GAIN Policy

Data Protection

Introduction

We hold personal data about our employees, clients, suppliers and other individuals for a variety of charitable purposes. This policy sets out how we seek to protect personal data and ensure that staff, trustees and volunteers understand the rules governing their use of personal data to which they have access.

Definitions

Charity purposes The purposes for which personal data may be used by us:

- To process a donation you have made
- To process orders that you have submitted
- To carry out our obligations arising from any contracts entered into by you and us
- Dealing with entries into a competition
- Seeking you views or comments on the services we provide
- Notifying you of changes to our services
- Sending you communications which you have requested and that may be of interest to you
- Process a grant or job application

Personal data - Information relating to identifiable individuals, such as job applicants, current and former employees, trustees, volunteers, members, patients, Medical Advisors, suppliers and donors. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Sensitive personal data Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all staff, trustees and volunteers. You must be familiar with this policy and comply with its terms. This policy supplements our other policies. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated after being adopted.

Who is responsible for this policy?

The Data Protection Officer, Caroline Morrice has overall responsibility for the day-to-day implementation of this policy.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Ensuring understanding of the policy and provision of training as required
- Answering questions on data protection
- Responding to individuals requesting a copy of the data held on them
- Checking and approving with third parties that handle the charity's data any contracts or agreement regarding data processing
- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Privacy Notice
Our Website contains a Privacy Notice to clients on data protection which:

- Sets out the purposes for which we hold personal data
- Highlights that our work may require us to give information to third parties
- Provides information on the right of access to the personal data that we hold about them

Sensitive personal data
In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Caroline Morrice

Your personal data
You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security
You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- printed paper should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention
We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data outside of Europe
The information provided to GAIN may be transferred to countries outside the European Union (EU). By way of example, this may happen if any of our servers are from time to time located in a country outside of the EU. These countries may not have similar laws to the UK. By submitting your personal data, you are agreeing to this transfer, storing or processing. If we transfer your information outside the EU in this way we will take steps to ensure that appropriate security measures are taken with the aim of ensuring your privacy rights continue to be protected as outlined in this policy.
If you use our services while you are outside the EU, your information may be transferred outside the EU in order to provide you with those services.

Subject access requests
Please note that under the General Data Protection Regulation, individuals are entitled, subject to certain exceptions, to request access to information held about them.
If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.
Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights
GAIN will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

GAIN will not send direct marketing material to someone electronically (e.g. via email) unless an existing business relationship with them in relation to the services being marketed exists.

GDPR provisions

Privacy Notice - transparency of data protection

This Policy explains when and why we collect personal information about people, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We may change this Policy from time to time so please check this page occasionally to ensure that you're happy with any changes.

Any questions regarding this Policy and our privacy practices should be sent by email to caroline.morrice@gaincharity.org.uk or by writing to Freepost RTHK-KGYY-LKYB, Guillain Barre & Associated Inflammatory Neuropathies, Woodholme House, Heckington Business Park, Station Road, Heckington, SLEAFORD NG34 9JH. Alternatively, you can telephone 01529 469910.

Who are we?

We're GAIN, the country's only charity dedicated to helping everyone affected by GBS, CIDP or one of the associated inflammatory neuropathies. GAIN is a registered charity (no. 1154843 & SCO39900). The registered address is Woodholme House, Heckington Business Park, Station Road, Heckington SLEAFORD NG34 9JH.

How do we collect information from you?

We obtain information about you when you contact us in writing, in person or use our website, for example, when you contact us about products and services, to make a donation, or if you register to receive our magazine.

What type of information is collected from you?

The personal information we collect might include your name, address, email address, IP address, and information regarding what pages are accessed and when. If you make a donation online or purchase a product from us, your card information is not held by us, it is collected by our third party payment processors, who specialise in the secure online capture and processing of credit/debit card transactions, as explained below.

How is your information used?

We may use your information to:

- process a donation that you have made;
- process orders that you have submitted;
- to carry out our obligations arising from any contracts entered into by you and us;
- dealing with entries into a competition;
- seek your views or comments on the services we provide;
- notify you of changes to our services;
- send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities, promotions of our goods and services;
- process a grant or job application.

We review our retention periods for personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations (for example the collection of Gift Aid). We will hold your personal information on our systems for as long as is necessary for the relevant activity, or as long as is set out in any relevant contract you hold with us.

Who has access to your information?

We will not sell or rent your information to third parties.

We will not share your information with third parties for marketing purposes.

Third Party Service Providers working on our behalf: We may pass your information to our third party service providers, agents subcontractors and other associated organisations for the purposes of completing tasks and providing services to you on our behalf (for example to process donations, handle direct debits and send you mailings). However, when we use third party service providers, we disclose only the personal information that is necessary to deliver the service and

we have a contract in place that requires them to keep your information secure and not to use it for their own direct marketing purposes. Please be reassured that we will not release your information to third parties for them to use for their own direct marketing purposes, unless you have requested us to do so, or we are required to do so by law, for example, by a court order or for the purposes of prevention of fraud or other crime.

Third Party Product Providers we work in association with: We work with various third party product providers to bring you a range of quality and reliable products.

When you are using our secure online donation pages, your donation is processed by a third party payment processor, who specialises in the secure online capture and processing of credit/debit card transactions. If you have any questions regarding secure transactions, please contact us.

We use a mailing house to print and distribute bulk mailings such as the magazine. They undertake not to use or sell your data.

Your choices

You have a choice about whether or not you wish to receive information from us. If you do not want to receive direct marketing communications from us about the vital work we do for people affected by GBS, CIDP and the associated inflammatory neuropathies and our exciting products and services, then you can select your choices by ticking the relevant boxes situated on the form on which we collect your information.

We will not contact you for marketing purposes by email, phone or text message unless you have given your prior consent. We will not contact you for marketing purposes by post if you have indicated that you do not wish to be contacted. You can change your marketing preferences at any time by contacting us by email: office@gaincharity.org.uk or telephone on 01529 469910.

How you can access and update your information

The accuracy of your information is important to us. We're working on ways to make it easier for you to review and correct the information that we hold about you. In the meantime, if you change email address, or any of the other information we hold is inaccurate or out of date, please email us at: office@gaincharity.org.uk , or write to us at: Freepost RTHK-KGYY-LKYB, Guillain Barre & Associated Inflammatory Neuropathies, Woodholme House, Heckington Business Park, Station Road, Heckington, SLEAFORD NG34 9JH. Alternatively, you can telephone 01529 469910.

You have the right to ask for a copy of the information GAIN hold about you (we may charge £10 for information requests) to cover our costs in providing you with details of the information we hold about you.

Security precautions in place to protect the loss, misuse or alteration of your information

When you give us personal information, we take steps to ensure that it's treated securely. We do not hold information about your credit/cards as we use third party processors.

Non-sensitive details (your email address etc.) are transmitted normally over the Internet, and this can never be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you

to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Profiling
We may analyse your personal information to create a profile of your interests and preferences so that we can contact you with information relevant to you. We may make use of additional information about you when it is available from external sources to help us do this effectively. We may also use your personal information to detect and reduce fraud and credit risk.

Links to other websites
Our website may contain links to other websites run by other organisations. This privacy policy applies only to our website, so we encourage you to read the privacy statements on the other websites you visit. We cannot be responsible for the privacy policies and practices of other sites even if you access them using links from our website.

In addition, if you linked to our website from a third party site, we cannot be responsible for the privacy policies and practices of the owners and operators of that third party site and recommend that you check the policy of that third party site.

16 or Under
We are concerned to protect the privacy of children aged 16 or under. If you are aged 16 or under, please get your parent/guardian's permission beforehand whenever you provide us with personal information.

Transferring your information outside of Europe
As part of the services offered to you through this website, the information which you provide to us may be transferred to countries outside the European Union (“EU”). By way of example, this may happen if any of our servers are from time to time located in a country outside of the EU. These countries may not have similar data protection laws to the UK. By submitting your personal data, you’re agreeing to this transfer, storing or processing. If we transfer your information outside of the EU in this way, we will take steps to ensure that appropriate security measures are taken with the aim of ensuring that your privacy rights continue to be protected as outlined in this Policy.

If you use our services while you are outside the EU, your information may be transferred outside the EU in order to provide you with those services.

Criminal record checks
Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability
Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten
A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan. When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data audit and register
Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches
All staff, trustees, volunteers and members have an obligation to report actual or potential data protection compliance failures to the DPO. This allows GAIN:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring
Everyone must observe this policy. The DPO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply
We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Review of this Policy

We keep this Policy under regular review. This Policy was last updated in January 2018.