# Privacy Policy

Amazing Healthcare Services LTD, trading and henceforth referred to as Smartly Staffing, needs to gather and use certain information about individuals. In data protection terminology, Smartly Staffing is defined as the Data Controller.

This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. These parties may be defined as the Data Processors.

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 that we:**

a. Comply with data protection law and follow good practice

b. Protect the rights of staff, customers and partners

c. Are open about how we store and process individuals' data

d. Protect ourselves from the risks of a data breach

## Data protection law

- The General Data Protection Regulation (GDPR) applies to the whole of the EU and companies holding data of EU citizens.

## Policy Scope

- **This policy applies to:**

a. The head office of Smartly Staffing

b. All branches of Smartly Staffing

c. All staff and volunteers of Smartly Staffing

d. All contractors, suppliers and other people working on behalf of Smartly Staffing

e. 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.

## What data do we collect and how do we use it?

- If you are a healthcare institution looking to book shifts through Smartly Staffing, we will collect information outlined in your preferences once logged in.

- If you are a nurse registering to find shifts through Smartly Staffing, we will collect information as outlined in your preferences once logged in.

## The basis on which we process data

- You are entitled to know the legal basis on which personal data are processed.

- **"Legitimate interests"**

a. In respect of any personal data processed before users register on the Smartly Staffing platform. This applies where a colleague sends you notifications from Smartly Staffing before you have registered for the purposes of referring you to the platform

- **"Consent"**

a. In respect of your personal data being shared with healthcare institutions. If a user withdraws their consent then they will not be able to access the Smartly Staffing. Any withdrawal of consent will not affect the lawfulness of the use of personal data prior to consent being withdrawn.

b. Occasionally personal data may continue to be used even if consent has been withdrawn, for example, if a healthcare provider makes a complaint about a Smartly Staffing nurse.

- **"Necessary for performance of a contract"**

a. The healthcare institution, acting through Smartly Staffing, will need to access your data to ensure that you meet compliance standards set by their organisation ahead of arrangement of a contract to work.

- **"Necessary for compliance with a legal obligation"**

a. This basis applies in special circumstances such as a police or other legal investigation or serious complaint requiring the healthcare institution or Smartly Staffing to release personal data.

- **"Public interest"**

a. In limited circumstances, healthcare institutions may use personal data to help it discharge its functions relating to providing care to patients and relatives and looking after their welfare.

## Who we share information with

- Smartly Staffing uses a range of specialised third party services to offer the best possible user experience; ensure the security and efficiency of the website and app and perform some statistical and analytic tasks. Where such third parties act as data processors in respect of your personal data, our contracts with them ensure that any information is protected in the manner required by current data protection legislation. The categories of third party service provider we use are as follows:

a. Analytic services to collect standard internet log information and details of visitor behaviour patterns to our website SmartlyStaffing.co.uk. This information is only processed in a way which does not identify anyone.

b. We do not make, and do not allow our providers to make, any attempt to find out the identities of those visiting our website.

c. Performance management services to help maintain the security and performance of the Smartly Staffing website. To deliver this service they process the IP addresses of visitors.

d. Enquiry handling software to help us respond quickly to set-up and registration requests.

e. Customer support services which collect your name, email address (optional) and the contents of your support session.

f. Social media services. If you send us a private or direct message via social media the message will be stored.

g. Survey services to gather user feedback. If any personal data is required users will be asked to consent to this in advance. This information will not be shared with any other organisations.

h. Inbound email services. Email monitoring and blocking software is used to manage inbound email. Any email and attachments sent to our various Smartly Staffing addresses may be monitored for security and content. Users should be aware that any email sent to us must be within the bounds of the law.

i. Outbound email services to deliver regular email updates and e-newsletters to Smartly Staffing members. We gather statistics around email opening and clicks using industry standard to help us monitor and improve this service.

j. Payment services to facilitate payment of nurses. We use payment providers who provide high levels of user security and keep any personal or payment data private and confidential.

k. Third party hosting services to hold your personal data in secure data centres located within the European Economic Area.

## Data protection risks

We use information held about you in the following ways:

- **This policy helps to protect Smartly Staffing from some very real data security risks, including:**

a. Breaches of confidentiality. For instance, information being given out inappropriately.

b. Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

c. Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

- In data protection terminology, the Data Controller is Smartly Staffing.
- Everyone who works for or with Smartly Staffing 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.
- **The following people have key areas of responsibility:**

a. The Board of Directors is ultimately responsible for ensuring that Amazing Healthcare Services LTD meets its legal obligations.

b. The data protection officer, Martial Niyonzima, 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 Smartly Staffing 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.

c. The Chief Technical Officer, Martial Niyonzima, 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.

d. The Chief Marketing Officer, Lyse Niyonzima, is responsible for:

- Approving data protection statements attached to communications such as email 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 the line managers.
- Amazing Healthcare Services 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 CTO or Data Controller.
- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- **These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:**

a. When not required, the paper or files should be kept in a locked drawer or filing cabinet.
b. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
c. Data printouts should be shredded and disposed of securely when no longer required.
d. When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
e. Data should be protected by strong password that are changed regularly and never shared between employees.
f. If data is stored on removable media (like a CD or DVD), these should be kept lock away securely when not being used.

g. Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.

h. Servers containing personal data should be sited in a secure location away from general office space.

i. Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

j. If data is stored to laptops, smartphone or tablets it should be deleted as soon after it has been used and no more than eight hours after the data has been received.

k. 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 Amazing Healthcare Services 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:**

a. When working with personal data, employees should ensure the screen of their computers are always locked when left unattended.

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

c. Data must be encrypted before being transferred electronically. The Chief Technical Officer can explain how to send data to authorized external contacts.

d. Personal data should never be transferred outside of the European Economic Area unless it is to a company compliant with EU-US Privacy Policy Shield.

## Data accuracy

- The law requires Amazing Healthcare Services 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 Amazing Healthcare Services 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.

- Smartly Staffing will make it easy for data subjects to update the information Smartly Staffing 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.

## Subject access request

- **All individuals who are the subject of personal data held by Smartly Staffing are entitled to:**

a. Ask what information the company holds about them and why

b. Ask how to gain access to it

c. Be informed how to keep it up to date

d. Be informed how the company is meeting its data protection obligations

- **If an individual contacts the company requesting this information, this is called a subject access request**

a. Subject access request from individual should be made by email, addressed to the data controller at martial@SmartlyStaffing.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

b. Individuals will not be charged for a subject access request. The data controller will aim to provide the relevant data within 14 days.

c. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

## Cookies

- Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and allows us to improve our site. For detailed information on the cookies we use and the purposes for which we use them see below.

- We use third party analytics providers to collect information about your use of our site and enable us to improve how our service works. The information allows us to see the overall patterns of usage on our site and helps us record any difficulties you have with it.

- These third party analytics providers use cookies and other, similar technologies to collect information about use of the site and to report statistics and trends to us without identifying you individually.

## Right to be forgotten

- The broad principle underpinning the right to be forgotten is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

- **This is not an absolute right and Smartly Staffing may not be able to comply with your request to be forgotten should any of the following conditions be deemed to apply:**

a. If we have a legal obligation for the performance of a public interest task or exercise of official authority.

b. For public health purposes in the public interest.

c. For archiving purposes in the public interest, scientific research historical research or statistical purposes.

## Consent

- When you create an account with Smartly Staffing, you will be explicitly asked to consent to the use of your personal data as outlined in this policy.

- Should you not consent to the use of your personal data as outlined in this policy, Smartly Staffing will not be able to offer the level of service expected from the platform.

## Security

- The security of your personal information is important to us. We maintain a variety of appropriate technical and organizational safeguards to protect your personal information.

- We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs. Further, we have implemented reasonable physical, electronic, and procedural safeguards designed to protect personal information about you.

- When you enter sensitive information (such as your password), we encrypt that information in transit using industry-standard Transport Layer Security (TLS) encryption technology.

- No method of transmission over the Internet, method of electronic storage or other security methods are one hundred per cent secure. Therefore, while we strive to use reasonable efforts to protect your personal information, we cannot guarantee its absolute security.