


Mistura Enterprise Ltd & Mistura Informatics Ltd

Privacy and Cookie Policy

(v3.1 June 23)

Version Issue Dated	Version: 3.1: 20th June 2023 Updated: Legal purpose for Type of Data Updated section 4: cookies General re-wording following advisor review
Date of Issue Update	NA
Policy Owner Position	DAWN PRICE Managing Director
Senior Management Team Approval	20th June 2023
Approval Signature	
Date of Director Approval	20th June 2023
Date of next Annual Review	Version 4: 2 nd January 2024

INTRODUCTION

Welcome to the Mistura Group, (Mistura Enterprise Ltd and Mistura Informatics Ltd) Privacy and Cookie Policy. We respect your privacy and are committed to protecting your personal information.

The purpose of this Privacy and Cookie policy is to inform you as to how we look after your personal information that you give us when you visit our website (regardless of where you visit it from) or use our applications and tell you about your privacy rights and how the law protects you.

These are our reasons for collecting it, what we do with it and what your rights are under the UK's data protection laws.

What is in our Privacy Policy?

1. **Important Information**
 - a. Who we are
 - b. Data Controller
 - c. Links to other websites (Third Party Links)
 - d. Children under 18
2. **Collection of Personal Data**
 - a. Purpose of Processing Personal Data
 - b. What Personal data do we Process
 - c. Special Category Data
 - d. If you Fail to Provide Personal Data
3. **How we collect your Personal Data**
 - a. Direct Interactions
 - b. Automated Technologies
 - c. Third Parties or Publically Available Sources
 - d. Technical Data
 - e. Contact Data
4. **Use of Cookies**
5. **The lawful basis for using your Personal Data**
 - a. Purposes of Use of Personal Data
 - b. Marketing
6. **Disclosure of Your Personal Data**
7. **International Transfers**
8. **Data Security**
 - a. Is my Information Being Held Securely?
 - b. How We Keep Your Personal Data Secure
9. **Data Retention**
 - a. How long will you use my personal data for?
 - b. How long do we keep your personal data for?
10. **Your Legal Rights**
 - a. Your Rights
 - b. No Fee usually Required
 - c. What We May Need From You
 - d. Time Limit to Respond
11. **If You Have a Complaint**
11. **Glossary**

1. IMPORTANT INFORMATION

a. Who We Are

Mistura Enterprise Ltd and Mistura Informatics Ltd are providers of medicines product information services. The companies are located in the UK and therefore adhere to any UK law.

Mistura Enterprise is a limited company (trading as Choice and Medication® and trading with candm app®), registered in England and Wales under the following full company details:

Company Name:	Mistura Enterprise Limited
Company Registration Number:	7012554
VAT Number:	GB 101 1559 67
I.C.O. Number:	Z3040639

Mistura Informatics is a limited company (trading with MaPPs® and What's my Drug?), registered in England and Wales under the following full company details:

Company Name:	Mistura Informatics Limited
Company Registration Number:	07844504
VAT Number:	GB 101 1559 67
I.C.O. Number:	Z3539183

All Registered Offices Located at:	Arch Centre for Enterprise, Lintonville Parkway Ashington, Northumberland NE63 9JZ
Physical Office Located at:	2 GEP's Place, Ashington Northumberland NE63 9JZ
Telephone Number:	01670 818229
Email:	admin@choiceandmedication.org.uk admin@misturainformatics.org

b. Data Controller

For the purposes of the Data Protection Act 2018, we are the “data controller” (i.e., the company who is responsible for, and controls the processing of, your personal data). The Managing Director is the data protection officer i.e., is responsible for overseeing questions in relation to this Privacy Policy, including any requests to exercise your legal rights. You can contact our data protection officer on mobile: 07732623547 or by email at: dawn.price@choiceandmedication.org.uk

As the regulator, you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk <http://www.ico.org.uk/>). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

c. Third Party Links

Our websites and application may include links to third-party websites, plug-ins, and supplementary applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

d. Children under 18

If you are aged 17 or under, please get your parent/guardian's permission beforehand whenever you provide us with any personal information.

2. COLLECTION OF PERSONAL DATA

a. What is the Purpose of processing personal data?

We process your personal data to:

- Ensure that our subscribers (including partner agency beneficiaries) are able to access our online services.
- To be able to respond to your enquiries, and requests for support, whether by email, text, online
- To ensure that subscribers to our newsletter receive the requested communications
- To process online orders made via our websites.
- To keep a record of your relationship with us.
- To research the impact of our services on you.
- To administer appropriate records where you work for us.
- To communicate with you about our activities and ways that you can support us, e.g, purchasing products and services, accessing new and existing services.

b. What Personal Data do we process?

For those using our websites for any of the following purposes: subscriptions/enquiries/ /e-newsletter sign-ups/training, consultancy, informal partnerships, research requests, advertising and sponsorship enquiries, self-help group listings, and those making an online purchase, we will collect all/some personal data

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.
- **Contact Data:** includes your email address and billing address, and telephone numbers.
- **Profile Data:** includes your username and password, entries that you make on application, purchases or orders made by you for applications, your feedback, and survey responses.
- **Technical Data:** includes your internet service provider name, operating system, and type of web browser you used, internet protocol (IP) address, your login data, time zone setting and location, browser plug-in types and versions, and other technology on the devices you use to access our website and applications.
- **Usage Data:** includes aggregate and user-specific information on which pages you view, content searched for, page response times, length of visits to certain pages, page interaction information.
- **Financial Data:** includes any payment information and financial details you provide in order to purchase the Websites or applications. Most Payment information such as credit card details are processed exclusively by our payments processing provider and we do not have access to those data.
- **Marketing and Communications Data:** includes your preferences in receiving marketing from us, and your communication preferences. We do not share your data with third parties.

We also collect, use, and share Aggregated Data including statistical or demographic data:

Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website or application feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data, which will be used in accordance with this privacy notice.

We do not obtain data about you from any third party without your knowledge or written consent. The above information is collected by us to ensure that the services provided are accessible and for monitoring, improving and evaluating our services together with enabling us to conduct

research into the effectiveness of our information service. We collect all/some of the above information depending on the product or service that you wish to access and/or your reason for making contact with us.

c. Special category data: Some types of personal data are more sensitive and require additional protections – these are known as Special Category Data. Unless you are submitting your personal data through our Recruitment, **we do not collect any Special Categories of Personal Data about you** (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about genetic and biometric data). **Nor do we collect any information about criminal convictions and offences.** We request that you do not enter any special categories of data when using the interactive features of our website or applications. If you volunteer any special category personal data whilst using a feature of our Websites or applications, we will process it in accordance with this Privacy Policy.

We will never pass on your details to anyone else without your permission except in exceptional circumstances. Examples of this might include anyone reporting serious self-harm or when posing a threat to themselves or others. If you share your personal experience with us for the purpose of it being shared on blogs or in our magazine, you can of course decide if you want to remain anonymous or not, if you are happy to share your personal details with staff members or if you would like us to share your story with the media or other parties then we will, subject always to you having provided your consent to such sharing.

d. If You Fail to Provide Personal Data:

Unfortunately, if you do not provide this information, then we will not be able to provide the products/services you have requested. In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time. **For full details see the Mistura terms and conditions available from: www.choiceandmedication.org and www.mappsorg.com**

3. HOW WE COLLECT YOUR PERSONAL DATA

We use different methods to collect data from and about you including:

a. Direct Interactions

You may give us your Identity, Contact and Financial Data by completing forms or by corresponding with us by post, phone, email or otherwise.

This includes personal data you provide when you apply for our products or services; register for and create an account on our websites or applications; sign up for an event run by us; subscribe to our service or publications; engage with interactive features of our websites or applications, including chat, groups and networks; request marketing to be sent to you; enter a competition, promotion or survey; or give us some feedback; to report a problem with our site; apply for a role through Recruitment; have information e.g. a direct message through a social media platform.

b. Automated Technologies or Interactions

As you interact with our websites and applications, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. Please see our cookie policy below for further details.

c. Third Parties or Publicly Available Sources

We may receive personal data about you from various third parties and public sources as set out below in section 3.4 and 3.5. (For sharing of data with third parties please see paragraph 5.1 and paragraph 6).

d. Technical Data

Technical data is received from the following parties:

- (a) analytics providers such as Google Analytics based outside the EU.
- (b) social networks such as Facebook and Instagram based outside the EU.

(c) search information providers such as Google based outside the EU.

e. Contact Data

Contact, Financial and Transaction Data from providers of technical, payment and delivery services such as PayPal based outside the EU.

Contact Data and Identity Data from publicly available sources such as Companies House and the Electoral Register based inside the EU.

4. USE OF COOKIES

Cookies are small text files containing unique data to identify your computer to the network. When you visit a website, it gives your browser a cookie to store in a cookie file that's placed in your browser's folder on your hard drive. The next time you visit the same website, the browser will give back the cookie to identify you. Then the website loads with a personalized experience.

Cookies do contain data, and that typically includes a unique identifier and a site name.

Our websites use cookies to distinguish you from other users of our website. All are essential and necessary to provide the service. In addition, we use an Analytics Service and inform our users that we track the number of visitors to understand the geolocation where people are from that access our websites to ensure that we safely provide them with the most appropriate information. We always ask for your consent before installing any non-essential cookies on your device. These are the cookies we use:

C&M WESITE SERVICE	TYPE	DESCRIPTION
YES	Functional (Essential) Cookie	Functionality cookies allow you to use the fundamental features of a website. The site features are not available without functional cookies. This could be anything from language preference to displaying news stories, allowing to browse multiple pages. Once you exit, your browser deletes all session cookies.
NONE	Session Cookie	Session cookies work by storing information while browsing a website. This means it won't have to reauthenticate every web page visit. Once you exit, your browser deletes all session cookies.
NONE	Persistent Cookie	Persistent cookies are used to track and collect information about you. This particular cookie enables websites to remember if you're logged in and under what account. It's also used to build a profile on your search history, so websites can recommend products, services, or content relevant to you. Most of these cookies usually have an expiration date
NONE	Advertising Cookie	Advertising cookies (also called targeting cookies) build a profile on you based on your interests, search history, and items you view. They then share that information with other websites, so they can advertise relevant products and services to you.
NONE	Performance Cookie	Performance cookies track your online movements, and that data is used to improve the website. They measure analytics like how many times you visited a page, how much time you spent on a page, or when you left the website.
GOOGLE ANALYTICS	Performance (Essential) Service	For user safety this service is used to understand how many people visit our site and the geolocation where people are from, and which pages they visit to provide them with the correct legal information for that location. All data collected is completely anonymous, it does not identify you as an individual in any way.

You are able and also reminded to set your cookie preferences and disable any cookies you prefer within your browser settings, before agreeing to the terms and conditions and pressing OK to use our site. You block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you will not be able to access all or parts of our site. Further information on deleting or controlling cookies is available at: www.AboutCookies.org

5. USING YOUR PERSONAL DATA

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract, we are about to enter into or have entered into with you.
- Where it is necessary for legitimate interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data other than Whatsmydrug? Application account and the Choice and Medication application account.

In these two instances you will be required to consent and confirm you wish to submit personal information. You have the right to withdraw consent at any time by logging onto your user account for applications or logging onto any of our websites and providing your request via “contact us” or by contacting us directly via: dawn.price@choiceandmedication.org.uk

a. Purposes of Use of Personal Data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the special purpose for which we are using your data. Please contact us if you need details about the special legal ground, we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose	Lawful Basis
Delivering services and other benefits to subscribers	Performance of a contract with you
Delivering our services and other benefits to service users	Our legitimate interest in providing the services we are contracted to provide
Responding to your enquiries as a subscriber or potential subscriber	Performance of a contract with you, or taking the steps necessary to enter a contract with you
Responding to your enquiries as a service user	Our legitimate interest in providing the services we are contracted to provide
Managing our relationship with you as an employee	Our legitimate interest in managing and maintaining appropriate records
To market our services to you	Your consent for us to do so

To promote our services to you for the purposes of new subscriptions	Your consent for us to do so
Recording of online events, webinars and other online services	Our legitimate interests where it is appropriate for us to maintain a record of the online event, webinar or other service
To process online orders	Performance of a contract with you, or our legitimate interest in performing a contract with your organisation
To conduct research to improve our services and to help us understand more about mental health related conditions	Our legitimate interest in improving our services and developing our understanding of mental health conditions and medicines
To conduct research to improve our services and to help us understand more about online medicines information service impact.	Our legitimate interest in improving our services and developing our understanding the utility of digital systems

Where we are processing special category data this will be with your explicit consent for us to do so. There are exceptional circumstances where we may need to process special category data if we believe that there is a risk of harm to you or others, in which case we will process because it is in your vital interests to do so.

b. MARKETING

We strive to provide you with choices regarding certain personal data uses, particularly around marketing of Mistura Products and Services only. Within your user account you can view and make certain decisions about your personal data use.

- **Promotional Offers and Newsletters from Us**

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing). You will receive marketing communications from us only if you have requested information from us, registered on our website or purchased goods or services from us within the last 24 months and, in each case, you have not opted out of receiving that marketing.

- **Third-Party Marketing**

We do not share your personal data with any company outside the Mistura companies for marketing purposes.

- **Opting Out**

You can ask us to stop sending you marketing messages at any time by logging into our Websites or applications and checking or unchecking relevant boxes to adjust your marketing preferences. Or by following the opt-out links on any marketing message sent to you or by contacting us at any time. Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase including registration for our applications, product/service experience or other transactions, please see paragraph 5 above.

- **Cookies**

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see paragraph 4 above.

- **Change Of Purpose**

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us. If we need to use your personal data for any unrelated purpose, we will notify you first and we will explain the legal basis that allows us to do so. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

- **Interactive Services**

There are parts of our website which permit registered users to post user generated content. All content posted in such areas must comply with our terms. We ask you not to enter content, which contains personal information.

6. DISCLOSURE OF YOUR PERSONAL DATA

Mistura will never share, sell or rent your personal information to third parties and we promise to keep your details safe and secure. We will not share your personal information with third parties for marketing purposes.

Mistura will not divulge information unless there is exceptional circumstances that we become aware of and after due consideration there is overriding reason that we may need to make a disclosure to appropriate authorities (police, courts, GP, social services etc).

Mistura would not usually need to contact your GP. However, as your welfare is of paramount importance, if issues of safety arise – for example, we believe or if you disclose that you are a risk to yourself or to others – we may need to contact your GP or relevant professional. When you are using our secure online payment system, your payment is processed by a third party payment processor, who specialises in the secure online capture and processing of credit/debit card transactions.

We may from time to time create statistical and aggregated data derived from your personal data to enable Mistura to share aggregated outcome data for the purpose of evaluation, promotion, marketing and research of services or otherwise evaluate and try to improve our services. Any aggregated data will be in anonymous form and will not identify you as an individual in any way.

We use a number of third party systems providers to deliver our services, some of which are cloud-based packages. Where we are using such third party systems we ensure that we have a data processing agreement in place to protect your rights and comply with data protection laws.

When you contribute content to public e.g. social media or shared areas of our websites or applications you will be credited as the contributor using your username. This accreditation will appear on the service and will therefore be visible to other users. The default setting for the user ID is your first name and surname. You can change these fields by logging in to your profile. We may have to share your personal data with the parties set out below for the purposes set out in the table in paragraph 5 above.

- External Third Parties as set out in the Glossary.
- PayPal in the processing of Financial Information for the purposes of delivering e-commerce services as specified in paragraph 5 above.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes or for marketing and only permit them to process your personal data for specified purposes in delivering the contract with you and in accordance with our instructions.

7. INTERNATIONAL TRANSFERS

We primarily process data in the UK: our website is hosted in the UK, and our Office environment is also hosted in the UK. However, we do use a number of cloud based tools which are based outside the UK, including the USA.

We ensure that we have a lawful basis for such international transfers which most often means that we have Standard Contractual Clauses (SCCs) in place with each provider. These SCCs are mandated by the Information Commissioner's Office (ICO) and aim to safeguard your rights when your personal data are transferred to any nation which lacks an agreement to uphold UK resident's data protection rights by default.

Some of our external third parties are based outside the European Economic Area (EEA) so their processing of your personal data will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU.
- Where we use certain service providers, we may use specific contracts approved by the European Commission, which give personal data the same protection it has in Europe.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield, which requires them to provide similar protection to personal data shared between the Europe and the US.
- Please Contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

8. SECURITY MEASURES

a. Is my information being held securely?

All call data is stored in the UK or EEA. All call recordings are automatically deleted after 30 days. Our supplier of this service is certified to ISO 27001 and Cyber Essentials, data are encrypted wherever possible and additional security measures implemented as appropriate. All processing of personal data for call recording purposes is performed by our supplier under a Data Processing Agreement as required under data protection legislation.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know.

They will only process your personal data on our instructions, and they are subject to a duty of confidentiality. Where you have access to a secure area of our websites or applications, you are responsible for keeping your login details and password(s) confidential and protected. We ask you not to share your password with anyone. You can change your password at any time by logging in. We accept no responsibility or liability if a third party obtains and uses your ID or password.

Please see [Mistura terms and conditions for further information available from:](#)

www.choiceandmedication.org and www.mappsorg.com

You must tell us immediately if you believe someone may have access to or use of this information. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

b. How we keep your personal data secure

We are committed to ensuring that your information is secure. In order 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.

The following key measures help keep us keep your personal data secure:

- Data collected via our website are all encrypted in transit
- Where possible, suitable encryption is used for data at rest
- We use multi-factor authentication where available
- We conduct regular security assessments and penetration testing
- We assess the security practices of our suppliers and partners
- We use encrypted email services where appropriate
- We password protect sensitive documents
- We limit access to personal data to only those members of staff who need it
- All members of staff have confidentiality clauses in their contracts of employment
- We provide regular security training for our staff, volunteers and associates
- We ensure that any paper files are kept in locked cabinets
- Our premises are protected by CCTV

c. How can you help keep your personal data secure?

If you are using our online services please keep you password confidential and do not share it with anyone else. We recommend that you follow the latest online security advice from the National Cyber Security Centre (NCSC).

9. DATA RETENTION

a. How long will you use my personal data for?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

The table below describes our data retention policy for different kinds of personal data and for the different purposes we have. We schedule data deletion activities on an annual basis in accordance with this schedule:

Type Of Record	Retention Period	Storage Media Location	Reason for Retention
Staff Emails	Up to 3 years	Electronic	Essential business continuity
Marketing Messages (Email or text)	6 months	Electronic	To deliver continuity of service

Training Records (externally delivered)	7 years	Electronic/Physical	Essential business continuity
Employee/Personnel Records	7 years after employment ceases unless legally required to retain longer	Electronic/Physical	For references and business continuity
Incidents, Complaints Data (including accident data)	7 years	Electronic/Physical	To comply with Charity Commission guidance
Subscriber forms	1 year	Physical	Essential business continuity
Subscriber info	24 months after end of subscription	Electronic	Essential business continuity
Proof of Postage Receipts	1 year	Physical	Essential business continuity
Recruitment data	1 year post application	Electronic/Physical	For monitoring purposes & HR compliance
Website user contact us interaction	7 years	Electronic	Essential business continuity

10. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

a. Your Rights. You have the right to:

- **Request access to your personal data** (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction of the personal data that we hold about you.** This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure of your personal data.** This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons, which will be notified to you, if applicable, at the time of your request.

- **Object to processing of your personal data.** This is where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information, which override your rights and freedoms.
- **Request restriction of processing of your personal data.** This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is lawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer of your personal data to you or to a third party.** We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent at any time where we are relying on consent to process your personal data.** However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent. If you wish to exercise any of the rights set out above, please contact our data protection officer: dawn.price@choiceandmedication.org.uk or using the contact details set out at the beginning of this policy.

Please note, some of these rights only apply in certain circumstances and we may not be able to fulfil every request and there may be some circumstances where Mistura is allowed to withhold information from you.

b. No Fee Usually Required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

c. What We May Need From You

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights) and this is outlined in Appendix 1 below. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

d. Time Limit To Respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

11. IF YOU HAVE A COMPLAINT

If you would like to lodge a complaint with us regarding the processing of your personal data then please contact us using the above details (see "Who we are").

You also have the right to complain to the Information Commissioner's Office (ICO). You can contact the ICO on their helpline 0303 123 1113 or online at www.ico.org.uk. If you should contact the ICO they will normally ask you to contact us first.

12. GLOSSARY

a. Lawful Basis

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of special activities by Contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract. Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

b. External Third Parties

Legitimate third parties we may share personal data with includes:

- Survey Monkey, based in the US, who provide services in connection with surveying members.
- Dotmailer, based in the EU, who provide customer mailing services and who sub-contract services to Microsoft Azure, Google Cloud Platform, Cloud is, Dynmark International Ltd, Amazon Web Services, GGR Communications, Red SMS, GTT, Interxion, Zayo, Magnetic One, Brooklands Mailing Services.
- GB Group, based in the EU, who provide identification verification services.
- HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances.
- Facebook, based in the US, we upload data to Facebook to allow us to target advertising that is relevant to you.
- Instagram, based in the US, we upload data to Instagram to allow us to target advertising that is relevant to you.
- Google, based in the US, who provide services in connection to website analytics with cookies that help us improve our services and improve patient experience of the services.

MISTURA ENTERPRISE Ltd and MISTURA INFORMATICS Ltd

Appendix 1

FREEDOM OF INFORMATION (F.O.I.) DATA REQUEST LOG

DATA PROTECTION OFFICER (DPO): Managing Director - Dawn Price

DATE	NAME ON REQUEST	CONTACT ADDRESS	DESCRIPTION OF INFORMATION REQUIRED	LEVEL OF DETAIL Summary Comprehensive	FORMAT Electronic Paper Large Print/Audio	Date Response Sent from DPO (within 20 working days)	EXTENSION date advised