1. PRIVACY POLICY

At Meridian HealthComms we take the privacy of the people visiting our website and the security of their personal information very seriously. We are committed to ensure that your privacy is protected.

Any personal information you provide, by which you can be identified, will be used only in accordance with this privacy policy.

The purpose of this privacy policy is to set out the principles governing our use of the personal data you give to us, or we obtain about you, via the website. By using this website, you agree to this use. We ask you to read this privacy policy very carefully; any dispute that may arise will be subject to this policy.

We may change this policy from time to time by updating this page. We therefore ask you to check this page to ensure you are aware and happy with any changes. The policy is effective from 15 May 2019.

INFORMATION COLLECTED ABOUT YOU

When you interact with the website, you may be asked to supply personal data, such as your name and email address. We only collect identifiable information when it is voluntarily submitted through the website.

We will also collect 'aggregate information' through the use of cookies (see below). Aggregate information is non-identifiable and is typically used to monitor the interaction with the website. Examples include measuring the number of users to a site or capturing internet browsers being used.

WHAT WE DO WITH THE INFORMATION

Your personal identifiable information is used for the following:

- For internal records
- To improve the user experience and our services

Aggregate information is used to understand how our users interact with our website and may be shared with a third party who are assisting with the development of the site. The type of data we receive from aggregate information and how it is used is listed below:

- We may monitor user traffic, behaviour patterns and website usage to help determine how we can improve the experience on site for our users.
- We may perform statistical analysis on our users to determine how the users are engaging with the content.
- We may monitor the time spent on the website.

If you provide information about another person, you confirm that they have appointed you to act for them, and given consent to the use of their personal data as set out in this privacy policy.

CONTACT

If you wish to contact us with any concerns, queries or requests relating to our privacy policy please send an email to enquiries@meridian-health.com, or a letter to Meridian HealthComms, The Station House, Plumley Moor Road, Plumley, Cheshire, WA16 9RX.

2. COOKIES

WHAT IS A COOKIE

A cookie is a simple file that is stored on your computer or a mobile device through a web browser. Cookies are used to collect anonymous information from your visit to the site in order to track navigation and usage, to remember your unique functionality of the website and to provide you with targeted information or advertising.

HOW WE USE COOKIES

Our cookies are used to help identify which web pages are being used. We use this information for statistical analysis of our web traffic and to help improve the functionality of the site. Please note, a cookie does not allow us access to your computer or any personal information about yourself.

HOW TO ACCEPT OR DELETE COOKIES

Cookies are voluntary to accept; however, most web browsers automatically accept the use of cookies. You may change this in your web browser settings to automatically decline cookies; in doing this you may not be taking full advantage of the website. To delete cookies that may already be stored on your computer, please refer to the instructions of your file management software to locate the file that stores the cookies. If you wish to find out more about the use of cookies and where they are stored, please visit http://www.aboutcookies.org/

3. DATA PRIVACY NOTICE FOR JOB APPLICANTS

ABOUT THIS DATA PRIVACY NOTICE

This notice is designed to provide information on how Meridian HealthComms Ltd (referred to as "we", "us", "our") processes the personal data of job applicants (referred to as "you", "your") who apply to us for a job.

As a "data controller", we are responsible for deciding how we process personal data about you. We take your privacy seriously and we are fully committed to protecting your personal data at all times. We will only process your personal data in accordance with, and adhere to the principles (as applicable) contained within, the General Data Protection Regulation and, when enacted, the Data Protection Bill 2017-19 (together referred to as the "GDPR").

This notice does not form part of any offer of employment and we may amend it at any time to reflect any changes in the way in which we process your personal data. If you are in the application process when any changes or updates are made to this notice, we will bring any such changes to your attention as soon as is practicable. We may also notify you in other ways from time to time about the processing of your personal data.

Our Head of Privacy & Data Protection is responsible for ensuring that this privacy notice is maintained. That post is held by Emma Hatt who may be contacted at **emma.hatt@meridian-health.com** or 01565 724850.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

"Personal data" is any information about a living individual from which they can be identified such as name, ID number, location data, any online identifier (such as IP address), or any factor specific to the physical, physiological, genetic, mental, economic or social identity of that person. It does not include data where any potential identifiers have been removed (anonymous data) or data held in an unstructured file.

There are “special categories” of more sensitive personal data which are more private in nature and therefore require a higher level of protection, such as genetic data, biometric data, information about sex life or sexual orientation, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health. For the purposes of this notice, personal data relating to criminal convictions will also fall within the description of ‘special category/ies’ personal data.

When we refer to “processing”, this means anything from collecting, using, storing, transferring, disclosing, altering or destroying personal data.

HOW WE USE YOUR PERSONAL DATA

We process your personal data for various reasons, relying on a variety of different bases for lawful processing under the GDPR as set out below.

To comply with our legal obligations or exercise legal rights conferred upon us. This may include:

- checks for eligibility to work in the UK as required by immigration laws, such as passport and visa documentation;
- formal identification documentation relating to you, such as a passport or driving licence, to verify your identity (including your date of birth);

To pursue our (or a third party's) legitimate interests as a business. This may include:

- your contact details such as your name, address, telephone number and personal email address which will be used to communicate with you in relation to the recruitment process;
- your CV, any education history, employment records, professional qualifications and certifications in order for us to consider your suitability for the job you are applying for;
- details of the job role you are applying for any interview notes made by us during or following an interview with you, in order to assess your suitability for that role;
- pay and benefit discussions with you to help determine whether a job offer may be made to you;
- voicemails, emails, correspondence, and other communications created, stored or transmitted by you on or to our computer or communications equipment in order to progress the application through the recruitment process;
- network and information security data in order for us to take steps to protect your information against loss, theft or unauthorised access.

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 we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

HOW WE USE YOUR SPECIAL CATEGORIES DATA

We also collect, store and use your special category personal data for a range of reasons, relying on a variety of different bases for lawful processing under the GDPR, as set out below.

To enable us to perform our legal obligations in respect of employment, social security, social protection law, or needed in the public interest. This may include:

- health information to assess and/or to comply with our obligations under the Equality Act 2010 (for example a requirement to make reasonable adjustments to your working conditions).

For occupational health reasons or where we are assessing your working capability, subject to appropriate confidentiality safeguards. This may include:

- information about your physical or mental health, or disability status, to assess whether any reasonable adjustments are required for you during the recruitment process, and, where you are successful in your role application, carrying out any medical assessment required for your role, pension and any insurance benefits.

To establish, defend or exercise legal claims in an employment tribunal or any other court of law.

For statistical purposes in the public interest such as equal opportunities monitoring (for example the collection of information about race, ethnic origin, sex or religion). Any such information shall only be used, once collected, in an anonymised form for statistical purposes and will not be not used in relation to your application for employment with us.

AUTOMATED DECISION MAKING / PROFILING

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Automated decision-making takes place when an electronic system uses information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration; and
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any special category of personal data, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

“Profiling” means any form of automated processing to evaluate certain personal aspects relating to you, in particular to analyse or predict aspects concerning performance at work, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements.

DATA SHARING

We may share your personal data and special category personal data internally. In particular, it may be shared with: HR employees involved in the recruitment process, employee relations and/or administration of your employment; line managers; consultants; advisers; and/or other appropriate persons who may be involved in the recruitment process for the job(s) you are applying for.

We may share your personal data and special category personal data with other Firm's within our Group. They may use your personal data as part of our usual reporting requirements, in the context of a business reorganisation or group restructuring exercise, for systems support and hosting of data.

We may share your personal data and special category personal data with third parties, agents, subcontractors and other organisations (as listed below) where it is necessary to administer the working relationship with you or where we have a lawful basis for doing so:

Category of personal information	**Recipient/relationship to us**	**Purpose of disclosure**
All personal information collected	IT service providers	To support, maintain and host our information systems, including the software and hardware infrastructure required for it to operate/be accessible online and to keep a backup of your personal information. We also use online IT service providers to provide contract execution services
All personal information collected	Recruitment agencies	To assist with recruitment into our organisation
All personal information collected	Employee benefits providers	For employee benefits to be provided
All personal information collected	Our legal and other professional advisers (including accounting and audit services)	To provide us with advice in relation to our business, including our legal, financial and other obligations and claims
Job role and health data	Occupational health providers	For working capacity of worker to be assessed

When we disclose your personal data to third parties, we only disclose to them any personal data that is necessary for them to provide their service. We have contracts in place with third parties in receipt of your personal data requiring them to keep your personal data secure and not to use it other than in accordance with our specific instructions.

When we disclose your personal data to third parties, they may disclose or transfer it to other organisations in accordance with their data protection policies. This does not affect any of your data subject rights set out at 12 below. In particular, where you ask us to rectify, erase or restrict (the processing of) your personal data, we have an obligation to ensure that this instruction is passed on to any third parties whom we have disclosed your personal information to.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may also share your personal data and special category personal data with other third parties for other reasons. For example: in the context of the possible sale or restructuring of the business; to provide information to a regulator; or to otherwise comply with the law. To comply with our legal obligations we may share your data with the following:

- HMRC for tax purposes;
- Home Office for immigration purposes

We may obtain personal data and/or special category personal data about you from third party sources, such as recruitment agencies, job boards, recruitment assessment centres, occupational health professionals and background check providers. Where we receive such information from these third parties, we will only use it in accordance with this notice.

In some cases, they will be acting as a controller of your personal data and therefore we advise you to read their privacy notice and/or data protection policy.

TRANSFERRING INFORMATION OUTSIDE THE EEA

We do not envisage that we will transfer your personal data outside of the EEA (meaning the EU 27 member states, the UK, Norway, Iceland and Liechtenstein), however we will notify you in writing if this position changes.

DATA STORAGE AND SECURITY

Your personal data and special category personal data is stored in a variety of locations, including: electronically on our secure servers/in hard copy form in access-restricted, locked filing cabinets.

We take appropriate technical and organisational security measures and have rules and procedures in place to guard against unauthorised access, improper use, alteration, disclosure and destruction and accidental loss of your personal data.

In addition, we limit access to your personal data to those who have a business need to know and they will only process your personal data on our instructions and subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected or actual data security breach and will notify you and the Information Commissioner's Office ("ICO") of a suspected breach where we are legally required to do so.

Whenever we propose using new technologies, or where processing is construed as 'high risk', we are obliged to carry out a data protection impact assessment which allows us to make sure appropriate security measures are always in place in relation to the processing of your personal data.

DATA RETENTION

We keep your personal data and special category personal data for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Information about how long we retain such personal data is set out in Appendix 1.

When applying for a job with us, we compile and keep an electronic file containing information about you which relates to your application for a job with us. Your information will be kept secure and will be used for the purposes of your job application, as explained above.

If you are offered and you accept a job with us, your personal data will be transferred to an electronic personnel file. Any hard copy personnel file will be kept in access-restricted, locked filing cabinets. The retention period varies depending on the role(s) which you have held during your employment with us, and your personal data will be permanently and securely deleted at the end of this retention period.

In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use and retain such information without further notice to you, as it falls outside of the definition of personal data under the GDPR.

YOUR DUTIES

We encourage you to ensure that the personal data that we hold about you for the purposes of your application or for the purposes of considering you for any similar roles is accurate and up to date by keeping us informed of any changes to your personal data.

YOUR RIGHTS

You may make a formal request for access to personal data and/or special category data that we hold about you at any time. This is known as a Subject Access Request. We must respond to any such request within a certain time period (being 40 days under the Data Protection Act 1998, reducing to 1 month under the GDPR from 25 May 2018). Please note that under the GDPR we are permitted to extend the 1 month time period for responding by an additional 2 months where in our view your request is complex or numerous in nature. We may also charge a reasonable fee based on administrative costs where in our view your request is manifestly unfounded, excessive or a request for further copies. Alternatively, we may refuse to comply with the request in such circumstances. For further details on subject access requests and the types of request listed below, please refer to please refer to our Subject Access Request Policy and Procedure by contacting our Head of Privacy & Data Protection.

Under certain circumstances, by law you also have the right to:

- have your personal data corrected where it is inaccurate;
- have your personal data erased where it is no longer required. Provided that we do not have any continuing lawful reason to continue processing your personal data, we will make reasonable efforts to comply with your request;
- have your personal data be transferred to another person in an appropriate format where we process that data in reliance on your consent and the processing is carried out by automated means;
- withdraw your consent to processing where this is our lawful basis for doing so;
- restrict the processing of your personal data where you believe it is unlawful for us to do so, you have objected to its use and our investigation is pending, or you require us to keep it in connection with legal proceedings; and
- to object to the processing of your personal data, where we rely on legitimate business interests as a lawful reason for the processing of your data. You also have the right to object where we are processing your personal data for direct marketing purposes. We have a duty to investigate the matter within a reasonable time and take action where it is deemed necessary. Except for the purposes for which we are sure we can continue to process your personal data, we will temporarily stop processing your personal data in line with your objection until we have investigated the matter. If we agree that your objection is justified in accordance with your rights, we will permanently stop using your data for those purposes. Otherwise, we will provide you with our justification as to why we need to continue using your data.

The way we process your personal data and the lawful basis on which we rely to process it may affect the extent to which these rights apply. If you would like to exercise any of these rights, please address them in writing to the Head of Privacy & Data Protection.

We may need to request specific information from you to help us to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an

appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Head of Privacy & Data Protection. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. If you withdraw your consent, our use of your personal data which was collected before your withdrawal is still lawful.

You have the right to complain to a supervisory body if you are concerned about the way we have processed your personal data. In the UK this is the ICO - **www.ico.org.uk**.

Although you have the right to complain to the ICO, we encourage you to contact us first with a view to letting us help in resolving any queries or questions.

QUESTIONS
If you have any questions about any matter relating to data protection or the personal data and/or special category personal data that that we process about you, please contact the Head of Privacy & Data Protection.

Appendix 1

Data category	Retention Period	Reason	Disposal
Job applications and interview records of candidates	12 months - unless following an unsuccessful application you specifically consent to us holding it for longer for the purpose of contacting you in the event that any similar jobs / roles become available. from time to time.	To defend against potential legal claims.	Securely destroyed by third party.