

SusSAR Data Privacy Notice

Documentation control

Field	Detail
Version	3.0
Ratified by	Management Committee / Trustees
Date Ratified	21/09/2026
Author	[Name]
Responsible Officer	Data Protection Advocate, [Name]
Date Issued	23/09/2026
Review Date	20/09/2026
Intended Audience	Members of the public, members, volunteers, applicants, donors, supporters, families and people affected by a search
Contact	Data Protection Advocate, DPA@sussar.org
Published by	Sussex Search and Rescue

Version	Reason	By	Date
1.0	Original issue	D Wood	21/09/2026
2.0	Full review	D Wood	21/09/2026
3.0	Condensed public notice; clearer police-controller, rights, complaints and lawful-basis information	D Wood	21/09/2026

Read with: SusSAR Data Protection Policy; Records and Information Management Policy and Retention Schedule; Information Security and Device Policy; Confidentiality Agreement.

1. About this notice

1.1 What this notice covers

Sussex Search and Rescue, known as SusSAR, is a volunteer search and rescue charity. This notice explains how we use personal information when we act for our own charitable purposes. It is for the public, our members, volunteers, applicants, donors, supporters, people who contact us and families affected by a search.

Personal information identifies you or could reasonably be linked to you. It includes paper and electronic records, forms, messages, photographs, video, location and website records. Some information needs extra care, including health, disability, racial or ethnic origin, religion, biometric information used to identify someone, sexual life, sexual orientation and criminal-offence information. We use it only where necessary and permitted.

1.2 Who we are and how to contact us

For the information covered by this notice, SusSAR is the controller. This means that we decide why and how it is used.

We are a registered charity in England and Wales, number **1204106**. Our registered office is **c/o Sussex Police, Police Station, Bolnore Road, Haywards Heath, RH16 4BA**. We are a Lowland Rescue affiliated volunteer auxiliary to Sussex Police and Surrey Police.

Our voluntary **Data Protection Advocate** can help with questions, requests and concerns. Email **DPA@sussar.org**, or write to the registered office marked for the Data Protection Advocate. We do not have to appoint a statutory Data Protection Officer.

1.3 When this notice applies

We give you this notice when you give information to us, such as through an application, donation, event, website or contact form. We may also give you a short notice at the point of collection.

We sometimes receive information from a referee, emergency contact, training or qualification provider, Lowland Rescue, a safeguarding partner, adviser, insurer, regulator, public authority, or someone making a concern or complaint. It may include contact or relationship details, references, qualifications, availability, welfare or safety information, correspondence and the facts of a concern.

For information from another source, we provide the Article 14 UK GDPR information within a reasonable period and no later than one month, or sooner if we contact you or disclose it. We may rely on a lawful exemption only after assessment. We do not routinely collect public-source information.

1.4 Whether you have to give us information

You do not have to provide optional supporter preferences, publicity information or other optional information. Some information is needed to process an application, arrange safe participation, administer a donation, respond to a request, or meet finance, tax, insurance, safeguarding or legal duties. Without it, we may be unable to do the relevant task. Consent to optional activity is never a condition of ordinary membership, volunteering or support.

2. How we use your information

2.1 Our lawful basis

Data protection law requires us to have a lawful basis for each use of personal information. Where we use special category information, we also need an additional condition.

We often rely on legitimate interests: our genuine interests in operating a safe, accountable rescue charity and supporting people who engage with us. We consider necessity and the effect on you before relying on this basis. You can object; see section 6.

The table gives our main uses and normal retention periods. We may keep a record longer for a legal duty, insurance, safeguarding, an investigation, a claim or a legal hold.

What we do	What information	Why	Our lawful basis	How long we keep it
Recruit, administer and support members, volunteers and applicants	Name, contact details, applications, references, role, skills, qualifications, emergency contacts, availability and correspondence	To assess applications and run a safe, capable and accountable volunteer charity	Article 6(1)(f): our legitimate interests in safe charity administration; Article 6(1)(c) where a legal duty applies. Where needed, Article 9(2)(g) and the Schedule 1 safeguarding condition for health, fitness, welfare or safeguarding information	Unsuccessful applications: 12 months after decision. Membership and training records: membership plus 3 years
Check vetting, safeguarding, fitness and readiness	Vetting status, qualifications, training,	To safeguard people and decide whether	Article 6(1)(f), or Article 6(1)(c) where required by law. Where needed,	Vetting and qualifications: membership plus 3

What we do	What information	Why	Our lawful basis	How long we keep it
	health, welfare, next-of-kin and equipment details	someone is ready for a role or deployment	Article 9(2)(g) and the Schedule 1 safeguarding condition; criminal-offence information is used only where an applicable legal condition is recorded	years. Health, welfare and emergency-contact details are reviewed at least annually and deleted at departure unless needed for a claim or safeguarding matter
Respond to an emergency, provide casualty care and hand over to clinical services	Identity, location, observations, care given, casualty and safety details, and handover information	To protect life, provide care and make a safe handover	Article 6(1)(d): vital interests. For care and clinical handover, Article 9(2)(h) with Schedule 1 Part 1 paragraph 2. If a person cannot consent, Article 9(2)(c): vital interests	Our own operational logs: 7 years. Serious safety, safeguarding or critical incident records: 7 years after closure, or longer while an inquiry, claim or legal hold continues
Share essential information with emergency services, other search and rescue teams, and safeguarding partners	The minimum identity, location, safety, welfare, casualty, capability or safeguarding information needed	To coordinate a search, emergency response, care, safeguarding or safe handover	Article 6(1)(ea): recognised legitimate interests, where sharing is necessary to safeguard a vulnerable person or respond to a stated public-task request. Any special category condition is identified before sharing	Kept only in the related record for the period shown above; recipients apply their own retention rules
Run governance, finance, tax, insurance, audit and legal claims	Trustee, meeting, donation, payment, Gift Aid, invoice, claim and correspondence records	To run the charity properly and meet our obligations	Article 6(1)(c), Article 6(1)(b) where a contract applies, and Article 6(1)(f). Article 9(2)(f) may apply to legal claims	Finance and donation records: 7 years. Meeting minutes and core governance records: permanent. Claims: 7 years after final resolution
Administer donations and supporter relationships	Name, contact details, donation, payment status, Gift Aid, preferences and correspondence	To process your donation, thank you and keep accurate charity records	Article 6(1)(b), Article 6(1)(c) and Article 6(1)(f)	Donation records: 7 years. Supporter correspondence: 3 years after last contact
Send fundraising or other electronic marketing	Name, email address, mobile number, interests, consent and opt-out records	To tell interested people about SusSAR's charitable purposes and ways to support us	Article 6(1)(a) consent, or Article 6(1)(f) where the charitable soft opt-in applies; see section 8	Until you withdraw consent or opt out. We keep a minimal suppression record for 7 years
Answer enquiries, feedback, complaints and rights requests	Name, contact details, your message, identity evidence, relevant records and outcome	To reply fairly, improve our work, demonstrate compliance and manage claims	Article 6(1)(c) and Article 6(1)(f). Article 9(2)(f), or another suitable condition, where necessary	3 years after closure. Legal claims: 7 years after final resolution
Run our website and protect our systems	Browser, device and cookie information, IP address, pages visited, account details where applicable, and security logs	To provide a secure, reliable website, understand use and prevent misuse	Article 6(1)(f): security and service improvement. Consent is used for non-essential cookies where required	Cookie periods are shown in our cookie controls. Security logs: normally 12 months. Website correspondence: 3 years

What we do	What information	Why	Our lawful basis	How long we keep it
Run training and use photographs, video, quotations or stories	Attendance, competence records, images, video, voice, quotations and stories	To train safely and, where agreed, tell the public about our work	Article 6(1)(f) for training and competence. We seek Article 6(1)(a) consent for identifiable publicity. Explicit Article 9(2)(a) consent is required if publicity reveals special category information	Training records: membership plus 3 years. Publicity material: until consent is withdrawn or the campaign ends; consent record: 6 years

2.2 Information about casualties and people we search for

We collect only what is needed to protect someone, search safely, give immediate assistance, record SusSAR's own activity and hand over care. This can include identity, location, description, safety or health information, observations and search findings. Many searches are requested by the police; see section 5. We do not use identifiable operational information for publicity, fundraising, research, statistics or training without proper authority and a further lawful assessment.

2.3 Photography, video, drones and body-worn cameras

We may use photography, video, drones or body-worn cameras in search activity or training. We assess necessity, privacy, access, security, retention and public awareness, and complete an impact assessment where required.

We seek specific consent before using an identifiable image, video, voice, quotation or story for publicity. You can withdraw consent. We will stop new use as soon as reasonably practicable, but may not retrieve material already printed or independently republished. We do not use identifiable operational material for publicity without the police force's written authority and any other consent required, or use retrospective facial recognition on police-originated images.

3. Who we share information with

3.1 Our sharing approach

We share information only when it is necessary, the recipient has a proper reason to receive it, and safeguards are in place. We share the minimum needed. We do not sell your information or give it to others for their unrelated marketing.

Depending on the reason, we may share information with:

- police forces we assist, including Sussex Police and Surrey Police;
- other Lowland Rescue and search and rescue teams;
- ambulance services and other emergency services;
- safeguarding partners;
- SARSTUFF Limited, which provides our Sarsys and Sarsys-Teamsite systems;
- Microsoft, which provides our IT services; and
- professional advisers, such as insurers, accountants, auditors and legal advisers.

We have written agreements in place with, or are putting appropriate written agreements in place with, each provider or partner where they handle information for us. Regular sharing relationships are supported by written arrangements. For a genuinely one-off sharing need, we document the reason, safeguards and case details.

We may also share information with banks, payment and fundraising providers, training or qualification bodies, Lowland Rescue, regulators, tax authorities, courts and tribunals where necessary. We will share information where the law requires it or where it is needed to protect someone from serious harm.

3.2 International transfers

We do not transfer your personal information outside the United Kingdom. If that position changes, we will tell you before the transfer and use the required protection.

4. Keeping information safe

We use proportionate safeguards including access controls, multi-factor authentication, encryption, device security, secure disposal and training. Access is limited to people who need the information for their role.

If we become aware of a personal data breach, we will investigate, contain it and meet notification duties. We do not make solely automated decisions about you with legal or similarly significant effects.

5. Police-originated information

5.1 The police force is the controller

When SusSAR searches at a police force's request, we may receive information about a missing person, casualty, family member, witness or another person. It can include identity, contact, description, location, vulnerability, health or safety information, images, intelligence and search records.

For this information, **the originating police force is the controller**. SusSAR handles it **on behalf of the police force** and follows its instructions. We do not decide a new purpose or use it for SusSAR's charitable activities.

Our minimum-necessary attendance, resource, safety and operational logs are SusSAR records. Police briefing material, intelligence and case information remain police information.

5.2 Requests, corrections and complaints about police information

If your request concerns police-originated information, contact the originating police force through its published data-protection, information-rights or subject-access route.

If you send it to us, we will forward it without delay, record the referral and assist the force where appropriate. We will not answer it as controller. For correction, deletion or restriction requests, we will notify the force within two working days. The force may lawfully limit information to protect an investigation, public safety or another person's rights. If you are unsure which force holds it, email DPA@sussar.org and we will help identify the referral route.

6. Your rights for SusSAR information

6.1 Your rights

For information that SusSAR controls, you have rights to:

- be told how we use your information;
- ask for access to your information;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information where the law allows;
- ask us to restrict use while an issue is checked;
- object to processing based on legitimate interests;
- receive information you gave us in a portable format in limited circumstances; and
- withdraw consent at any time, where we rely on consent.

You have an absolute right to object to direct marketing. We will stop sending it. Stopping marketing does not stop essential operational, safety, membership, donation-administration or legal messages.

6.2 How to make a request

Email **DPA@sussar.org**, write to our registered office, or make your request clearly to any SusSAR member. No special form is needed. We may ask for proportionate proof of identity to protect your information.

We normally respond within one month. We may extend this by up to two further months for a complex or numerous request, and will tell you within the first month. If a broad request needs clarification, the one-month period pauses from the day we ask until the day after you reply. This is the Article 12A UK GDPR clarification rule. We make reasonable and proportionate searches.

Some rights are not absolute. We may need to retain information for a legal duty, safeguarding, accounting, insurance, a legal claim or another person's rights. If we cannot do what you ask, we will explain why and how to complain.

7. Complaints

7.1 Complain to SusSAR

You can complain directly to SusSAR about how we have used your information. Use our online data protection complaint form or email **DPA@sussar.org**. You can also write to our registered office marked for the Data Protection Advocate.

For complaints received on or after 19 June 2026, this is our route under section 164A of the Data Protection Act 2018. We will acknowledge your complaint within 30 days, investigate it without undue delay, keep you informed of progress and tell you the outcome.

7.2 Complain to the ICO

You can complain to the Information Commissioner's Office at any time. You do not have to use SusSAR's complaint process first.

ICO helpline: **0303 123 1113**

ICO website: **ico.org.uk/make-a-complaint**

For a complaint about police-originated information, you may complain to the originating police force and to the ICO. We will cooperate with the force but cannot overturn its decisions or disclose its information independently.

8. Website cookies, marketing and children

8.1 Cookies and analytics

Our website uses cookies and similar technologies. Some are necessary for the website to work or to keep it secure. Others may help us understand how people use the website. We ask for your consent before placing non-essential cookies, including analytics cookies, where this is required. You can change your choice through our cookie controls. Blocking some cookies may affect how the website works.

8.2 Marketing

We send electronic fundraising or marketing messages only where the rules allow it. This is normally with your consent.

We may use the charitable soft opt-in only if we received your contact details directly on or after **5 February 2026**; you expressed interest in, offered, or gave support for SusSAR's charitable purposes; the message only furthers those purposes; and we offered a clear opt-out when we collected your details and in every message. We do not apply this to details collected before that date or received from a third party.

Every marketing message gives you a simple, free way to opt out. We keep a limited record of your opt-out so that we can respect it.

8.3 Children and young people

We may hold information about children and young people. We collect only what we need and give extra weight to their interests in our decisions about collection, sharing, security and retention. Where a child needs privacy information, we aim to make it concise, prominent and age-appropriate. Please contact us if you need this notice in a format suitable for a child or young person.

9. Changes to this notice

We review this notice at least annually and sooner if our processing, systems, services, legal duties or risks change. We will make material changes available through an appropriate channel.

You can ask the Data Protection Advocate for this notice in an accessible format or for help understanding it.