GDPR Privacy Policy

Last Updated: 22 March 2022

This Privacy Policy (the "Policy") describes the personal data that www.millennialpsychology.co.uk / Millennial Psychology Ltd. ("Millennial Psychology Ltd.", "we", "us" or "our") collects from or about you when you use website www.millennialpsychology.co.uk and related services (the "Services"), how we use that information, and to whom we disclose it. For the purposes of the Policy, the term "personal data" will have the same meaning as in EU General Data Protection Regulation 2016/679 ("GDPR") and California Consumer Privacy Act (CCPA).

This Policy should be read in conjunction with the Terms of Use, into which it is incorporated by reference.

We may modify this Policy from time to time. We will provide you with notice of any material changes to this Policy by publishing or communicate the changes through our Services or by other means so that you may review the changes before continuing to use our Services. Your continued use of the Services after we publish or communicate a notice about any changes to this Policy means that you are consenting to the changes.

In short, Millennial Psychology Ltd. stores and processes your personal data and your contacts' personal data solely to perform the services you have signed up for. We do not sell your information or use it for profiling secondary business objectives. The policies below describe this in greater detail.

1. Accountability and Openness/Compliance

Millennial Psychology Ltd. is responsible for personal data under our control. We have established policies and procedures to effectively safeguard any confidential personal data that we collect and to deal with complaints and inquiries. We are committed to maintaining the accuracy, confidentiality, and security of your personal data, and we will ensure that you have access to information regarding the policies and procedures that we use to manage your personal data. Millennial Psychology Ltd. has designated a Privacy Officer/Data Protection Officer ("Privacy Officer") who is accountable for our compliance with this Policy and for ensuring that information about our policies and practices relating to the management of personal data is easily accessible. All questions or concerns regarding this Policy and our compliance with it should be directed to the Privacy Officer in writing and sent by email or postal mail to:

Millennial Psychology Ltd.
2a Connaught Avenue, London, E4 7AA.
General Inquiries: info@millennialpsychology.co.uk
Website: www.millennialpsychology.co.uk

Every complaint or challenge regarding our compliance with this Policy will be investigated, and where a deficiency is found to exist, we will take appropriate measures to address it. This may include amending our policies and procedures as necessary. We will also cooperate with regulatory authorities to resolve any complaints that cannot be resolved between us and an individual user.

2. Consent

By using the Services, you signify your agreement to the terms and conditions of this Policy and to our collection, use and disclosure of your personal data as set out herein. You may change or withdraw your consent to the collection, use or disclosure of your personal data at any time by contacting the Privacy Officer in writing at the address listed above (see: Accountability and Openness/ Compliance). In some circumstances, a change or withdrawal of consent may affect your ability to use the Services.

3. Collection and Retention of Information

We collect personal data only to the extent that it is necessary for the purposes set out below (see: Purpose – Why We Collect, Use and Disclose Information). Subject to any legal or accounting requirements, we will retain personal data only as long as necessary to fulfill the purposes for which it was collected. Personal data that is no longer required will be destroyed, erased or made anonymous, although copies of deleted information may continue to exist on backup media. Information that we may collect includes:

User Submitted Information

We collect certain personal data at the time users register to create an account or update their account details including a user's name, e-mail address, and other contact information. We also collect personal data that users submit through their use of the Services, including when they submit contact and other information, they have collected from their email subscribers and when they create and send email campaigns.

Usage Data

We collect certain non-identifying information about the usage of the Services, including information about how users are using the Services and the characteristics of those users. This information is anonymized and is not used by us to identify you as an individual.

Account Deletion Requests

At any time, you can request to have your account data deleted by contacting us. Upon receiving the request, we will send you an email to confirm this request. After successful confirmation, your account will be marked for deletion in 30 days. During this 30-day period, you may request to have your account reactivated by contacting us. After 30 days your account is permanently deleted and cannot be reactivated. For more information about account deletion processes, please see the section called Data Retention Policy below. Account Inactivity To protect your privacy and your data, if your account is not active for a period of 1 year, it will automatically be permanently deleted. 30 days prior to this deletion, an email notification will be sent to the account email address with information about the deletion and instructions on how to keep the account active if desired. For more information about account deletion processes, please see the section called Data Retention Policy below.

Data Retention Policy

An account can be permanently deleted by either a deletion request or from account inactivity. We retain personal data only for as long as necessary to provide the Services you have requested and thereafter for a variety of legitimate legal or business purposes. These may include retention periods:

- needed to maintain adequate and accurate business and financial records
- for resolving, preserving, enforcing or defending our contractual/legal rights
- mandated by law, contract or similar obligations applicable to our business operations
- to protect recipients from spam or malicious emails

Technical and Device Information

We collect certain non-identifying information related to a user's access to the Services, including the Internet Protocol (IP) address of the user's computer, the date and time the user accessed the Services

and the operating system that the user is using. We make no attempt to link this information with the identity of individuals visiting our website without express permission. We may, however, review server logs and anonymous traffic for system administration and security purposes, for example, to detect intrusions into our network, for planning and improving web services, and to monitor and compile statistics about website usage. The possibility, therefore, exists that server log data, which contains users' IP addresses, could in instances of criminal malfeasance be used to trace and identify individuals. In such instances, we may share raw data logs with the appropriate authorities for the purpose of investigating security breaches.

Cookies and Web Beacons

A "cookie" is a small piece of information stored on your computer by a web page. It is used to identify you to the web server. It tells the server who you are when you return to a page on the same website. Your browser will only send a cookie back to the domain that originally sent it to you. A cookie cannot run any programs, deliver any viruses, or send back information about your system.

We use cookies to determine your access privileges on our websites, to complete and support a current activity, and to track website usage. Most web browsers automatically accept cookies, but if you do not wish to have cookies on your system, you should adjust your browser settings to decline them or to alert you when cookies are being sent. If you decline cookies, you will still be able to use the Services, but your ability to access certain features and functions may be affected.

As the means by which you can refuse cookies through your web browser controls vary from browser-to browser, you should visit your browser's help menu for more information. Here are the current relevant information pages for the main browsers:

Microsoft Internet Explorer: http://www.microsoft.com/info/cookies.htm
Google Chrome: https://support.google.com/accounts/answer/61416
Mozilla Firefox: http://www.mozilla.org/projects/security/pki/psm/help_21/using_priv_help.htm

A "web beacon" is an invisible electronic image that is used to track certain information. We use web beacons on our websites, in emails, we send to you and in emails, you send through the Services. The information gathered from the web beacons, such as who opened emails or clicked on links in the emails or on our websites, allows us to measure the success of email campaigns and to improve the Services.

4. Purpose – Why We Collect, Use and Disclose Information

We will identify the purposes for which we collect personal data before or when we request the information. We will not collect personal data which is not necessary and, except as specified below, will not use or disclose personal data for any purpose other than the purpose(s) for which it was collected without first obtaining your consent. The information that we collect is used and disclosed only for business purposes. This includes: • to enable you to access and use the Services;

- to process, track and communicate with you about the usage of the Services;
- to establish, maintain and manage business relations with you so that we may provide you with the information, products or services that you request;
- internal business purposes, such as administering or improving the Services;
- to perform internal market research and conduct polls and surveys;
- to obtain feedback regarding the Services and our ability to address a user's needs;

- to provide users with information and promotional materials regarding Millennial Psychology Ltd. products and services;
- to protect us against error, fraud, theft or damage to our goods, our business or our property;
- to comply with any legal, accounting and regulatory requirements, including reporting requirements, applicable laws, and any search warrants, subpoenas or court orders; and any other reasonable purpose for which you provide consent.

We may collect, use or disclose your personal data without your knowledge or consent where we are permitted or required to do so by applicable law, government request or court order, or based on our good faith belief that it is necessary to do so in order to comply with such law, request or court order, or to protect our assets, the users of our website, or the public.

5. Disclosure to Third Parties

We may disclose your personal data in response to requests from government agencies, law enforcement authorities, and regulators, or to satisfy legal or regulatory requirements. We may also disclose your personal data when we buy a business or sell all or part of our business.

You further acknowledge and agree that, in the course of providing the Services to you, we may delegate our authority to collect, access, use, and disseminate your information to third party subcontractors. Third party subcontractors may include web hosts, payment processors, delivery and logistics providers, social network integrators, and membership vendors. If we transfer any personal data to a third-party subcontractor, we will provide the subcontractors only with the information needed to perform the subcontracted service, and will use appropriate contractual or other means to provide a comparable level of protection while the information is being used by them.

6. Safeguards – How Information is Protected

We maintain reasonable security safeguards to protect personal data in our possession or under our control from loss or theft, and from unauthorized access, disclosure, copying, use or modification, regardless of the format in which the information is held. The safeguards applied will depend on the sensitivity of the personal data, with the highest level of protection given to the most sensitive personal data. We use user IDs, passwords and encryption technology, and restrict the employees and contractors who have access to personal data to those having a “need to know” and who are bound by confidentiality obligations in order to ensure that information is handled and stored in a confidential and secure manner.

When destroying personal data, we delete electronically stored personal data and shred any tangible materials containing personal data. While we will endeavor to destroy all copies of personal data, you acknowledge that deleted information may continue to exist on backup media but will not be used unless permitted by law.

We will continually review and update our security policies and controls as technology evolves. However, no security technology can be guaranteed to be failsafe. Using the Internet or other public means of communication to collect and process personal data may involve the transmission of data on an international basis and across networks not owned and/or operated by us.

Therefore, by using the Services and/or communicating electronically with us, you acknowledge and agree to our processing of personal data in this way and agree that we are not responsible for any personal data which is lost, or which is altered, intercepted or stored by a third party without authorization.

7. Accuracy / Access

Millennial Psychology Ltd. has a responsibility to ensure that all personal data contained in our records or which is disclosed to third parties for the purposes described above is accurate, complete and up-to-date. You may make a request in writing for access to your personal data. We will inform you of your personal data held by us, and provide an account of the use that has been made of the information, as well as identify any third parties to whom the information has been disclosed. You may have reasonable access to your personal data, and if you demonstrate the inaccuracy or incompleteness of personal data, the information will be amended as appropriate. You should advise us immediately if you discover inaccuracies in our data, if your personal data changes, or if you wish to have your information removed from our files. All notices and requests should be in writing and sent to the Privacy Officer at the address listed above (see: Accountability and Openness/Compliance).

8. International Transfer and Storage of Information

You acknowledge and agree that your personal data may be transmitted, transferred, processed, and/or stored outside of Canada, including in the United States and in the EU, and therefore may be available to governmental authorities under lawful orders and laws applicable in such jurisdictions. We will use reasonable means to ensure that your information is protected, but cannot guarantee that the laws of any foreign jurisdiction will accord the same degree of protection as the laws of Canada.

9. Third Party Content and Links to other Websites

The Services may contain optional links to third party Internet websites and services. You acknowledge that these third parties may collect data from users or their computers. The accessing and use of third party websites or services is at your own risk, and we cannot assume responsibility for the privacy practices, policies or actions of the third parties who operate those websites or services. This Policy applies only to the Millennial Psychology Ltd. Services, and we encourage you to review the privacy policies of any third parties when using their websites or services.

10. Minors

Minors (persons under the age of majority as defined in your jurisdiction) are not eligible to use the Services unsupervised, and we request that minors do not submit any personal data to us directly on www.millennialpsychology.co.uk. If you are under the age of majority in your jurisdiction, you may only use the Services in conjunction with and under the supervision of an individual who has parental responsibility. Millennial Psychology Ltd. does not knowingly collect personal data directly from minors www.millennialpsychology.co.uk.

11. Notice of Breach

In the event of a security breach causing unauthorized intrusion of our Services that materially affects you or your contacts, Millennial Psychology Ltd. will notify you as soon as possible and later provide a report of the action we took in response to this intrusion.

12. Other Data Rights

Millennial Psychology Ltd. takes reasonable steps to ensure the data we collect is accurate, complete and up to date and is reliable for its intended use. You can manage most of your data through the Services, however, you can always contact us directly through our contact page if you have any questions about your data. If you would like to contact us directly about deleting, updating or accessing your personal data you can email us directly at info@millennialpsychology.co.uk. We will honor your request in accordance

with applicable laws. If you are using our Services to process personal data from certain territories such as the European Union, you may have broader data protection rights identified below:

- The right to be informed: (see: Collection and Retention of Information)
- The right of access/rectification: (see: Collection and Retention of Information for details on what data we collect and how we use it). Contacts can contact Millennial Psychology Ltd. directly to request their information to be updated or corrected.
- The right to erasure: At any time you can cancel your Millennial Psychology Ltd. account as referenced in section 9 of our Terms of Use.
- The right to restrict processing: You can ask us to restrict processing your personal data in certain circumstances.
- The right to data portability: At any time you can export your data and you can ask us to provide your personal data in a structured, commonly used and machine-readable form in certain circumstances.
- The right to object: You may object to the further processing of your personal data in certain circumstances.

13. Contact Information:
Millennial Psychology Ltd.
2a Connaught Avenue, London, E4 7AA
info@millennialpsychology.co.uk

GDPR Cookies

Last Updated: 22 March 2022

Millennial Psychology Ltd. uses Website Navigational Information to collect information about how our visitors and users navigate our website (https://www.millennialpsychology.co.uk), its subdomains and other websites). The technology we use to collect this information is called cookies and it helps us analyze trends, track and measure user's movement around our websites and services and save targeted advertisements. This article explains what this technology is and why we use it as well as visitors' and users' rights to control our use of it.

Cookies
What are cookies?

A "cookie" is a small piece of information stored on your computer by a web page. It is used to identify you to the web server. It tells the server who you are when you return to a page on the same website. Your browser will only send a cookie back to the domain that originally sent it to you. A cookie cannot run any programs, deliver any viruses, or send back information about your system.

Why do we use cookies?
We use cookies to determine your access privileges on our websites, to complete and support your current activity, and to track website usage. Most web browsers automatically accept cookies, but if you do not wish to have cookies on your system, you should adjust your browser settings to decline them or to alert you when cookies are being sent. If you decline cookies, you will still be able to use our services, but your ability to access certain features and functions may be affected.

What cookies are served through our website and our services?
Analytics cookies

• These cookies are used to collect information to help us understand how our websites and services are being used or how effective our marketing campaigns are.
• These cookies are served by Google Analytics and Hotjar.
• To opt-out please click here for Google Analytics and here for Hotjar.

Advertising cookies
• These cookies are used to serve you ads more relevant to you and your interests.
• These cookies are served by Google. To opt-out, please click here.

Social Networking cookies
These cookies are used for advertising purposes as well as to enable you to share content from our websites through third-party social networking platforms. These cookies are served by Facebook, Twitter, and LinkedIn. To opt-out please use:
• for Facebook: https://www.facebook.com/ads/settings
• for Twitter: https://twitter.com/personalization
• for LinkedIn: https://www.linkedin.com/psettings/guest-controls?trk

How you can control cookies
You can manage your cookie preferences in two ways. You can click on one of the opt-out links provided above or you can change your set up in your browser settings. Most web browsers automatically accept cookies, but if you don't wish to have cookies on your system, you should adjust your browser settings to decline them or to alert you when cookies are being sent. If you would like to opt-out of targeted advertising you can use one of these links to set up your ads preferences:
• http://youronlinechoices.com/
• http://www.aboutads.info/choices/
• http://www.networkadvertising.org/choices/ Additional information

If you have questions or concerns regarding cookies, please contact us at info@YOURWEBSITE.COM or email our Privacy Officer/Data Protection Officer at info@millennialpsychology.co.uk

GDPR Data Protection Policy

Context and overview

Key details
– Policy prepared by: Millennial Psychology Ltd.
– Approved by board / management on: 23 March, 2022
– Policy became operational on: 23 March, 2022
– Next review date: 22 march, 2023

Introduction
Millennial Psychology Ltd. 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.

Why this policy exists

This data protection policy ensures Millennial Psychology Ltd.:
– Complies with data protection law and follow good practice
– Protects the rights of staff, customers and partners
– Is open about how it stores and processes individuals' data
– Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including Millennial Psychology Ltd. — 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
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:
– The head office of Millennial Psychology Ltd.
– All branches of Millennial Psychology Ltd.
– All staff and volunteers of Millennial Psychology Ltd.
– All contractors, suppliers and other people working on behalf of Millennial Psychology Ltd.

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
– …plus any other information relating to individuals

Data protection risks

This policy helps to protect Millennial Psychology Ltd. 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 them.
– Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Millennial Psychology Ltd. 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 board of directors is ultimately responsible for ensuring that Millennial Psychology Ltd. meets its legal obligations.

The data protection officer, Dr. Ama Collison, is responsible for:

– Keeping the board updated about data protection responsibilities, risks and issues.
– Reviewing all data protection procedures and related policies, in line with an agreed schedule.
– Arranging data protection training and advice for the people covered by this policy.
– Handling data protection questions from staff and anyone else covered by this policy.
– Dealing with requests from individuals to see the data Millennial Psychology Ltd. 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.

The web developer, Dr. Ama Collison, is responsible for:

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

The marketing manager, REAL PERSON NAME, is responsible for:

– Approving any data protection statements attached to communications such as emails and letters. – Addressing any data protection queries from journalists or media outlets like newspapers.
– Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

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, employees can request it from their line managers.
– Millennial Psychology Ltd. will provide training to all employees to help them understand their responsibilities when handling data.
– Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
– 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 externally.
– 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 of.
– Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

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 printer.

– 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 and never shared between employees.

– If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

– 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 space.

– 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 phones.

– 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 Millennial Psychology Ltd. 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, employees should ensure the screens of their computers are always locked when left unattended.

– Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

– Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.

– Personal data should never be transferred outside of the European Economic Area.

– Employees 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 Millennial Psychology Ltd. 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 Millennial Psychology Ltd. should put into ensuring its accuracy. It is the responsibility of all employees 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 sets. – Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

– Millennial Psychology Ltd. will make it easy for data subjects to update the information Millennial Psychology Ltd. holds about them. For instance, via the company website.

– 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.
– It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests
All individuals who are the subject of personal data held by Millennial Psychology Ltd. are entitled to: –
Ask what information the company holds about them and why.
– Ask how to gain access to it.
– Be informed how to keep it up to date.
– Be informed how the company is meeting its data protection obligations.

If an individual contact 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 at info@millennialpsychology.co.uk The data controller can supply a standard request form, although individuals do not have to use this. Individuals will be charged AMOUNT £10 per subject access request. The data controller will aim to provide the relevant data within 14 days. 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, Millennial Psychology Ltd. will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information
Millennial Psychology Ltd. 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

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request.

Contact Information
Millennial Psychology Ltd.
2a Connaught Avenue, London, E4 7AA
info@millennialpsychology.co.uk
www.millennialpsychology.co.uk