



Data Protection and Privacy Policy

Nonfiction Authors Association

Who we are

Our website address is: <https://nonfictionauthorsassociation.com>.

What personal data we collect and why we collect it

Comments

When visitors leave comments on the site we collect the data shown in the comments form, and also the visitor's IP address and browser user agent string to help spam detection.

An anonymized string created from your email address (also called a hash) may be provided to the Gravatar service to see if you are using it. The Gravatar service privacy policy is available here: <https://automattic.com/privacy/>. After approval of your comment, your profile picture is visible to the public in the context of your comment.

Media

If you upload images to the website, you should avoid uploading images with embedded location data (EXIF GPS) included. Visitors to the website can download and extract any location data from images on the website.

Cookies

If you leave a comment on our site you may opt-in to saving your name, email address and website in cookies. These are for your convenience so that you do not have to fill in your details again when you leave another comment. These cookies will last for one year.

If you have an account and you log in to this site, we will set a temporary cookie to determine if your browser accepts cookies. This cookie contains no personal data and is discarded when you close your browser.

When you log in, we will also set up several cookies to save your login information and your screen display choices. Login cookies last for two days, and screen options cookies last for a year. If you select "Remember Me", your login will persist for two weeks. If you log out of your account, the login cookies will be removed.

If you edit or publish an article, an additional cookie will be saved in your browser. This cookie includes no personal data and simply indicates the post ID of the article you just edited. It expires after 1 day.

Embedded content from other websites

Articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracing your interaction with the embedded content if you have an account and are logged in to that website.

Who we share your data with and how long we retain your data

If you leave a comment, the comment and its metadata are retained indefinitely. This is so we can recognize and approve any follow-up comments automatically instead of holding them in a moderation queue.

For users that register on our website (if any), we also store the personal information they provide in their user profile. All users can see, edit, or delete their personal information at any time (except they cannot change their username). Website administrators can also see and edit that information.

What rights you have over your data

If you have an account on this site, or have left comments, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we erase any personal data we hold about you. This does not include any data we are obliged to keep for administrative, legal, or security purposes.

Where we send your comment data

Visitor comments may be checked through an automated spam detection service.

Additional information

The Nonfiction Authors Association needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other

people the organization has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

The Nonfiction Authors Association discloses the following data collection policies:

- We utilize Constant Contact as our primary commercial email tool and rely on them to keep customer data secure.
- We occasionally offer free downloadable reports via Leadpages.net, which collects customer first and last name plus email address, and that data is automatically added to Constant Contact. These forms have a disclaimer indicating that the subscriber is providing consent.
- We process payments with Paypal and Square and rely on these respective vendors to keep customer data secure. We do NOT store any customer payment information on our websites or anywhere internally. All payment information is maintained by Paypal and Square. If a payment is processed manually by phone, payment information is immediately destroyed and not kept on file.
- We utilize Google Analytics to monitor website traffic and rely on this vendor to protect any data collected.
- As a membership organization, our members have the option to create public member profiles to share information about their books and where they can be reached. This is an opt-in program.
- Our website content is backed up daily and securely stored with Carbonite.
- We have additional security plugins on the site to prevent data hacking.
- We also have a team of web professionals who monitor the site and respond to server attacks and other occasional issues that are inherent with websites that receive a lot of traffic.
- All personal computers are protected by firewalls.
- We take data protection very seriously and have never rented or sold our mailing list or any kind of personal customer data, nor will we ever do so.

Why this policy exists

This data protection policy ensures The Nonfiction Authors Association complies with data protection laws, including GDPR, and follows good practices, protects the rights of staff, customers and partners, is open about how it stores and processes individuals' data, and protects itself from the risks of a data breach.

Data protection law

The Data Protection Act 1998, and GDPR, describe how organizations — including The Nonfiction Authors Association— must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To

comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

This policy applies to:

- The head office of The Nonfiction Authors Association
- All branches of The Nonfiction Authors Association
- All staff and volunteers of The Nonfiction Authors Association
- All contractors, suppliers and other people working on behalf of The Nonfiction Authors Association

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information shared by individuals

Data protection risks

This policy helps to protect The Nonfiction Authors Association from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive

Responsibilities

Everyone who works for or with The Nonfiction Authors Association has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Data Protection Officer, Stephanie Chandler**, is responsible for:

- Keeping internal staff updated about data protection responsibilities, risks and
- Reviewing all data protection procedures and related policies, in line with an agreed
- Arranging data protection training and advice for the people covered by this
- Handling data protection questions from staff and anyone else covered by this
- Dealing with requests from individuals to see the data The Nonfiction Authors Association holds about them (also called ‘subject access requests’).
- Checking and approving any contracts or agreements with third
- parties that may handle the company’s sensitive data.
- Approving any data protection statements attached to communications such as emails and
- Addressing any data protection queries from journalists or media outlets like
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection

The **IT manager for The Nonfiction Authors Association** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security
- Performing regular checks and scans to ensure security hardware and software is functioning
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, staff can request it from their managers.
- Staff should keep all data secure, by taking sensible precautions and following the guidelines
- In particular, **strong passwords must be used** and they should never be shared.

- Personal data **should not be disclosed** to unauthorized people, either within the company or
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed
- Staff **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller. When data is **stored on paper**, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorized people could see them**, like on a
- **Data printouts should be shredded** and disposed of securely when no longer required.
- When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:
- Data should be **protected by strong passwords** that are changed regularly.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office
- Data should be **backed up frequently**. Those backups should be tested
- regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to The Nonfiction Authors Association unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, staff should ensure **the screens of their computers are always locked** when left
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure
- Staff should not save copies of personal data to their own computers.
- Always access and update the central copy of any data.

Data accuracy

The law requires The Nonfiction Authors Association to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort The Nonfiction Authors Association should put into ensuring its accuracy.

It is the responsibility of all staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they
- The Nonfiction Authors Association will make it **easy for data subjects to update the information** The Nonfiction Authors Association holds about them. For instance, via the company
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database

Subject access requests

All individuals who are the subject of personal data held by The Nonfiction Authors Association are entitled to:

- Ask what information the company holds about them and
- Ask how to gain access to the data
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller. The data controller will always verify the identity of anyone making a subject access request before handing over any information.



Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, The Nonfiction Authors Association will disclose requested data.

Providing information

The Nonfiction Authors Association aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

The Nonfiction Authors Association is a division of Stephanie Chandler Enterprises, LLC. The above policy applies to our sister websites as well: NonfictionWritersConference.com, AuthorityPublishing.com, and StephanieChander.com.

To these ends, the company has published this privacy statement, setting out how data relating to individuals is used by the company. [Contact us](#) with any questions.