Data Protection Policy

Introduction

Suffolk Preservation Society ("SPS") is subject to the Data Protection Act 2018. Additionally, we are now subject to the UK General Data Protection Regulation 2021 The Data Protection Act and the GDPR were both introduced in order to ensure the safety and security of individuals' personal data, and to give individuals control over how organisations store and process that data. We recognise and support these aims, and take our obligations under the Data Protection Act and the GDPR very seriously.

This policy sets out the standard operating procedures that SPS' employees are expected to follow when storing and/or processing personal data. Suppliers to, and subcontractors of, SPS who process personal data on our behalf are also expected to comply fully with this policy.

Policy scope

This policy applies to all SPS employees, of all levels of seniority. It also applies to all suppliers to, and subcontractors of, SPS who process personal data on our behalf. Before a supplier or subcontractor is engaged to process personal data on our behalf, written authorisation must be obtained from a SPS Director.

This policy is written in such a way as to ensure compliance with the Data Protection Act and the GDPR. As such, any deviation from the standard operating procedures contained within this policy risks contravening one or both of these pieces of legislation. Such a contravention would have serious consequences for the individuals whose personal data we process. SPS would also be at risk from serious reputational damage and significant regulatory action. As such, any breach of this policy by a SPS employee will be treated as an extremely serious incident. A breach of this policy may result in disciplinary action in accordance with the SPS Disciplinary Procedure. Dependent on the severity of the breach, the employee(s) responsible may also be found to have committed gross misconduct.

We would prefer that an employee asks us before processing personal data, rather than taking a decision they are uncertain about and contravening data protection legislation. Employees who would like to ask questions about data protection, our standard operating procedures and/or what they should do in a particular situation, should contact director@suffolksociety.org before any processing of personal data takes place. We can then advise on the best course of action without any breach occurring.

Scope of SPS's responsibilities

SPS has responsibilities as a Data Controller and a Data Processor under the Data Protection Act. SPS handles personal data pertaining to members, suppliers, potential members and employees. The scope and method of processing of some of this data is decided upon by SPS. We are the Data Controller for this data. For other data, our members decide upon the scope and method of processing. In these cases, the member would be the Data Controller and we would be the Data Processor.

Irrespective of whether we are the Data Controller or the Data Processor, SPS employees are expected to act to safeguard personal data and protect the rights of the subjects of that data.

SPS is registered with the Information Commissioner's Office under Registration Number ZA427098. This registration is to be renewed annually by the Director responsible for compliance.

Data protection principles

SPS undertakes to comply with the 8 data protection principles laid down by the Data Protection Act. These principles are as follows:

1. Personal data will be processed fairly and lawfully.
2. Personal data will be obtained only for one or more specified and lawful purposes, and will not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data will be adequate, relevant and not excessive.
4. Personal data will be accurate and, where necessary, kept up to date.
5. Personal data will not be kept for longer than is necessary for a particular purpose or purposes.
6. Personal data will be processed in accordance with the rights of data subjects.
7. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data will not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The rights of data subjects

The Data Protection Act confers some rights upon data subjects in relation to their data. The GDPR confers further rights upon data subjects, and within these additional rights the rights granted by the Data Protection Act are also covered.

In brief, data subjects have the following rights under the Data Protection Act and the GDPR:

1. The right to be informed about the collection and use of their personal data
2. The right to access their personal data
3. The right to have inaccurate / incomplete personal data rectified / completed
4. The right to have their personal data erased
5. The right to restrict processing of their personal data
6. The right to obtain and reuse their personal data for their own purposes across different services
7. The right to object to the processing of their personal data
8. Rights relating to automated decision making, including profiling

The specific application of each of these rights is covered in section 11.

Personal data

Data processing regulations only pertain to personal data. This means that, whilst a lot of the data stored by SPS will be subject to the standard operating procedures contained within this policy, not all of it will.

Personal data consists of any information from which a living individual can be identified. This includes names, addresses, email addresses and job titles. It also includes less obvious examples such as car registration numbers (where the vehicle is registered to an individual).

Additionally, for data to be classed as personal data, it must be easily retrievable. Data is generally classed as personal data if it is stored electronically on any media, including DVDs, Blu-Ray discs, USB sticks, mobile telephones and computer hard drives. Data stored in manual form such as paper-based files or card index systems is also usually classed as personal data. The only exception to this is where the paper-based data is so unstructured that information relating to a specific individual is extremely difficult or impossible to retrieve. An example of this would be a disorderly pile of papers.

SPS operates on a “paper free” basis. This means that employees should not routinely store any data in paper form. Any such data must be destroyed securely as soon as it is no longer being actively worked on.

Additionally, employees are not permitted to store or transfer data using portable media (e.g. USB drives, portable hard drives). All data should be stored and transferred using Dropbox. Employees must not store SPS data on personal devices, including desktop PCs and laptops. This should be stored and saved to the Cloud.

SPS’s expectation is that SPS staff should treat any information (in any form) relating to individuals as personal data. Personal data does not need to be factual or numerical and will include any expression of opinion about an individual and any indication of intention about an individual. Information which is completely anonymous or which relates to companies or deceased persons will not be personal data but should still be treated with sensitivity. Information about individual contacts at companies will be personal data.

Certain types of personal data are classed as sensitive personal data. Information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, physical and mental health, sexual life and/or orientation, trade union membership, genetic data, biometric data, criminal convictions or alleged offences is classed as sensitive personal data.

SPS employees should exercise great caution when processing personal data. It is imperative that any data which could be construed to be personal data is treated as if it is personal data. Particular care should be taken when handling sensitive personal data.

What is data processing?

The definition of processing is very wide and as such all conceivable activities involving personal data should be taken to be processing of that data. Processing therefore includes obtaining, recording, consulting and/or storing personal data and carrying out any operation or set of operations on personal data.

Guidelines for SPS staff

New tasks and activities

Whenever a new task or activity is to be undertaken, the member of SPS staff responsible for the task or activity should consider whether the task or activity involves the processing of personal data.

If it does, the member of SPS staff responsible for the task or activity should notify the Data Protection Officer via sps@suffolksociety.org prior to the activity taking place. The Data Protection Officer will log the activity, confirm this to the member of SPS staff responsible for the task or activity and update SPS’s ICO registration where applicable. If, during the course of a task or activity, it becomes necessary for data to be processed in a different

way or for different purposes to that carried out previously, the Data Controller must be informed as soon as possible.

Processing of personal data

Personal data must only be processed fairly and lawfully. In particular, personal data must only be used in connection with, and to the extent necessary for the purposes of, a member of staff's employment. SPS should not collect personal data which is excessive when compared to the purposes for which it will be used. Irrelevant data should not be collected.

In order for us to process personal data, we need to prove that we have a lawful basis for doing so. The two most common lawful bases for processing for the activities that we carry out are "Contract" and "Legitimate interests". It is the responsibility of the Data Protection Officer to determine the most appropriate lawful basis for processing personal data. This must happen before the processing takes place, because information about what lawful basis has been selected must be communicated to the data subjects. This is why it is essential that SPS employees contact the Data Protection Officer before commencing any new processing of personal data.

Indirect personal data

If SPS employees collect personal data indirectly (for example from a third party or a published source), they must consider whether it is necessary to inform the subjects of that personal data that SPS is holding their data, and whether it is necessary to tell them how we will process the data. The subjects should not be informed where the effort involved in providing this information would be disproportionate to the value to the individual of being informed. The Data Protection Officer should be contacted for advice where required, and any decision not to inform the individual(s) concerned should be reported to the Data Protection Officer.

Disclosure of personal data

Employees must never disclose personal data to a third party (including any data processors) without the written permission of the Data Protection Officer. This permission may be given on a one-off basis, or on an ongoing basis for a regular disclosure requirement. In all cases permission must be sought prior to disclosure, and disclosure must be recorded on a Data Disclosure Form, which should then be returned to the Data Protection Officer once completed.

Sensitive personal data

SPS employees should not seek to collect sensitive personal data (as defined in section 8) unless it is directly needed for the purposes of the staff member's employment. Where such data is collected employees must ensure that the data subject concerned has a full understanding of why the data is being collected, what it will be used for and how it will be processed, and the individual must consent to the collection of this data in writing. Sensitive personal data must never be collected indirectly.

Updating personal data

SPS employees should ensure that, as far as is reasonably practicable, personal data which they collect and use is kept accurate and up to date. If a data subject notifies you that their data is incorrect or incomplete, you should rectify / complete it. Please consult section 11 for further information on this.

Deletion of personal data

Our data will only be kept for as long as there is an administrative need to do so in order to enable our charity to carry out its business or support functions, or for as long as it is required to demonstrate compliance for audit purposes or to meet legislative requirements.

In general, records are kept for 6 years after the end of the accounting year to which they relate but we do not keep personal records any longer than necessary and certain records may be required to be retained for longer. Factors affecting retention periods include legal requirements, storage costs, historical value, industry standards, and archival needs.

Annex 3 contains details of the retention periods for all personal data currently being processed by SPS. This will be updated by the Data Protection Officer when data processing activities are added, removed or modified. SPS employees should consult this Annex and retain / delete personal data in accordance with the retention periods specified.

It is essential that SPS employees delete / dispose of personal data carefully. Digitally stored data should only be deleted after discussions with the IT Consultant, who will advise on the most secure way to delete the data. Paper based data should be shredded securely, using a suitable shredding contractor or an appropriate company-owned shredder. Any employee working remotely who requires secure destruction facilities to comply with this requirement should contact their Line Manager, who will arrange for the secure destruction of the data.

Transfer of personal data

SPS staff must never use any kind of portable media to transfer any personal data under any circumstances. Such transfers should be effected securely, using Dropbox or MS Outlook and with an appropriate degree of security based on the nature of the data.

Personal data must not be transferred to organisations outside of SPS without the written permission of the Data Protection Officer, except where such a transfer is permitted in accordance with Annex 2.

Data subjects' rights under the GDPR

The right to be informed about the collection and use of their personal data

Data subjects have the right to be informed about how we will collect, store and use their personal data. We need to provide data subjects with the following information:

- Our purpose(s) for processing their personal data
- How long we will keep their personal data for
- Who their personal data will be shared with

This information is called “Privacy Information”. When personal data is collected directly from data subjects, we must provide Privacy Information at the point that we collect the data. When personal data is obtained from other sources, we must provide Privacy Information to the data subject(s) within a reasonable period of obtaining the data (and no later than one month from obtaining the data). The Data Protection Officer will advise further on this upon request.

The right to access their personal data

Individuals have the right to ask us to confirm that we are processing their personal data. They also have a right to a copy of all of the personal data that we hold about them.

Additionally, they can ask us for supplementary information about how we process their personal data. This supplementary information will have been contained in the Privacy Notice relating to the personal data that they are enquiring about. As such, it is acceptable to supply the relevant Privacy Notice(s) in response to a request for supplementary information.

Requests for access to personal data can be made electronically, in writing, by telephone or in person.

Any SPS employee who is contacted by anybody who is, or might be, requesting access to their personal data should do the following:

1. Record the name and contact details of the person making the request
2. Record the personal data that they are requesting
3. Tell them that the SPS Data Protection Officer will be in touch in due course
4. IMMEDIATELY email the information to the Data Protection Officer at (sps@suffolksociety.org)
5. Any further contact / chasing / follow up by the data subject should be forwarded to the Data Protection Officer for a response

Data subjects have the right to request all of the data that we hold about them. However, locating all the data that we hold about a specific individual is time consuming and expensive. Most data subjects making a request will want a specific piece of information. Please engage with the data subject proactively to find out what they actually want to know, and in the first instance suggest that the request be narrowed in scope to just that information. If they would like to make a full subject access request then they must of course be allowed to do so.

NEVER DISCLOSE PERSONAL DATA TO ANY DATA SUBJECT. ALWAYS FOLLOW THE ABOVE PROCEDURE AND REFER THE REQUEST TO THE DATA PROTECTION OFFICER.

The right to have inaccurate / incomplete personal data rectified / completed

Individuals have the right to ask us to rectify inaccurate personal data that we hold about them, and also to complete incomplete personal data that we hold about them.

Requests for rectification / completion of personal data can be made electronically, in writing, by telephone or in person. Any SPS employee who is contacted by anybody who is, or might be, requesting rectification / completion of their personal data should do the following:

1. Record the name and contact details of the person making the request
2. Record the personal data that they are requesting be rectified / completed
3. Tell them that the SPS Data Protection Officer will be in touch in due course
4. IMMEDIATELY email the information to the Data Protection Officer (sps@suffolksociety.org)
5. Any further contact / chasing / follow up by the data subject should be forwarded to the Data Protection Officer for a response

The right to have their personal data erased

In some circumstances, individuals have the right to ask us to erase personal data that we are holding about them.

Requests for erasure of personal data can be made electronically, in writing, by telephone or in person. Any SPS employee who is contacted by anybody who is, or might be, requesting erasure of their personal data should do the following:

1. Record the name and contact details of the person making the request
2. Record the personal data that they are requesting be erased, and their reason(s) for requesting its erasure
3. Tell them that the SPS Data Protection Officer will be in touch in due course
4. IMMEDIATELY email the information to the Data Protection Officer (sps@suffolksociety.org)
5. Any further contact / chasing / follow up by the data subject should be forwarded to the Data Protection Officer for a response

The right to restrict processing of their personal data

Individuals have the right to request us to restrict the processing of their personal data in the following circumstances:

- The individual contests the accuracy of their personal data and we are verifying the accuracy of the data

- The data has been unlawfully processed and the individual opposes erasure and requests restriction instead
- We no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim
- The individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual

Requests for restriction of processing of personal data can be made electronically, in writing, by telephone or in person. Any SPS employee who is contacted by anybody who is,

or might be, requesting restriction of processing of their personal data should do the following:

1. Record the name and contact details of the person making the request
2. Record the personal data that they are requesting processing be restricted for, and their reason(s) for requesting the restriction of processing
3. Tell them that the SPS Data Protection Officer will be in touch in due course
4. IMMEDIATELY email the information to the Data Protection Officer (sps@suffolksociety.org)
5. Any further contact / chasing / follow up by the data subject should be forwarded to the Data Protection Officer for a response

The right to obtain and reuse their personal data for their own purposes across different services

Individuals have the right to request us to supply them with personal data that they have provided to us. We have to provide it to them in a structured, commonly used and machine readable format, and they can also request that we transmit it directly to another data controller on their behalf. Individuals only have this right in respect of personal data that is processed automatically (i.e. on a computer) and processed under a lawful basis of "Consent" or "Contract". However, based on our Personal Data Audit, we predict that the vast majority of our data will meet this definition.

Requests relating to the portability of personal data can be made electronically, in writing, by telephone or in person. Any SPS employee who is contacted by anybody who is, or might be, making a request related to the portability of their personal data should do the following:

1. Record the name and contact details of the person making the request
2. Record the personal data that they are requesting be supplied to them / another data controller
3. Obtain details of the Data Controller(s) that they wish their data to be supplied to (if applicable)
4. Tell them that the SPS Data Protection Officer will be in touch in due course
5. IMMEDIATELY email the information to the Data Protection Officer (sps@suffolksociety.org)
6. Any further contact / chasing / follow up by the data subject should be forwarded to the Data Protection Officer for a response

The right to object to the processing of their personal data

Individuals have the right to object to the processing of their personal data. They only have the right to object to this processing if we are processing the data for direct marketing, a task carried out in the public interest, the exercise of official authority vested in us or the legitimate interests of ourselves or a third party. At the moment, we only process personal

data for direct marketing purposes. If we commence processing of personal data for any of the other purposes listed above, this section of the policy will be updated.

Objections to processing of personal data for direct marketing can be made electronically, in writing, by telephone or in person. Any SPS employee who is contacted by anybody who is, or might be, making an objection to the processing of their personal data for direct marketing should do the following:

1. Record the name and contact details of the person making the objection
2. Record the personal data that they are objecting about the processing of
3. Tell them that the SPS Data Protection Officer will be in touch in due course
4. IMMEDIATELY email the information to the Data Protection Officer (sps@suffolksociety.org)
5. Any further contact / chasing / follow up by the data subject should be forwarded to the Data Protection Officer for a response

Any employee wishing to commence a direct marketing campaign must first discuss the campaign with, and seek permission from, the Data Protection Officer. This requirement applies irrespective of whether the personal data required for the campaign is already held by SPS or it needs to be collected / obtained.

Rights relating to automated decision making, including profiling

Individuals have certain rights relating to automated decision making and profiling using their data. However, at this time, SPS does not process any personal data in ways that would fall under the scope of this right. If we commence processing of personal data in one or more of these ways, this section of the policy will be updated.

Informing staff about their data protection responsibilities

All SPS employees and directors must be emailed a copy of the current data protection policy when they join the company. They must also be emailed a copy of the current data protection policy every year following its annual update, if the policy has been updated.

All SPS employees and directors must read, understand and sign a copy of Annex 1 – Summary of guidance for staff. This annex summarises the principal duties of SPS employees in relation to data protection, and is considered to be the principal method for informing employees of their obligations and duties under data protection regulations.

Annex 1 – Summary of guidance for staff

The SPS Data Protection Officer is the Office Manager responsible for compliance within SPS and can be contacted via email at sps@suffolksociety.org or on 01787 247179. You should consult them if you have any data protection queries.

THINK: Am I sharing something containing a person's name / other identifiable data to ANYBODY who is not a direct employee of SPS? IF SO, STOP! Contact sps@suffolksociety.org for advice FIRST!

You must NEVER disclose personal data to ANY third party without the express permission from the Data Protection Officer, except where doing so is permitted under Annex 2. In all other cases, you MUST seek permission prior to disclosing data, and all instances of disclosure must be recorded on a Data Disclosure Form, signed by the Data Protection Officer before disclosure occurs.

SPS Data Disclosure Process:

1. Check the Client Disclosure List (see Annex 2) to see if the data you wish to disclose, and the recipient, are listed. If they are, we have an existing contractual arrangement with the recipient to disclose data to them and data subjects are informed of this when they give us their personal data. This means that you can disclose the data without seeking permission from the Data Protection Officer.
2. If the data you wish to disclose, and the recipient, are not BOTH listed in the Client Disclosure List, you must contact the Data Protection Officer requesting permission to disclose data (summarise data to be disclosed, frequency of disclosure, reason for disclosure, who disclosure will be made to)
3. Data Protection Officer will complete and sign relevant sections of a Data Disclosure Form and return it to you
4. Disclose data in accordance with instructions from Data Protection Officer
5. Complete relevant sections of Data Disclosure Form and return it to the Data Protection Officer

SPS employees responsible for introducing new processes or tasks should consider whether any processing of personal data is involved. If it does, permission should be sought from the Data Protection Officer in advance. In particular, permission must be sought if the data will be processed in a different way or for a different purpose to processing carried out previously.

You should collect as little personal data as possible, and data that is collected must only be used for official company purposes, as authorised/requested by your Line Manager or a Director.

In order for us to process personal data, we need to prove that we have a lawful basis for doing so. The two most common lawful bases for processing for the activities that we

carry out are “Contract” and “Consent”. It is the responsibility of the Data Protection Officer to determine the most appropriate lawful basis for processing personal data. This must happen before the processing takes place, because information about what lawful basis has been selected must be communicated to the data subjects. This is why it is essential that SPS employees contact the Data Protection Officer before commencing any new processing of personal data.

Information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, physical and mental health, sexual life and/or orientation, trade union membership, genetic data, biometric data, criminal convictions or alleged offences is classed as sensitive personal data.

Be aware of collecting personal data indirectly (for example from a third party or a published source) – if you do this, you may need to inform the people whose data has been collected. The Data Protection Officer should be consulted for advice in these cases. Sensitive personal data must never be collected indirectly.

SPS employees should ensure that, as far as is reasonably practicable, personal data which they collect and use is kept accurate and up to date.

Data subjects have a wide range of rights relating to the processing, storage and transfer of their personal data. Requests relating to these rights can be made electronically, in writing, by telephone or in person, and they can be made to any SPS employee. Section 12 of the Data Protection Policy contains full details of these rights, and the procedures that should be followed if you know or suspect that a data subject is making a request to you in relation to their personal data.

Annex 3 of the Data Protection Policy summarises all current personal data held by SPS, and lists the arrangements for its retention. Employees responsible for data listed in Annex 3 should manage this data in accordance with the Data Protection Policy, and delete it in accordance with the retention periods specified in Annex 3.

It is essential that SPS employees delete / dispose of personal data carefully. Digitally stored data should only be deleted after discussions with the IT Consultant, who will advise on the most secure way to delete the data. Paper based data should be shredded securely, using a suitable shredding contractor or an appropriate company-owned shredder. Any employee working remotely who requires secure destruction facilities to comply with this requirement should contact their Line Manager, who will arrange for the secure destruction of the data.

SPS staff must never use any kind of portable media to transfer any personal data under any circumstances. Such transfers should be affected securely, using Google Drive or Gmail, in consultation with the IT Consultant, and with an appropriate degree of security based on the nature of the data.

Employee declaration

I have read and understood, and agree to comply with, the information contained within this Annex. I understand that I am also required to comply with the SPS Data Protection Policy, and that I should consult this policy and/or the Data Protection Officer if I am unsure of anything relating to data protection.

Name: .....

Signature: .....

Date: .....

Annex 2 – Permitted data disclosure under existing Privacy Notices

Personal data must normally never be disclosed to third parties outside of SPS without reference to the SPS Data Protection Officer and the completion of a Data Disclosure Form. However, if we have a Privacy Notice in place between us and the data subjects that covers the desired data disclosure, reference to the SPS Data Protection Officer is not required.

Release of customer data stored on the SPS Membership database

SPS remains the Data Controller for all data processed using the membership database. However, in each case, our client is named in the relevant Privacy Notice as a Data Processor. This means that we are permitted to disclose personal data collected from the membership database to certain employees of our clients.

Data disclosure is only permitted for data from a specific web address, to the client who is named below for that web address. If you are unsure, please contact director@suffolksociety.org before disclosing personal data.

IMPORTANT: Email addresses can look very similar – double check for any characters or symbols in unexpected places. In particular, make sure the last part of the email address (the part after the @ symbol) is exactly as stated below. If it's not, you could be sending personal data to a completely different person to the one you think you are!

Prior to any requirement for data processing or disclosure, a SPS Director will supply the current Client Disclosure List to the employee(s) who require it. This document lists all the current people at each of our clients who, under existing Privacy Notices, we are permitted to disclose data to. If you receive an email from a client requesting personal data, please do not respond before you have checked with the Director (director@suffolksociety.org)

Annex 3 – Personal data retention periods

Personal data	Retention period	Justification	Privacy Notice
Employee emergency contact information	Immediately following end of employment	No need for information once employee no longer works for us	Employee, additional letter
Documents proving employee's right to work in the UK	2 years following end of employment	Home Office recommended practice	Employee
Copies of employee's driving licence and records of any endorsements on the licence	3 years following end of employment	Limitation Act 1980 – 3 year statute of limitations	Employee
All other employee personal data	10 years following end of employment	Various HMRC, HSE and internal requirements	Employee
Outlook contacts (personal and shared) and emails	Indefinitely	Business critical information for ongoing operations	Website
Personal data collected from customers via websites	6 years from the end of the relevant academic year	Business critical information with liability and financial implications	Website
Personal data collected from customers via SPS	1 year from the end of the relevant academic year	Business critical information with liability and financial implications	Website
Data collected by Google Analytics when website users visit a website	50 months from date of accessing the website	Business critical information with liability and commercial implications	Website

Personal data collected as part of consultancy projects	6 years from the end of the relevant academic year	Business critical information with liability and financial implications	Website / bespoke notice

Data Protection Policy

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Board	Sept 2025	Initial draft approved	Annually