is held on Enterprise MRM data base system. Cheques received & Credit Card Details used to enable payment collection – via Epay for Direct Debit processing & SAGE PAY for Credit Card processing Excel reports are prepared solely for Reconciliation purposes & stored on the secured WLS network, until is reconciled, then deleted. Use of bank statements for the reconciliation (6 years storage)	The processing is essential to keep records of our members in order to communicate with them, to process payments, and donations via various methods.	The processing is necessary to enable the type of relationship /service that the data subject requires & has contracted to with WLS by completing the Membership form and by supplying WLS with their personal/banking details	Internal: Within the finance, membership and credit control departments. External: Bank Processing via E-PAY for Direct Debit & SAGE PAY for Credit Card processing	6 years

		Storage of historic and current documentation inc bank statements, cheques & Credit Cards processed. (After the payment is processed the Credit card form is altered so as not to show full details & hence prevent re-use) Hard copies can be found in the locked file cabinet in the Accounts office and in the locked small storage room near Accounts dept				
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Non-Members (Adults & Major donors)	Name Address Telephone number Date of Birth Gender Next of Kin information Personal email address, work email address. Bank details, copy of cheques, forms with credit/ debit card details only for payment processing of ticket sales for events or donation requests from the Data Subject including High Holy Days Appeal forms received.	As above	As above	The processing is necessary to enable the type of relationship /service that the data subject requires and has consented to, by supplying WLS with their personal details for a specific purpose	Internal: Within the finance, membership and credit control departments. External: Bank Processing via E-PAY for Direct Debit & SAGE PAY for Credit Card processing	6 years
Employees	Salaries via Payroll: Name Address Telephone number Date of Birth NI Number Gender	Information held via payroll spreadsheets held on the secured WLS network in a password protected folder & payslip/benefits invoice documentation in order	Review monthly salaries for sign-off purposes via spreadsheets and payslips	This processing is necessary for the purposes of carrying out the obligations and	Internal-shared between HR and Finance External: Banking details shared with External Payroll to	Payroll information is retained indefinitely

	Personal email address, work email address. Bank details	to review & give sign off to approve payment of monthly salaries. (Payroll storage as above is controlled & retained by the HR dept)		exercising the specific rights of employees in the field of their employment with WLS. It is necessary for the performance of a contract to which the data subject is party	enable that company to pay salaries via BACS	
	Reimbursement of Expenses	Expenses Forms storage is controlled by Finance – paper copies of forms & BACS records are in locked file cabinet in the Accounts office.	Employees submit their expenses forms together with all receipts. Then this is processed by BACS payment, the bank details are taken from the payroll password protected excel sheet (but not stored in Finance) Or a Petty Cash payment made if less than £30.00		BACS payment processed via Barclays Online Banking	6 years

MEMBERSHIP DEPARTMENT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Members (Adults, Religion school students, Child members Major donors)	Name Address Telephone number Date of Birth Gender Next of Kin information Personal email address, work email address (Under certain circumstances usually when hardship reduction is requested: Medical disclosure, Financial situation) Correspondence, payments record, Jewish documentation	Information is held on Enterprise MRM data base system. Reports can be sent to excel sheets which at time are sent forward to the rabbis or other members of staff. Storage of historic and current documentation. Hardcopies are storted in the locked Membership Filing cabinet.	The processing is essential to keep records of our members in order to communicate with them, bill them, arrange for pastoral support if needed, advertise events and activities, promote ways in which members can donate and also to keep a records as to their Jewish life and important rites of passage.	The processing has been consented to by the Data Subject & is necessary for fulfilment of the Membership contract with WLS by completing the Membership form or by supplying WLS with their personal details in exchange for provision of a service the Data Subject has requested from WLS	Internal – within the different department in the synagogue (see details by dept)	For the duration of the Membership
<u>Non-Members</u> (Resigned, Deceased, Suspended, & Major donors)	Name Address Telephone number Date of Birth Gender Next of Kin information Personal email address, work email address (Under certain circumstances usually when hardship reduction is requested: Medical disclosure, Financial situation) Correspondence, payments record, Jewish documentation	Information is held on Enterprise MRM data base system.	Storage of historic and current documentation	The processing has been consented to by the Data Subject via the provision of the data. Necessary for the legitimate interests of the data controller: it enables WLS chase unpaid fees or sell tickets etc… Also in maintaining our	Internal: Accessed & used by relevant departments in the synagogue (as specified by department, elsewhere within this Privacy Policy) External: On occasion we receive requests from relatives of deceased members for information (date of death, dates of membership). In these	Indefinite (unless the Data Subject requests erasure from the WLS database)

				historic Jewish records so as to be able to provide on request from the Data Subject themselves, or to their family Jewish documentation. Being able to provide this type of service is valued within the Jewish community	cases, we asked for an identification and provided the information that was needed.	
MARKETING, IT & COMMUNICATIONS DEPARTMENT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Members & Friends (Anyone paying a membership/friend fee)	Names email addresses	Once a Member or Friend provides their details, it is added to a membership record in the Enterprise Database System. Their email address is added to MailChimp (an online marketing automation platform and an email marketing service)	To send weekly emails containing: - Links to various items on our website, ie Haftarah Sheet, Live Broadcast - Rabbis TFTW - Weekly Calendar information - Upcoming events - Link to MRJ & BoD & issue of any one-off announcements, such as: - Community announcements - Board notices - AGM Notices	The data subject has given consent to the processing & it's also in fulfilment of the Data Subject's provision of service as a paid for Membership of WLS	External – MailChimp (an online marketing automation platform and an email marketing service)	Ongoing – Unless data subject ceases Membership or unsubscribes from receiving emails from WLS

	Names Home Addresses	A list of all members who wish to receive the Newsletter. Consent provided if they wish to receive this by email. The list is generated from Enterprise and exported to labels, put on envelopes and mailed out to the congregation. The labelled envelopes are stored securely at reception or in the office until such a time that they are put in the post.	To send quarterly postal Newsletters	The data subject has given consent to the processing & it's also in fulfilment of the Data Subject's provision of service as a paid for Membership of WLS	Internal – labels and envelopes are handled by specific WLS staff, and securely retained for up to a week then collected by Royal mail for delivery.	Ongoing – Unless data subject ceases Membership or unsubscribes from receiving communications from WLS
SECURITY DEPARTMENT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Employees	**Name & date of attendance at WLS**	Information is held securely at reception before being given to HR	Record keeping of physical Attendance at Work	Necessary for the legitimate interests of the data controller as the employer in maintaining attendance records and for the purposes of carrying out the obligations and exercising the specific rights of employees in the field of their employment with WLS.	Internal: Handed over to HR (on a monthly basis)	1 year
Visitors (not employees)	**Visitors Name, Their Company Name (if applicable), Arrival & Departure Time, Name of Person they are visiting**	The data subject provides this information by writing in the Vistors Book	Record of physical entry & exit to/from the premises	The data subject has given consent to the processing by by "signing in" and	Used & retained only within Security Dept (unless WLS as the Data Controller was subject to a legal	1 Month

		which is held at reception		the processing is necessary for the purposes of carrying out the security obligations of WLS to keep both staff & Visitors safe (legal duty of care)	obligation to share the information with the Police, due to a criminal matter)	
FACILTIES DEPARTMENT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Members Events	**Name, Address** **Email & telephone number**	Information is held in the Enterprise Database and transferred into an Excel Spreadsheet which is held on the secured WLS network in a password protected folder	To process lists of names only for 1)Events which includes the names of guests only mainly for admission and security purposes To enable access by the Data Subject into the WLS event 2) Table plans 3) Attendees List with Contact Details	The Data Subject has consented by confirming that they wish to attend or hold the event Arranging events for Members is necessary for the legitimate interests of the data controller in fulfilling a provision of service possible for Members, by being a paid for WLS Membership	Internal Use Only: Names are listed only 1)For issue to the Security Team at WLS 2) are displayed on Table Plans for use by Guests at the event 3) Used by the Events Co-Ordinator only for the purpose of the Event	1) & 2) lists are destroyed once the event is over The Events Co-ordinator deletes Events Details & Lists after 12 months
	Name, telephone number & Credit Card Payment Information	Some WLS events carry a charge above the basic Membership Fee and using the Members event requirement instruction and contact details, the events co-ordinator contacts the data subject by 'phone	The Events co-ordinator needs to process a payment for the event The one-off payment is processed and receipted via the	The data subject has given consent to processing and its in the legitimate interests of the Data Controller to be paid in exchange for the	The WLS Enterprise system interfaces with SAGE PAY for Credit Card processing	No credit card details are stored anywhere.

		to obtain their Credit Card.	WLS Enterprise system.	supply of the event.		
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Non-Members Events	**Name, Address and sometimes email and telephone number**	Information is obtained from the Data Subject and input into the Enterprise Database (as a Non-Member) and transferred into an Excel Spreadsheet which is held on the secured WLS network in a password protected folder	To process lists for 1)Events which includes the names of guests only mainly for admission and security purposes, to enable access by the Data Subject into the WLS event 2) Table plans.	The Data Subject has consented by confirming that they wish to attend or hold the event & by providing their details for inclusion in the WLS Database as a Non-Member.	Internal only for table plans and security. Guests will see the list as I have to put up a table plan but this is destroyed once the event is over. Security will also see the list – but again this is destroyed after the event.	Ongoing storage in a secure database, unless the data subject asks to be removed
	Name, telephone number & Credit Card Payment Information	Some WLS events carry a charge and using the data subjects event requirement instruction their contact details, the events co-ordinator contacts the data subject by 'phone to obtain their Credit Card detail.	The Events co-ordinator needs to process a payment The one-off payment is processed and receipted via the WLS Enterprise system.	The data subject has given consent to processing and its in the legitimate interests of the Data Controller to be paid in exchange for the supply of the event.	The WLS Enterprise system interfaces with SAGE PAY for Credit Card processing	No credit card details are stored anywhere.
Venue Bookings (Members and Non-Members)	**Terms and Conditions including name, address, email addresses are stored in these contracts**	Hard copies are kept for reference purposes in a ring binder which is stored in a locked cabinet in my office.	Confirmation of what the event consists of & when its going to take place and	The processing is necessary for the performance of a contract with the data subject. It also is legally	Internal and external – client receives a copy of the contract	Ongoing

		Also held on the secured WLS network	copies retained since 2011	binding document which protects both the client and WLS.		
SOCIAL ACTION DEPARTMENT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Volunteers (Members)	Name Email phone	Held on synagogue database (cross refer Membership Dept)	To invite volunteers to participate in the project, seeking volunteers being in the legitimate interests of WLS as the Data Controller	Each volunteer has given written consent on their Membership Form or subsequent written consent to the Social Action Dept for their data to be used for the purpose of contacting them for volunteering	None	Until they ask to be removed from the Volunteer list
Volunteers (Non-Members)	Name Email Phone Home Address	Held on synagogue database		Each volunteer gives written consent to be added to the database for the purpose of contact for volunteering	None	
Volunteers (Feeding Folk, ESOL, Employment support)	Name Email Phone number	Held on a spreadsheet on WLS server		Each volunteer has consented to join the mailing list and by provision of their details. Each email sent contains the option for them to be removed	None	For length of the project (unless they ask to be removed from volunteer list for a project)
Interfaith Mailing List	Name Organisation Phone number Email Events attended	Held on a spreadsheet on WLS server	To invite people to interfaith events being in the legitimate interests of WLS		None	Until they ask to be removed from the mailing list

			as the Data Controller	from the mailing list if they wish		
Volunteers (Grenfell Kids Day Camp)	Name Age Phone Email Answers to questions from questionnaire assessing skills to volunteer with us	Held on a spreadsheet on WLS server	To manage volunteers for the project – including volunteers who registered interest but were unable to make the project itself	Each person has consented by completing the form to register themselves as a Volunteer participate in the project	None	For the length of the project (unless they ask to be removed from volunteer list
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Asylum Seeker Drop-In – Guests Registration	Name Phone number Nationality Children's names Children's ages	Held on a spreadsheet on WLS server	To manage the Drop-In through the identification of eligible guests when they arrive at the project. Project requires family to have children under the age of sixteen	Each family voluntarily attends the Drop-In, and is consenting to the processing of their Data by completing a 'new guest' form to enable their participation	Once a Letter of Authority is signed by the Data Subject, their eligibility status is shared with new North London Synagogue and Liberal Jewish Synagogue	6 months
Asylum Seeker Drop-In - Social Work	Name Personal medical information Personal family circumstances	Held on paper in files in the office of the Head of Social Action	To manage the ongoing support of clients	The Data Subject is consenting to the processing of their Data by providing their information voluntarily, and seeing it written down in front of them	None	For as long as they remain clients of the Drop-In (unless they ask for them to be removed)

RABBINIC (updated May 2018 - awaiting confirmation for 2019)						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Employees	Name Personal email address, work email address, Medical disclosure Disciplinary/capability records, Employee correspondence References	Information held in electronic files and spreadsheets and locked paper files (at Synagogue and in secure storage in rabbis' homes), on Synagogue email server, drives, personal email servers and personal and mobile phones.	Storage of historic and current personal and employment documentation of employees, paper copies of current employment documentation	This processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of employees in the field of their employment. It is necessary for the performance of a contract to which the data subject is party.	Internal: Shared within HR	6 years
Members	Name Address Telephone number Date of Birth Gender Family information Personal email address, work email address, Medical disclosure Personal History, Financial situation/Court Records/Notes, Correspondence, meeting & contact/assessment	Information held in WLS database on secure network and electronic files and spreadsheets and locked paper files (at Synagogue and in secure storage in rabbis' homes), on Synagogue email server, drives, personal email servers and computers and personal and mobile	This processing is necessary for the purposes of carrying out the Rabbi's & Ritual Co-ordination obligations by the Synagogue to its Community and for the fulfillment of the Rabbi's & ritualistic	The processing is necessary to enable the type of relationship that the data subject requires & has contracted to with WLS by completing the Membership form or by supplying WLS with their personal details in exchange for	Internal: Shared with other departments and volunteers where relevant. This may include with Wardens for allocation of honours in services and to commemorate the anniversary of a funeral. External: Support Organisations relevant	Ongoing storage within secured Membership Database

	Photographs on phones and computers	phones. Rabbi's day-books (Notebooks for recording day to day information) Legitimate Duty of Care Safeguarding Referrals to Local Authority, Police or other organization: where Safety of Client or another person is at risk	obligations to represent the synagogue in public life. Including, pastoral care, home visits, lifecycle events (baby blessings, bar mitzvah's weddings, conversions, funerals), teaching, service arrangements, social action activities, synagogues administrative meetings, public engagements.	provision of a service the Data Subject has requested from WLS	to particular needs only with consent from data subject. Eg. Funeral Directors & Cemetaries Local Authority, Police or other professional organization that needs to be referred to where the Safety of the member or another person is at risk	
Marriage Secretaries & Assistants of WLS, Westminster & New London Synagogue	Name Home Address	Provide information by letter of any changes to the Marriage Secretaries and Assistants of all Reform Synagogues in the UK, also Westminster Synagogue and New London Synagogue (hence WLS are supplied with their personal details)	To seek agreement for the appointment or deletion of the individual registration & to specify if the appointee will perform a) opposite sex marriages or b) both opposite and same sex marriages	This processing is necessary and required by the Data Subject so as to enable them to undertake the function within their Synagogue. WLS are carrying out the legitimate obligations of the Synagogue to its Community & other synagogues.	Internal: Records held at WLS External: Information shared with & approval sought from the General Register Office	

SOCIAL CARE DEPARTMENT (updated May 2018 - awaiting confirmation for 2019)						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Social Care Clients (WLS Members and Non-Members)	Client Disclosed: Name Address Telephone number Date of Birth Gender Next of Kin information Personal email address, work email address, Social Benefits Details National insurance number Passport, visa, nationality Medical disclosure Personal History, Financial situation/Court Records/Notes, Correspondence, meeting & contact/assessment records	Information held in secure electronic files and spreadsheets and locked paper files for use in Supporting Social Care Clients via Social Care activities undertaken by the Social Care Team and Social Care Volunteers (and WLS Rabbi's)	Storage of historic and current Social Care Client documentation, for the purposes of carrying out the Social Care obligations of the Synagogue to its Community.	This processing is necessary for the purposes of carrying out the legitimate Social Care obligations of the Synagogue to its Community.	Internal: Shared with Social Care Team & Social Care Event Volunteers (and WLS Rabbi's)	For the duration of data subjects life
	Where Data Subject Consented to a referral being made by WLS to an external Support Organisation: Client disclosed detail as above & correspondence, contact, what is contact meeting/assessment & records shared between Social Care Contacts in both organisations.	WLS Social Care team referrals to other any other Support Organisations: eg. Jewish Care etc	This processing is necessary for the purposes of carrying out the Social Care obligations of the Synagogue to its Community.	This processing is necessary for the purposes of carrying out the legitimate Social Care obligations of the Synagogue to its Community.	Internal: As Above External: Support Organisations relevant to the Social Care Clients particular needs: eg. Jewish Care	

	Personal Details as above, History, Financial situation, Notes, Correspondence, meeting & contact/assessment records	Legitimate Duty of Care Safeguarding Referrals may be made to Local Authority, Police or other organization: where Safety of Client or another person is at risk. WLS has an appropriate policy in place.Correspondence, contact, meeting/assessment & records shared & held by Social Care Contacts in both organisations	The processing is necessary for the purposes of performing or exercising legal obligations	The processing is necessary for the purposes of performing or exercising legal obligations of WLS under Safeguarding guidance and a duty of care (Children & Vulnerable Adults) or the law relating to social protection	Internal: As Above External: Local Authority, Police or other professional organization that needs to be referred to where the Safety of the Social Care Client or another person is at risk	For the duration of the "live status" of the Safeguarding matter
Social Care Clients (WLS Members & Non-Members Attendees at Events held at WLS)	Attendee Disclosed: Name Address Telephone number Date of Birth Gender	Information held in secure electronic files and spreadsheets and locked paper files for use in Supporting Social Care Clients via Social Care activities undertaken by the Social Care Team and Social Care Event Volunteers	This processing is necessary for the purposes of carrying out the Social Care obligations of the Synagogue to its Community. Eg. Contact Details for pick up for attendance at events & detail necessary to ensure safe care whilst at event & in case medical attention &/or family emergency contact needed.	Data subject provided and consented details with processing is necessary for the purposes of carrying out the Social Care obligations of the Synagogue to the Membership & wider Jewish Community in a safe manner	Internal: Shared with Social Care Team & Social Care Event Volunteers	Only as long as the individual keeps attending events at WLS
	Next of kin contact details Disclosed Medical Information				External: Only in the event emergency - to Paramedic	
	Photos of Attendees at WLS Social Events	With data subject consent: Publication in Community Magazine/Newsletter	To encourage other attendees to Social Care events	Data subject consented with processing necessary for the purposes of carrying out the	Internal: Shared with Social Care Team & Social Care Event Volunteers	

				Social Care obligations of the Synagogue to the Membership & wider Jewish Community	External: Community Magazine/Newsletter. A list of publications is available on request	
EDUCATION DEPARTMENT						
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Education Dept Volunteers	Special Categories of Personal Data: CRB check information, criminal conviction disclosure. The Data Subject provides their personal data to enable a DBS Check to be undertaken.	Information held on personnel files of Volunteers and on DBS status spreadsheets (password protected) stored on secure network and in paper personnel files for use in volunteer management. WLS has an appropriate policy in place.	Storage of historic and current documentation of volunteers	Necessary for the purposes of performing or exercising obligations or rights of WLS as the managing organization responsible for the data subject, under employment or the law relating to social protection	Internal – within Education Dept & on occasion HR. External: DBS checking organization	3 years
Education Dept Clients (WLS Members - Adult & under 18)	Client or parent of child Disclosed: Name Address Telephone number Date of Birth Gender Next of Kin information Personal email address, work email address,	Information held in secure electronic files and spreadsheets and locked paper files for use in Supporting Educational Dept Clients via Educational activities undertaken by the Education Team	Storage of historic and current Educational Client documentation.	the data subject has given consent to the processing and it is necessary for the legitimate interests of the data controller in carrying out the	Internal: Shared with Educational Team & Educational Volunteers (and on occasion where pastoral or additional	For the duration of being an Education Dept client

	Passport, visa, nationality Medical disclosure Dietry requirements This is often collected by the Parent completing the detail in Google Forms. Personal Details as above, History, Financial situation, Notes, Correspondence, meeting & contact/assessment records	and Education Volunteers (and on occasion WLS Rabbi's) Legitimate Duty of Care Safeguarding Referrals may be made to Local Authority, Police or other organization: where Safety of Client or another person is at risk. WLS has an appropriate policy in place. Correspondence, contact, meeting/assessment & records shared between & held by Educational Contacts in both organisations)	This processing is necessary for the purposes of carrying out the Legal and Educational obligations of the Synagogue to its Community.	Educational obligations of the Synagogue to its Community. The processing is necessary for the purposes of performing or exercising legal obligations of the Organisation under Safeguarding Law (Children & Vulnerable Adults) or the law relating to social protection	support is needed WLS Rabbi's and the WLS Social Care Department) Local Authority, Police or other professional organization that needs to be referred to where the Safety of the Education Dept Client or another person is at risk	For the duration of the Safeguarding matter
Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Education Dept Clients (WLS Members & Non-Members attending events held at WLS - Adult & under 18's)	Attendee or Parent Disclosed: Name Address Telephone number Date of Birth Gender Next of kin contact details Disclosed Medical Information Dietry requirements and allergies	Information held in secure electronic files and spreadsheets and locked paper files for use in Supporting Education Dept Clients via Educational activities undertaken by the Education Team and Education Volunteers	Use of Contact Details for promotion of attendance at events & on trips detail necessary to ensure safe care whilst at event & in case medical attention &/or family emergency contact needed.	the data subject has given consent to the processing and it is necessary for the purposes of carrying out the Educational obligations of the Synagogue to the Membership & wider Jewish Community in a safe manner	Internal: Shared with Education Team & Education Volunteers External: Only in the event of emergency – eg. to Paramedic or other medical staff	Only as long as the individual is a Member of WLS, or in case of a non-member, whilst that person or parents child keeps attending to events at WLS
	Photos of Attendees at WLS Educational Events	With data subject consent:	To promote the fun to be had at Educational	the data subject has given consent to the	Internal: Shared with Education	Only as long as the individual is a Member of WLS, or in case of a

		Publication in Community Magazine/Newsletter	events & to encourage new attendees	processing and it is necessary for the legitimate purposes of WLS to carry out the Educational obligations to the Membership & wider Jewish Community	Team & Education Volunteers External: With data Subject Consent: Community Magazine/Newsletter A full list of third parties is available on request	non-member, whilst that person or parents child keeps attending to events at WLS