



Data Protection & Privacy Policy

At Abby's Heroes, we are committed to protecting your personal information and being open about when and why we collect it, how we use it, the conditions under which we may share it with others, how we keep it safe and secure, and your rights and choices in relation to your information.

If you have any questions regarding this policy, please contact our Data Protection Officer, Sally Randall by email info@abbys-heroes.org or by telephone on 07555 908 385.

Changes to this privacy notice

We keep our privacy notice under regular review. This privacy notice was last updated on 19th January 2023.

Who we are

Abby's Heroes is a registered charity in England and Wales under charity number 1170676:

(<https://register-of-charities.charitycommission.gov.uk/charity-search/-/charity-details/5092569>).

We are also register with the Fundraising Regulator:

(<https://www.fundraisingregulator.org.uk/directory/abbys-heroes>).

Our registered address is Basepoint Southampton, Unit 18, Andersons Road, Southampton, SO14 2FE.

This Privacy Policy relates to information which is obtained by Abby's Heroes and for which Abby's Heroes is the Data Controller and the Data Processor. This means that we decide on when, what, how, and why the data is collected and used.

When and how we collect data

From the first moment you interact with Abby's Heroes, we are collecting data. Sometimes you provide us with data, sometimes data about you is collected automatically.

Here's when and how we do this:

- ★ You browse any page of our website or social media
- ★ One of our Abby's Heroes Family Support Workers contacts you directly
- ★ You complete our Patient Form
- ★ A Social Worker (such as from Young Lives vs Cancer) or other party shares your information with us with your consent
- ★ You contact us directly (via the website, email, telephone, at an event, or other way)
- ★ You opt-in and consent to direct marketing messages
- ★ You purchase any of our merchandise from our online shop
- ★ You fundraise or volunteer for us
- ★ You attend an Abby's Heroes event
- ★ You donate to Abby's Heroes



The data we collect is different depending on our relationship with you, for instance, whether you are a supporter of Abby's Heroes, a member of the Abby's Heroes team, or a family we are providing help to.

What information we collect



Personal Data & Contact Details

- Name, Age, Date of Birth
- Address, Telephone Number, Email Address



Financial Information

- Bank Account (Account number & sort code), credit or debit card details
- NOTE: *Payment details will be deleted from our system as soon as the payment is processed. A record of the transaction will be kept in accordance with our legal obligations.*



Sensitive Data

- Medical Condition/Diagnosis, Treatment, Medical Status, Religion, Ethnicity
- NOTE: *Sensitive information will ONLY be collected in relation to our families (not our supporters).*



Relevant Information

- Information about you and your family, family status and personal circumstances, siblings, working or education status, benefit allowance status, marital status, consultant name, hospital ward location
- NOTE: *This information will only ever be collected where it is required for us to process an Abby's Heroes Grant application or other Abby's Heroes service.*



Identifying Electronic Data

- Your IP address, login information, browser type and version, time zone setting, browser plug-in types, geolocation information about where you might be, etc.



Website Use

- Your URL clickstreams (the path you take through our site), products/services viewed, page response times, download errors, how long you stay on our pages, what you do on those pages, how often, and other actions



Why we collect this information

The information which you provide to us, along with other information relating to you, will be held by Abby's Heroes, and used for the following purposes, and under specific lawful basis or lawful reasons.

The law allows for different ways to legally process personal data (and additional ways for sensitive personal data, such as medical information). Only some of these are relevant to how we process data:

1. Your consent (for example, to send you direct marketing by email or SMS).
2. Your explicit consent (for example, to process sensitive personal information for the Abby's Heroes Grant applications).
3. A contractual relationship (for example, to provide you with goods or services that you have purchased from us).
4. Processing that is necessary for compliance with a legal obligation (for example to process a Gift Aid declaration or carrying out due diligence on large donations).
5. Our legitimate interests.

Legitimate Interests

Personal data may be legally collected and used if it is necessary for a **legitimate interest** of the Abby's Heroes, if its use is fair and does not adversely impact the interests, rights and freedoms of the individual concerned.

When we use your personal information, we will always consider if it is fair and balanced to do so and if it is within your reasonable expectations. We will balance your rights and our legitimate interests to ensure that we use your personal information in a reasonable way. Our legitimate interests include:

- ★ Charity Governance: including the delivery of our charitable purposes, statutory and financial reporting and other regulatory compliance purposes, and transfers of data to those required to be involved in order to carry out those purposes.
- ★ Administration and operational management: including responding to solicited enquiries, providing information and services, research, data analytics, events management, the administration of volunteers and employment, and recruitment requirements.
- ★ Fundraising and Campaigning: including administering campaigns and donations and sending direct marketing by post (and in some cases making marketing calls) and maintaining communication.
- ★ Gifts in Wills: If you have notified us that you intend to leave a legacy in your Will to Abby's Heroes, we will continue to communicate with you until we are informed otherwise.

Our Families Information

We hold and process our families information:

PURPOSE	LAWFUL BASIS
★ For the purposes of making Charity Grants for applicants	Explicit Consent in relation to the processing of sensitive information Legitimate Interests Processing is carried out to meet contractual obligations or in order to enter into a contract



	legal obligation (for example, charitable records)
★ For processing an Abby's Heroes Grant applications and making payments for successful applications	Legitimate Interests Processing is carried out to carry out to meet contractual obligations or in order to enter into a contract legal obligation (for example, charitable records)
★ To provide information and access to support	Legitimate Interests
★ To keep a record of who we have helped, applications made, and charity grants processed.	Legitimate Interests Processing is necessary for compliance with a legal obligation (for example, charitable records)
★ For internal record keeping	Legitimate Interests and Processing is necessary for compliance with a legal obligation (for example, charitable records)

Supporters Information

We hold and process supporters' personal data:

PURPOSE	LAWFUL BASIS
★ To keep a record of donations made and actions taken by our supporters and our communications with them.	Legitimate Interests Processing is necessary for compliance with a legal obligation (for example, financial records)
★ To send our supporters marketing information about our projects, fundraising activities, and events where we have your consent or are otherwise allowed to.	Your Consent is required to for us to send you marketing. You can opt-out of this at any time.
★ To support volunteers participating in fundraising events.	Legitimate Interests
★ To record campaigning actions by supporters.	Legitimate Interests
★ To support community-based fundraising and campaigning.	Legitimate Interests
★ To claim gift aid on donations and receiving donations.	Processing is necessary for compliance with a legal obligation (for example to process a Gift Aid declaration, and carrying out due diligence on large donations)
★ To fulfil contractual obligations entered with supporters e.g., online purchases.	Processing is carried out to carry out to meet contractual obligations or in order to enter into a contract



★ To keep people safe, whether they are visitors, staff, or participants in events.	Processing is necessary for compliance with a legal obligation (for example, health and safety)
★ To comply with legal obligations.	Processing is necessary for compliance with a legal obligation (for example, in relation with our charitable status)
★ To manage our organisation.	Legitimate Interests
★ For internal record keeping	Legitimate Interests Processing is necessary for compliance with a legal obligation (for example, charitable records)

Trustees, Staff and Volunteers

In addition to the information in this privacy notice, there are some individuals whose personal data is used for specific purposes that are covered by other privacy statements:

Trustees

We process the personal details of Trustees to comply with our legal obligations, to comply with the requirements of the Charity Commission, and to keep in regular contact.

We maintain a list of Retired Trustees for the purposes of keeping in touch with newsletters and invitations to events.

We are sometimes required to provide Trustee information to third parties in line with our legal obligations and legitimate business interests (such as, opening a bank account, or agreeing to a new office lease).

Staff

As part of any recruitment and joining process, Abby's Heroes collects and processes personal data relating to job applicants.

Once you have taken up employment with Abby's Heroes, we will supply you with more details on the use and storage of your data.

Volunteers

There are a wide range of volunteering roles at Abby's Heroes. For any potential volunteering opportunities where you complete an application form you will need to supply personal data for purposes such as gathering references and to ensure we are able to support you well while you are volunteering. We will provide you with more details on the use and storage of your data during the application process and, if you take up a volunteer role, through your induction pack.



People who use our online services

We hold the details of the people who have requested our services so we can provide them. However, we only use these details to provide the service the person has requested. When people do subscribe to our services, they can cancel their subscription at any time and are given an easy way of doing this.

Electronic Communications

To those who subscribe to our mailing list (including our families and supporters), we send out regular e-newsletters, details of upcoming events, and other useful local updates and information.

We use a third-party service, MailChimp, to manage this. We may gather statistics around email opening and clicks using industry standard technologies including clear gifs to help us monitor and improve our e-newsletters. For more information, visit www.mailchimp.com/legal/privacy/

People who contact us via social media

We manage our social media interactions via Facebook, LinkedIn, Twitter, and Instagram. If you send us a private or direct message via social media, the message may be stored by the social media website as per their privacy policy. It will not be shared with any other third party by us. To view their privacy policies, visit:

- ★ Facebook - www.en-gb.facebook.com/full_data_use_policy
- ★ LinkedIn - <https://www.linkedin.com/legal/privacy-policy>
- ★ Twitter - <https://twitter.com/en/privacy>
- ★ Instagram - https://help.instagram.com/519522125107875/?helpref=uf_share

People who email us

Any email sent to us, including any attachments, may be monitored, and used by us for reasons of security and for monitoring compliance with office policy. Email monitoring or blocking software is also used. Please be aware that you have a responsibility to ensure that any email you send to us is within the bounds of the law.

People who message us via our websites contact form

We use a third-party provider, Mailgun, to manage our email traffic from our website. Mailgun is a company based in the USA, but Mailgun participates and has certified its compliance with the EU-U.S. Privacy Shield Framework.

If you send us a direct message via the website, the message will be stored by Mailgun temporarily. It will not be shared with any other organisations or third parties. For more information about how Mailgun processes data, please see their Privacy Policy here: <https://www.mailgun.com/privacy-policy>

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst



visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Events & Online Shop

We regularly hold fundraising and charity events. We do not currently use any booking platforms to manage this but do use SumUp to manage card payments during the event. You can read their privacy policy here: <https://www.sumup.com/en-gb/general-privacy-policy/>

Payments for the Merchandise we sell through our online shop are processed using Zapper <https://www.zapper.com/privacypolicy/> or PayPal [PayPal](https://www.paypal.com/myaccount/privacy/privacyhub) (<https://www.paypal.com/myaccount/privacy/privacyhub>).

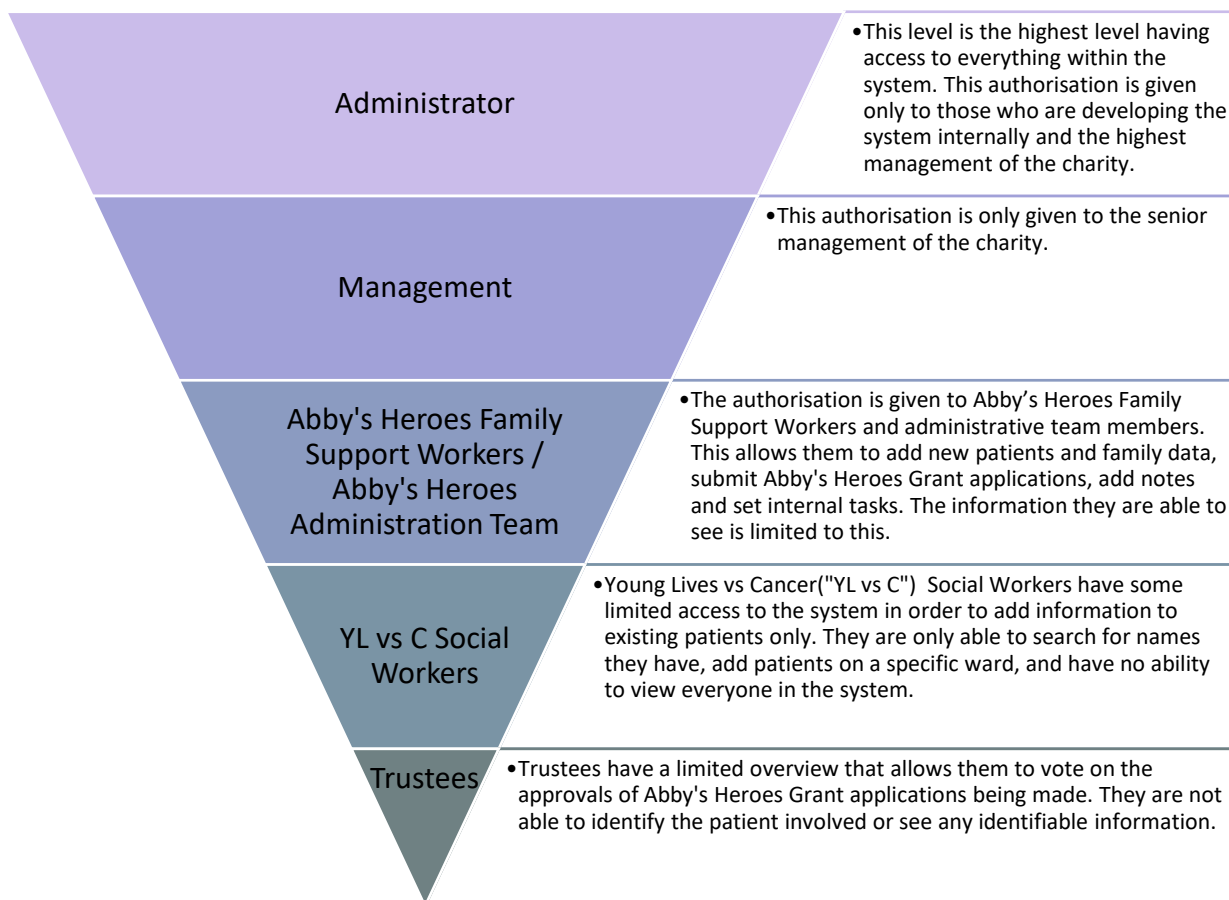
How we look after your data

We ensure that there are appropriate technical controls in place to protect your personal details in accordance with current data protection legislation; this includes secure cloud servers, firewalls, and SSL encryption. We follow payment card industry (PCI) security compliance guidelines when processing credit card payments and personal information transferred between locations will be encrypted and password protected.

Patient Management System

We have a purpose-built cloud-based system that allows us to manage our relationships with our families, and the support we are providing. It allows us to process the required data efficiently and securely for Abby's Heroes Grant applications and manage our support effectively.

Access to this system is restricted. Users are only permitted access to specific areas of the system, and are only able to view the data within it in accordance with their user access level.



The data stored in our system is only kept in line with our retention policy. Patient information in particular will be anonymised after 5 years from the last date of treatment.

We retain some information and data (anonymised) for statistical research and our own archival records. No identifying data is used for this purpose.

How long we keep your data

We keep your data for no longer than necessary for the purposes for which it was collected, considering guidance issued by the Information Commissioner's Office (ICO).

The length of time that data will be kept depends on the reasons for which we are processing the data as well as any applicable or regulations that the information falls under, such as financial regulations, Health and Safety regulation etc., or any contractual obligation we might have – such as local government contracts.

For example, we will keep a record of donations subject to gift aid for six years to comply with HMRC rules.



Legacy income is vital to the running of the charity. So, we can carry out legacy administration and communicate effectively with the families of people leaving us legacies, we will keep the data you provide us for the long term. This also enables us to identify and analyse the source of legacy income we receive.

If you request to receive no further contact from us, although we will act on that, we will keep some basic information about you on our suppression list to enable us to comply with your request.

Below is a summary of our data retention schedule.

DATA TYPE	RETENTION PERIOD
Bank or Card Payment Details	Deleted as soon as the transaction is completed.
Payment Transaction Records / Financial and account records / Donations / Gift Aid claims	6 years
Website analytics	7 years
Grant applications	6 years after grant completion
Patient Information	10 years from start of treatment or until the child reaches 18 years of age 6 years from date of death
Employee/Volunteer application forms, CV's	Successful – 7 years after engagement (employees), 1 year after engagement (volunteers) Unsuccessful – 6 months
Employee/Volunteer Personnel file – non-essential elements	7 years after engagement (employees) 1 year after engagement (Volunteers) Indefinitely (limited record of employees)
Trustees contact information, public details	1 year after Trustee's role end
Trustees essential contact information	Indefinitely
Emails/communication records	As soon as possible (maximum 5 years)
Legacy Details	Until probate has been completed

Security and performance

We are committed to ensuring that your information is secure. To prevent unauthorised access or disclosure, we have put in place suitable physical, electronic, and managerial procedures to safeguard and secure the information we collect online and in completing our services to you.

We process any personal data identified in this Policy where it is deemed necessary for the purposes of maintaining insurance coverage, managing risks, obtaining professional advice, or establishing, exercising, or defending legal claims, we do this for the proper protection of our charity. We also process such data where processing is required to comply with a legal obligation to protect yours or another person's vital interests.

How secure is the data we collect?

We have physical, electronic, and managerial procedures to safeguard and secure the information we collect.

And please remember:



- You provide personal data at your own risk: unfortunately, no data transmission is guaranteed to be 100% secure
- You are responsible of your username and password: keep them secret and safe!
- If you believe your privacy has been breached, please contact us immediately on **07555 908 385** or info@abbys-heroes.org

Use of Third Parties

As part of our services to you, and in the day to day running of our charity, we use some third-party support or software. Before contracting with any supplier, we review their data protection policies and processes to ensure that your (and our) data will be suitably protected when processed by them and assess where their data is stored.

The legal basis for processing this data is both our legitimate business interests, namely the proper administration of our charity, consent, or the performance of a contract between us and/or taking steps, at your request, to enter such a contract.



Microsoft 365

We use Microsoft 365 to manage all our email communications and we use SharePoint to store our electronic files and data. You can review their privacy policy [here](https://www.microsoft.com/online/legal/v2/?docid=43): <https://www.microsoft.com/online/legal/v2/?docid=43>



Xero Accounting

We use Xero for our own accounting software. Xero take their responsibilities under GDPR seriously. That's why they've embarked on a programme to identify which measures they need to implement to be compliant with GDPR. You can read more about their privacy processes [here](https://www.xero.com/uk/about/terms/privacy/): <https://www.xero.com/uk/about/terms/privacy/> and <https://www.xero.com/uk/gdpr/>



Mailgun

Mailgun is used within our Patient Management System to control and manage transactional emails within the system. <https://www.mailgun.com/legal/privacy-policy/>



Mailchimp

We use MailChimp to manage our email marketing, consent to receive marketing and our unsubscribe process. <https://www.intuit.com/privacy/statement/>



DocuSign

DocuSign is used by Abby's Heroes to seek consent from our families to process information to order to support them in submitting Abby's Heroes Grant applications and our other services. DocuSign has adopted Binding Corporate Rules to facilitate the transfer of personal information from the European Economic Area and/or United Kingdom ("EEA") to DocuSign outside of the EEA. Read more [here](#):



<https://www.docusign.co.uk/en-gb/privacy/>

<https://www.docusign.co.uk/en-gb/legal/terms-and-conditions/>



Amazon S3

Amazon S3 or Amazon Simple Storage Service is a service offered by Amazon Web Services that provides object storage through a web service interface. We use this to save backups of our Patient Management System.

https://aws.amazon.com/privacy/?nc1=f_pr



Digital Ocean

Our Patient Management System utilises the cloud-based servers through Digital Ocean. These servers are UK based.

<https://www.digitalocean.com/legal/privacy-policy>



JustGiving

We use JustGiving to fundraise and manage our online donations.

<https://www.justgiving.com/about/info/privacy-policy/privacy-policy-v30>

Where do we store the data?

The personal data we collect is processed at our offices in Southampton and in any data processing facilities operated by the third parties identified above.

By submitting your personal data, you agree to the transfer, storing, and processing by us. If we transfer or store your information outside the EEA in any way, we will take steps to ensure that your privacy rights continue to be protected as outlined in this Privacy Policy.

How we monitor our data security

Abby's Heroes is committed to ensuring the security of your Personal Data. Your information is stored using appropriate technical and organisational measures to ensure its security, we monitor this by:

- ★ regular review of security measures of all data storage systems and emerging security risks
- ★ regular training of Charity staff that access the information. We keep your personal information in accordance with our Retention Policy, which considers:
 - the purpose(s) for which the information was collected and how long we need to keep the information to achieve the purpose
 - any applicable legal, accounting, reporting or regulatory requirements to keep the information.

Transferring your information out of the UK

We may transfer your Personal Data out of the UK where our service providers referred to above are based outside or have servers outside the UK. Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring one of the following safeguards is implemented:



- ★ We ensure that the country we are transferring the data to has been deemed under UK data protection laws to provide an adequate level of protection for Personal Data.
- ★ If the country has not been deemed to provide an adequate level of protection, we use specific contracts approved for use under UK data protection laws which give Personal Data an equivalent level of protection as it has in the UK.

Visitors to our website or social media

If you browse, read pages, or download information from our website, we will gather and store certain limited information about your visit. This information collected or stored is used by us only for the purpose of improving the content of our web services and to help us understand how people are using our services.

Google Analytics

Our website uses Google Analytics, a web analytics service provided by Google, Inc. ('Google'). Google Analytics uses cookies (text files placed on your computer) to help the website operators analyse how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States.

Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. If you do not wish for your data to be processed this way, please do not enter our website.

Google Analytics automatically collects and stores the following information about your visit:

- ★ The Internet Protocol (IP) address and domain name used. The IP address is a numerical identifier assigned either to your internet service or directly to your computer. We use the IP address to direct internet traffic to you. This address can be translated to determine the domain name of your service provider (e.g., abccompany.com, xyz-school.edu, and so on)
- ★ The type of browser and operating system you used
- ★ The date and time you visited this site
- ★ The web pages or services you accessed at this site; and
- ★ The website you visited prior to coming to this site.

The legal basis for processing this data is both our legitimate business interests, namely monitoring and improving our website and services.

Use of cookies

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used to make websites work, or work more efficiently, as well as to provide information to the owners of the site.



You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website. To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit www.aboutcookies.org or www.allaboutcookies.org. To opt out of being tracked by Google Analytics across all websites visit <http://tools.google.com/dlpage/gaoptout>.

Complaints and queries

Abby's Heroes tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading, or inappropriate. We would also welcome any suggestions for improving our procedures.

This privacy notice was drafted with brevity and clarity in mind. It does not provide in exhaustive detail of all aspects of Abby's Heroes collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below.

People who make a complaint to us

When we receive a complaint from a person, we make up a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint.

We will only use the personal information we collect to process the complaint and to check on the level of service we provide. We do compile and publish statistics showing information like the number of complaints we receive, but not in a form which identifies anyone.

We usually need disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis.

We will keep personal information contained in complaint files in line with our retention policy. This means that information relating to a complaint will be retained for two years from closure. It will be retained in a secure environment and access to it will be restricted according to the 'need to know' principle.

Similarly, where enquiries are submitted to us, we will only use the information supplied to us to deal with the enquiry and any subsequent issues and to check on the level of service we provide.

Access to personal information

Abby's Heroes tries to be as open as it can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request' under the Data Protection Act 2018 and subsequent legislation. If we do hold information about you, we will:



- ✓ give you a description of it;
- ✓ tell you why we are holding it;
- ✓ tell you who it could be disclosed to; and
- ✓ let you have a copy of the information in an intelligible form.

To make a request to Abby's Heroes for any personal information we may hold you need to put the request in writing addressing it to our Data Protection Officer at our registered office or emailing it to the address provided below.



Sally Randall

Email:
info@abbys-heroes.org

Telephone:
07555 908 385.

Address:
Data Protection Officer,
Basepoint Southampton,
Unit 20, Andersons Road,
Southampton, SO14 2FE

If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need. You will be asked for proof of your identity before we are able to provide you with the information requested.

We will provide you with the information within one month of your request, unless doing so would adversely affect the rights and freedoms of another (e.g., another person's confidentiality). We'll tell you if we can't meet your request for that reason.

Controlling your personal information

- We will not sell, distribute, or lease your personal information to third parties unless we have your permission or are required by law to do so.
- You may request details of personal information which we hold about you under the Data Protection Act 2018 and UK GDPR.
- If you believe that any information, we are holding on you is incorrect or incomplete, please write to or email us as soon as possible, at the above address. We will promptly correct any information found to be incorrect.



Your rights

You have specific rights under data protection legislation. You can exercise these rights by emailing us. Please visit the Information Commissioners Office website to learn all about the rights you have: <https://ico.org.uk/for-the-public/>



Right to be Informed

- Transparency over how we use your personal information
- This privacy notice, as well as any additional information that is provided to you either at the time you provided your details, or later, is intended to provide you with this information.



Right of Access

- Request a copy of the information we hold about you – this is sometimes called a data subject access or data subject request. We will supply requested information that we hold about you as soon as possible, but this may take up to 30 days. We will not charge you for this other than in exceptional circumstances. You will be asked for proof of identity for us to do this.



Right of Rectification

- Update or amend the information we hold about you if it is wrong



Right to Restrict Processing

- Ask us to stop using your information
- In certain situations, you have the right to ask for processing of your personal data to be restricted because there is some disagreement about its accuracy or legitimate usage.



Right to be "Forgotten"

- Ask us to remove your personal information from our records
- Note: where you have requested that we do not send you marketing materials, we will need to keep some limited information to ensure that you are not contacted in the future



Withdraw Consent

- Where we process your data based on your consent (for example, to send you marketing texts or emails), you can withdraw that consent at any time.



Right to Object

- Object to the processing of your information for marketing purposes
- ★ You also have a right to object to us processing data where we are relying on it being within our legitimate interests to do so (for example, to send you direct marketing by post).



Right to Data Portability

- Obtain and reuse your personal data for your own purposes



Rights relating to Automated Decisions & Profiling

- Not be subject to a decision when it is based on automated processing