

# The SUN Network Cambridgeshire and Peterborough

## Data Protection Policy

### Policy statement

The SUN Network recognises the role it has to protect the rights, freedoms and privacy of the people who share personal data with it. This policy applies to all directors, staff, and volunteers of The SUN Network.

The SUN Network collects and uses personal data, including sensitive personal data, which means it is responsible for complying with the Data Protection Act\* (UK GDPR)

### Definitions

A 'data subject' is the person whose personal data is being held and used. The SUN Network's data subjects include employees, volunteers, job applicants and members of the public.

'Personal data' is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

'Sensitive personal data' is defined as personal data consisting of information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, transmission, dissemination or adaption of the data.

\* <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

### Purpose of this Policy

The aim of this document is to assist and inform the directors, staff and volunteers of The SUN Network to comply with the requirements of the Data Protection Act (DPA) 2018 (UK GDPR), to minimise any risks to The SUN Network and its data subjects, and to provide clear good practice guidelines for all involved. It sets out what The SUN Network will do, what is expected of directors, staff, and volunteers. It must be fully understood and adopted by all directors, staff, and volunteers.

### Principles

The SUN Network endorse and adhere to the principles of the Data Protection Act 2018. The way we will do this is summarised below.

- We will process data lawfully, fairly, and transparently

- We will only collect data for explicit and lawful purposes
- Data must be relevant and necessary for the purpose it is being collected
- We will keep data up to date and accurate
- We will keep data only if required and for no longer than necessary (see the Information Asset Register)
- We will keep data secure
- We will process data in such a way as to protect the rights and freedoms of data subjects

and

- Personal data will be transferred outside of the UK and EU only in certain specific circumstances and ways

These principles apply to obtaining, handling, processing, transporting and storage of personal data. Directors, staff, and volunteers, as well as agents of The SUN Network who obtain, handle, process, transport, and store personal data, must adhere to these principles at all times. The SUN Network will provide reasonable levels of training, support, and resources to do so.

## The rights of data subjects, and how we meet them

The table below sets out the rights of data subjects as defined in the Data Protection Act. In the table we describe the way that we assure we maximise these rights and minimise the risk that these rights are infringed.

The data subject rights	What this means	What we do
The right to fair processing	That data subjects have the right to information about the processing of their data and about their rights	Data subjects will be informed at the point at which information is collected: <ul style="list-style-type: none"> <li>• What data is being collected and for what purpose</li> <li>• How long the data is held for</li> <li>• Their rights in relation to that data</li> <li>• Anyone else who will have access to the data, why, and how they will use the data. We will either name the third party or describe groups of third parties</li> <li>• Any data that is crossing UK/EU borders, where to, and how it is protected. This information will be clearly presented in a privacy notice on The SUN Network's website(s). Short versions will be on forms and signing in registers. Staff will be given information in their terms and conditions and volunteers in volunteer welcome packs.</li> </ul>
The right of access	That data subjects have the right to receive a copy of their data, including any data being processed by third parties. This allows them to be aware of, and verify, the lawfulness of the processing	The SUN Network will ensure that all individuals who have personal data held and used by The SUN Network can easily <ul style="list-style-type: none"> <li>• Ask what personal data The SUN Network holds about them, with a description of the data</li> <li>• Ask why The SUN Network holds this data</li> <li>• Ask how long data is held for, and why</li> <li>• Ask for a copy of the personal data</li> <li>• Ask about anyone else who has access to this data and why, including anyone outside the EU, and how this data was transferred legally and safely</li> </ul> Asking about personal data is called a 'subject access request' or SAR. To enable data subjects to do this The SUN Network will:

		<ul style="list-style-type: none"> <li>• Train all directors, staff, and volunteers to recognise a SAR (including one from a person who does not know the correct term, or what their rights are)</li> <li>• Make a SAR request form available. In some cases, The SUN Network may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify the individual's identity and the documents required</li> <li>• Ask the data subject which data they want, and in what format</li> <li>• Allocate a staff member to manage the request. This may be the Data Protection Officer or a SUN Network staff member, and the data subject may be offered, where possible, the choice</li> <li>• Remove any third party information from the record</li> <li>• In most cases within 30 days, provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise. It will only be provided to the data subject. The SUN Network will also provide information about where the data has or will be disclosed, how long it will be stored for and the criteria used to determine that period of time</li> <li>• In some cases, such as where The SUN Network processes large amounts of a data subject's data, it may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell them if this is the case</li> <li>• If a subject access request is manifestly unfounded or excessive, The SUN Network is not obliged to comply with it. Alternatively, The SUN Network can agree to respond but will charge a fee, which will be transparently based on the administrative cost of responding to the request. A SAR is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, The SUN</li> </ul>
--	--	--

		Network will notify the data subject that this is the case and whether or not it will respond to it.
The right of rectification	The data subject has the right to correct any inaccuracies in the data	<p>The SUN Network will make every effort to ensure the quality and accuracy of data it collects. The SUN Network will enable data subjects to rectify their data by</p> <ul style="list-style-type: none"> <li>• Regularly reviewing and updating personal information in their systems</li> <li>• Telling data subjects that it is their right to rectify their data, and make it easy to do so</li> <li>• In the case of a data subject request, tell the data subject about his/her rights to rectification or erasure of data, or to restrict or object to processing</li> </ul>
The right to be forgotten	That the data subject can have their personal data removed or erased at any time without delay	<p>The SUN Network will enable this by</p> <ul style="list-style-type: none"> <li>• Telling data subjects that it is their right to ask for their data to be erased, and making it easy to do so</li> <li>• Collecting and processing personal information only to the extent that it is needed to fulfil operational needs or legal requirements</li> <li>• Giving a clear explanation of any erasure decision in writing to the data subject</li> <li>• Not keeping information for longer than required, operationally or legally</li> <li>• Having a clear process by which data is erased in a timely way</li> <li>• Making it clear what the exceptions are: where personal data is held to protect the right to freedom of expression or information, to comply with legal obligations, to perform a task in the wider public interest or exercise of official authority, for public health reasons, for archiving, scientific or historical research, or for the establishment or defence of a legal claim</li> <li>• Giving a clear explanation of any erasure decision in writing to the data subject</li> </ul>
The right to restriction of processing	That a data subject is allowed, in specific circumstances, to prevent The SUN Network from	This may be because they feel the data is inaccurate, is being processed unlawfully, is no longer needed or they object on some other grounds. The SUN Network will enable this by

	conducting specific processing tasks	<ul style="list-style-type: none"> <li>• Telling data subjects that it is their right to restrict processing, and make it easy to do so</li> <li>• Clearly describing the processing activities that are being done so that data subjects can make informed choices</li> <li>• Holding the data securely while a request to restrict processing is considered (and halting all processing)</li> <li>• Involving the Data Protection Officer in managing and documenting a process to consider the request, comparing their grounds with the legal grounds that The SUN Network have for the processing</li> <li>• Giving a clear explanation of any restriction in writing to the data subject</li> </ul>
The right to data portability	That the data subject can request copies of their data in a useful format in order to pass them to another service provider	<p>The SUN Network will enable this by:</p> <ul style="list-style-type: none"> <li>• Telling data subjects that it is their right to data portability</li> <li>• Providing data in an easy read, electronic format (see data subject access requests, above).</li> </ul>
The right to object	That if a data subject objects to how their data is being controlled or processed, The SUN Network must halt processing until it has investigated and demonstrated its legitimate grounds for processing	<p>The SUN Network will enable this by:</p> <ul style="list-style-type: none"> <li>• Telling data subjects that it is their right to object to processing, and make it easy to do so</li> <li>• Telling the data subject about their right to complain to the Information Commissioner if they think The SUN Network has failed to comply with their data protection rights</li> <li>• Involving the Data Protection Officer to mediate where appropriate in any request to halt processing.</li> </ul>
The right to appropriate decision making	That The SUN Network will ensure decisions are not made solely by automated means	<p>The SUN Network will ensure this happens by ensuring the following roles are clearly in place and that the people in those roles are trained and equipped:</p> <ul style="list-style-type: none"> <li>• All directors, staff and volunteers will have received induction training on data protection and will have been told what their responsibilities and roles are in their role description. All employees are responsible for ensuring that personal information is appropriately collected, is not kept for longer</li> </ul>

		<p>than necessary and that all information is kept secure. They must read and understand this policy. They will be appropriately trained and supervised to fulfil their data protection role. They will be given the appropriate resources to protect the rights and freedoms of data subjects, including access to security systems and information for data subjects. Specifically, they will be enabled to recognise and refer subject access requests, and to ensure personal data is accurate, up to date and erased where appropriate</p> <ul style="list-style-type: none"> <li>• Some staff with specific responsibilities for handling personal data will understand that they are contractually responsible for following good data protection practice, will be trained to do so and appropriately supervised</li> <li>• The CEO will be the Senior Information Risk Owner</li> </ul> <p>The Data Protection Officer will carry out the following tasks</p> <ul style="list-style-type: none"> <li>• Inform and advise The SUN Network of The SUN Network's obligations in relation to data protection</li> <li>• Monitor compliance with UK data protection law</li> <li>• Provide advice where requested about Data Protection Impact Assessments</li> <li>• Cooperate with the Information Commissioner's Office</li> <li>• Act as a contact point for the Information Commissioner's Office</li> <li>• Support with data subject requests and other data protection tasks as and when required.</li> </ul>
--	--	---



## **Data security at The SUN Network**

The SUN Network endeavour to safeguard personal data (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically; and ensuring that individual passwords are not easily compromised);

### ***Paper records***

All hard copy personal data is kept in locked cabinets in The SUN Network's office, a secure building.

### ***Electronically stored personal data***

Data stored electronically (e.g. in databases, survey providers etc.) will be kept to an appropriate standard and audited annually.

Data retained on laptops, smartphones and any other electronic equipment that is removed from The SUN Network offices is protected by the use of passwords.

Access to information on the main database is controlled by a password and only those needing access are given the password. All directors, staff and volunteers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

## **Data security; Third parties and data processors**

Any data passed to a third party, including to a processor, will be specified in a written agreement, setting out the scope and limits of the sharing. These parties are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. They have to confirm their conformance to the requirements of the DPA. Where a third party does not conform entirely to DPA, data subjects are explicitly informed of this and then are able to give their informed consent. Specifically:

- The data subject will be informed about any third parties who are in receipt of their data from The SUN Network
- Any disclosure of personal data will be in compliance with approved procedure
- Data stored electronically (e.g. in databases, survey providers etc.) will be kept to an appropriate standard and audited annually
- By law, The SUN Network is required to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings Regulations (TUPE)



- References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body)

## **Particular groups of data subjects**

### ***Employees***

- The SUN Network hold personal information about all employees as part of general employee records. This includes address and contact details, marital status, educational background, employment application, employment history with The SUN Network, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness, and other leave, working time records and other management records
- This information is used for a variety of administration and management purposes, including payroll administration, benefits administration, facilitating the management of work and employees, performance, and salary reviews, complying with record keeping and other contractual obligations
- The SUN Network may also process information relating to employee's health which may amount to sensitive personal data. This includes pre-employment health questionnaires, records of sickness absence and medical certificates (including self-certification of absence forms), VDU assessments, noise assessments and any other medical reports. This information is used to administer contractual and Statutory Sick Pay, monitor, and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations
- From time to time The SUN Network may ask employees to review and update the personal information that is held about them

### ***Children 17 and under***

- Wherever possible, The SUN Network will avoid holding personal data about people under the age of 18. Where it is working with children, it will seek to work with a third party who controls the data in line with that organisations data protection policy
- If personal data is held about a child, then the consent of that child's legal parent or guardian will be sought and appropriately stored
- The only exception is that The SUN Network will share information as per their Safeguarding Children policy

### ***Adults in need of care and support***

- In some cases, information will be shared with The SUN Network about a person's care by their carer or family member
- In these cases, The SUN Network will only hold personal data with the explicit consent of the person who the information is about
- A carers experiences of caring may be gathered and shared. If the information identifies the person they care for, it will only be processed with the informed

consent of the cared for person. If the person receiving care does not consent, The SUN Network will ensure any information is fully anonymised

- The only exception is that The SUN Network will share information as per their Safeguarding Adults policy

## **Monitoring data protection and assessing risk**

**Annual auditing** The SUN Network will maintain an information asset register. The information asset register is a list of personal and non-personal information assets that The SUN Network controls and processes. The SUN Network will undertake an annual audit of its compliance with this policy and with best practice. This will be overseen by the Data Protection Officer.

### **Data Protection Impact Assessments**

DPIAs are used to identify specific risks to personal data as a result of processing activities. Their role is to maintain security and prevent processing infringements of GDPR. The SUN Network will use them when required to evaluate the risks inherent in our work. A DPIA must contain:

- A description of processing and purposes
- The legal basis pursued by the controller
- An assessment of the necessity and proportionality of the processing
- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks
- Timeframes of processing for retention and erasure of data
- Recipients of data
- Any evidence of compliance
- Details of consultation with and consent of data subjects

This information is held within the information asset register. The register identifies which personal data processing presents any particular risk, and how this is managed, including the decision to use a DPIA.

The SUN Network will add to the information risk register in advance of any new project where a new category of personal data is collected, or when existing processing activities are changed.

### **Data breaches**

If The SUN Network discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect. The DPO will be informed. If the breach is likely to result in a high risk to the rights and freedoms of individuals, The SUN Network will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken. Describing lawful basis for controlling and processing data The SUN Network will only hold or use data for which it has a lawful basis for doing so.

The six lawful bases are:

1. Consent; the data subject gives consent based on real choice and control. The consent must be freely given with a full understanding of what it means. This means a positive opt-in to sharing the data. Consent should be kept separate from any other terms and conditions. Consent for different kinds of data will be separately sought. Records of consent will be kept
2. Contract; the processing is necessary for a contract The SUN Network has with the data subject, or because they have asked The SUN Network to take specific steps before entering into a contract (e.g. employee contract)
3. Legal obligation; the processing is necessary for The SUN Network to comply with the law (not including contractual obligations) (e.g. prevention of fraud)
4. Vital interests: the processing is necessary to protect someone's life (e.g. child protection disclosures)
5. Public task: the processing is necessary for The SUN Network to perform a task in the public interest and for their official functions, and the task or function has a clear basis in law. While The SUN Network provides a public function, the public has a right to refuse to take part in The SUN Network activities, and it will seek consent to process data in most cases
6. Legitimate interests: the processing is necessary for The SUN Network's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This basis does not apply to public authorities and so The SUN Network cannot use this as a legal ground. The legal bases are recorded in the Information Asset Register.

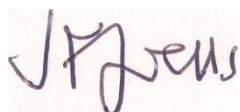
### ***Retention and disposal of data***

Information will be kept in line with the requirements of the DPA 2018 (UK GDPR). Documents containing any personal information will be disposed of securely, and paper copies will be shredded. Information stored on obsolete electronic equipment (desktops, laptops, and other devices) will be erased prior to them being sold or disposed of. Registration The SUN Network registered in the Information Commissioner's public register of data controllers.

**Approved by The SUN Network Board of Directors: April 2024**

Date of next review: April 2027

Responsible Officer: Executive Director



Jonathan Wells  
Chair of Directors

29<sup>th</sup> April 2024



Lois Sidney  
Executive Director

29<sup>th</sup> April 2024