



Data Protection — UK GDPR Policy

Sir Joseph Isherwood Limited is fully committed to prepare for and to comply with the UK General Data Protection Regulation (UK GDPR). The UK GDPR applies to all organisations that process data relating to their employees, as well as to others including customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed.

To this end, Sir Joseph Isherwood Limited endorses fully and adheres to the six principles of data protection, as set out in the UK GDPR.

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Data must 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.
5. 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 is processed.
6. 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.

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, Sir Joseph Isherwood Limited will:

- Observe fully the conditions regarding the fair collection and use of information including the giving of consent.
- Meet its legal obligations to specify the purposes for which information is used.

- Collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Ensure that the information is held for no longer than is necessary.
- Ensure that the rights of people about whom information is held can be fully exercised under the UK GDPR (ie the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect).
- Take appropriate technical and organisational security measures to safeguard personal information.
- Publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection.
- Ensure that personal information is not transferred abroad without suitable safeguards.

Status of this Policy

This Policy was initially approved on 23rd May 2018. It was subsequently reviewed on 16th May 2019 and 13th May 2020 and no changes were deemed necessary.

It was reviewed on 3rd February 2021 to take into account the impact of Brexit. Under the Brexit agreement the GDPR has been incorporated into UK data protection law as the UK GDPR. As such all references to GDPR have been changed to UK GDPR. It was subsequently reviewed on 7th February 2022, 3rd February 2023, 2nd February 2024, 9th September 2025 and 6th February 2026 and no changes were deemed necessary.

The policy was reviewed on 3rd June 2026 and a new section was included to set out the procedures if you consider that we have breached data protection laws because of the way we have handled your personal data (or the personal data of someone you are acting on behalf of).

This policy will be reviewed again no later than 28th February 2027.

Designated Data Controllers and Data Protection Officers

The designated Data Protection Officer (DPO) (Stephen Thompson) will deal with day-to-day matters. Any member of staff, or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the DPO.

Staff Responsibilities & Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Personal information must be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it must be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Disaster Recovery

1. Sir Joseph Isherwood Limited backs up data every day and has multiple copies (at least one set for each day of the week and additional weekly ones in order to have at least a month's worth of data at any one time). Records of these are kept.
2. Backups are kept in multiple physical locations, including a fire-proof safe.
3. Backups are verified regularly.
4. Firewalls and virus checkers are kept up to date and running, and users are regularly advised of the latest virus avoidance and detection techniques.
5. Computers are protected from physical harm, theft or damage.
6. Sir Joseph Isherwood Limited plans for how to deal with loss of electricity, external data links, server failure, and network problems.

Subject Consent

The UK GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the UK GDPR, Sir Joseph Isherwood Limited takes a "granular" approach i.e., it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, Sir Joseph Isherwood Limited ensures that people can easily withdraw consent (and tells them how this can be done).

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others may include the following.

- Contract: if processing someone's personal data is necessary to fulfil Sir Joseph Isherwood Limited's contractual obligations to them (eg to provide a quote).
- Legal obligation: if processing personal data is necessary to comply with a common law or statutory obligation.

- Vital interests: this refers to processing personal data to protect someone's life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent).
- Legitimate interests: the most flexible lawful basis for processing and one which applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Note that the UK GDPR provides for special protection for children's personal data and Sir Joseph Isherwood Limited will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

Subject Access

Any person may request details of personal information which Sir Joseph Isherwood Limited holds about him or her under the UK GDPR. A small fee may be payable and will be based on the administrative cost of providing the information. If an employee would like a copy of the information held on him or her, they should write to The Data Protection Officer, Sir Joseph Isherwood Limited, Centre for Advanced Industry, Coble Dene, Royal Quays, North Shields, Tyne & Wear, NE29 6DE, United Kingdom (email: data.protection@isherwoods.com). The requested information will be provided within one month. If there is any reason for delay, that will be communicated within the four week time period. A request which is manifestly unfounded or excessive may be refused. The person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).

If any person believes that any information held on him or her is incorrect or incomplete, then they should write to or email the Data Protection Officer as soon as possible, at the above address. Sir Joseph Isherwood Limited will promptly correct any information found to be incorrect.

Data Protection Complaints Policy

Introduction

The Data Protection Act 2018 is the main law governing data protection. You have the right to complain directly to us if you consider that we have breached data protection laws because of the way we have handled your personal data (or the personal data of someone you are acting on behalf of). This section explains your right to complain and how we will handle your complaint.

Roles and Responsibilities

Our Data Protection Officer (DPO) is responsible for handling data protection complaints within our organisation. They will work alongside other members of our organisation who have been identified as relevant to the investigation of each complaint.

All staff are responsible for recognising data protection complaints.

Staff who receive or identify a data protection complaint, whether in person, via social media or through any other channels, must inform the DPO as soon as possible.

We are committed to handling data protection complaints in line with our legal obligations and in an accessible, fair, transparent and timely manner. We will handle complaints confidentially and only share information where appropriate to investigate and resolve the complaint, as required or authorised by law or otherwise in accordance with our privacy notices.

Types of Complaint

Examples of a data protection complaint include (but are not limited to) the following:

- the way we have responded to a subject access request (SAR), or other data rights request (for more information on individual data rights, see the Data Protection Policy)
- the security measures we have used to store your information (eg where you have been impacted by a data breach)
- how we have collected or used your personal information (eg where we have stored it, how long we have kept it for, or its accuracy).

This list is not exhaustive. You have the right to complain to us at any time if you consider that there has been an infringement of any of your rights in relation to your personal data. Information on how we handle your personal data is set out in our separate privacy notice.

Complaints about other matters that do not relate to data protection, such as customer service issues, will not be treated as a data protection complaint.

If we are not sure whether you are making a data protection complaint, we will contact you to clarify the nature of your complaint.

Employees who want to raise a grievance should do so under our grievance procedure.

If your complaint relates to whistleblowing, please read our separate whistleblowing procedure.

How to Make a Data Protection Complaint to Us

You can submit a complaint directly by emailing data.protection@isherwoods.com.

We will take appropriate steps to respond to data protection complaints that we receive from any channels, including via social media.

We will comply with our duty to make reasonable adjustments to our data protection complaints process for disabled people under the Equality Act 2010. If you feel that you would benefit from any adjustments to our data protection complaints process, you should raise this with us when making your complaint.

Complaints Made on Social Media

Although data protection complaints may be made on social media, we would advise that a complaint may be dealt with more efficiently and effectively if it is made using one of the methods set out above.

Where we identify a data protection complaint about our organisation on social media, we will take appropriate steps to respond to the complaint in line with this policy. However, as responding on social media is not usually a secure way of providing information, we will ask the individual making the complaint for an alternative contact method that we can use to respond to their complaint.

Complaints from children

We will respond to data protection complaints from children in plain, clear language they can understand at all stages of the complaints process. We will comply with our obligations to assess the competence of the child to understand and exercise their rights.

Responding to Your Complaint

When we receive a data protection complaint, we will acknowledge receipt no later than 30 days from receiving it.

If we have any doubts about your identity, we may need to ask you for proof of ID before we respond to your complaint.

Complaints made on your behalf by a third party must be accompanied by evidence that the third party is authorised to act on your behalf. If this is not provided, we will contact the third party to ask that such evidence is provided before we respond to your complaint. If we are unsure whether a letter of authority is valid, we will contact you about this before we respond to your complaint.

We will take appropriate steps to respond to your complaint without undue delay, including making enquiries into the complaint and keeping you informed about the progress of our investigation and timescales for the next update or outcome.

We may need to contact you to request further information to assist with our investigation. It may take us longer to investigate and resolve complaints which are complex, serious or which relate to multiple data protection issues.

Following our investigation, we will inform you of the outcome of your complaint without undue delay, explaining our findings, whether the complaint is upheld (in whole or in part), any action taken or proposed, and, where no action is taken, the reasons for that decision.

Complaints About Data Processors

Where we receive a complaint that relates to the processing of personal information by our service providers, we will ask them to provide us with information relevant to the complaint without undue delay and in line with our contractual terms with the service provider.

Training

We will provide training for all staff on recognising a data protection complaint and what to do if they receive one, including where to direct a complaint within our organisation.

Record Keeping

We will keep a record of:

- the date we receive the data protection complaint
- our acknowledgement
- any relevant conversations and documents
- the outcome of the complaint
- any actions we take because of our investigation.

We will use these records to demonstrate compliance, for audit and monitoring purposes, training, to support consistent handling and to identify recurring issues, trends or areas for organisational improvements or remediation.

We will not retain personal data relating to complaints for longer than is necessary.

Complaints to the Information Commissioner's Office

You have the right to make a data protection complaint at any time to the Information Commissioner's Office (ICO).

The ICO's contact details are as follows:

Information Access Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113
ICO website: <https://www.ico.org.uk>

Conclusion

This policy sets out this organisation's commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.

Signed: S Thompson (signed on original)

Date: 23rd May 2018

Policy review record:

16 th May 2019	No Changes (S Thompson)
13 th May 2020	No Changes (S Thompson)
3 rd February 2021	Updated to reflect the impact of Brexit (S Thompson)
7 th February 2022	No Changes (S Thompson)
3 rd February 2023	No Changes (S Thompson)
2 nd February 2024	No Changes (S Thompson)
9 th September 2025	No Changes (S Thompson)
6 th February 2026	No Changes (S Thompson)
3 rd June 2026	Updated to include the complaints policy (S Thompson)

Next Policy Review Date: 28th February 2027