

Shield Worker Privacy Notice

Updated: Jan 2021

Shield Hospitality Staffing Solutions Ltd ("Shield") has issued this Privacy Notice ("Notice") for contingent workers this notice may apply to ("you", "your").

This notice sets out the personal information that we collect and process about you, the purposes of the processing and the rights that you have in connection with the collection and processing of your personal data (your "**Privacy Notice**");

The term "contingent worker" means all those who work on a non-permanent basis, including casual workers, consultants, independent contractors, professional advisors or interns.

We respect the privacy rights of individuals and are committed to handling personal information responsibly and in accordance with applicable law. If you are in any doubt regarding the applicable standards, or have any questions about this Policy, please contact emma.hulme@shieldhospitality.co.uk

1. Types of personal information we collect about contingent workers

- 1.1 In the course of your work at Shield, we may process personal information about you and your family members and other individuals whose personal information has been provided to us.
- 1.2 The types of personal information we process include, but are not limited to:
 - 1.2.1 Identification data e.g., name, photograph, gender, date of birth, payroll number;
 - 1.2.2 Contact details e.g., home address, telephone/email, emergency contact details;
 - 1.2.3 Position details e.g., job title/position, work location, contract, training records, attendance records, work outputs and standards;
 - 1.2.4 Professional qualifications skills information e.g., academic/professional qualifications, education, CV/resume, languages;
 - 1.2.5 National identifiers e.g., national ID/passport, immigration status, driver's licence, social security numbers;
 - 1.2.6 Family members (or person nominated as next of kin) information – such as names, relationship to you, contact details;

- 1.2.7 Financial information e.g., bank account details, tax information, rates of pay expenses, company allowances;
 - 1.2.8 Pension information e.g., employer pensions contributions, scheme membership, pension entitlements, retirement information (if applicable);
 - 1.2.9 IT related data if applicable e.g., computer ID, user ID, IP addresses, service access logs, software and hardware inventory, cookies (if applicable);
 - 1.2.10 Medical information e.g. details of any disabilities or conditions which may result in further assistance being required at work, or any information which we are required to collect in accordance with law and/or government guidelines;
 - 1.2.11 Health and safety information e.g., records of accidents at work, and
 - 1.2.12 Criminal records / Disclosure and Barring Service (DBS) checks.
- 1.3 In certain circumstances, we will collect information that reveals information about your health or genetic data or biometric data for the purposes of unique identification ("**Sensitive Personal Information**"). All the categories of data just mentioned are considered by European data protection law as Sensitive Personal Information. For example, you may need to provide us with information about your physical or mental condition for occupational health reasons (so that we can provide work-related accommodations) or so that you can manage absences from work due to ill health. We will request, on a voluntary disclosure basis only, certain Sensitive Personal Information such as information about your disabilities where required to comply with anti-discrimination laws which we will use to help ensure equal employment opportunities.

2. Sources of personal information

Usually you will have provided the information we hold about you but there may be situations where we collect personal information from other sources. The following are the types of information we may collect about you and the source of the information:

- 2.1 References from nominated third party referees;
- 2.2 Feedback from colleagues or clients on standard of work outputs;
- 2.3 Tax and other criminal or regulatory information where HMRC and/or other authorities such as the police choose to contact us in connection with investigations;
- 2.4 IT related data e.g., computer ID, user ID, IP addresses, service access logs, software and hardware inventory, cookies.

2.5 Medical information where relevant government authorities choose to contact us in connection with matters of national interest.

3. Purposes for processing personal information

3.1 Shield collects and uses your personal information primarily for the purpose of managing our relationship with you – for example, your worker agreement and worker records (to manage your relationship with us), your bank account and pay details (so we can pay you) and details of your dependents (for emergency contact).

3.2 Shield may also collect and use personal information when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently – for example, for IT security/management, accounting purposes, or financial planning. We may also process your personal information to investigate breaches of law or of our own internal policies.

3.3 Shield may also use your personal information where we consider it necessary for complying with laws and regulations, including collecting and disclosing worker personal information as required by law (e.g., for tax, health and safety, anti-discrimination laws) or under judicial authorisation.

4. Monitoring

4.1 Shield will carry out automated monitoring of its IT and communications systems through automated tools such as anti-malware software, website filtering and spam filtering. It will also carry out monitoring of its physical premises where relevant, for example by using CCTV and security badges.

4.2 The primary purpose of this monitoring is to protect Shield, its workers, customers and business partners, for example:

4.2.1 for general network operation and security, including in particular the security of Shield's IT systems and assets, and the optimal operation of its network and devices;

4.2.2 for proof of business transactions and archiving;

4.2.3 for coaching, training and evaluation of workers;

4.2.4 for the protection of confidential information and intellectual property;

4.2.5 for investigating breaches of internal policies, fraud or other unlawful or wrongful activity, or to respond to a particular personnel or company incident;

4.2.6 for business continuity (such as monitoring business-related emails following a worker's departure); and

4.2.7 for physical security of its premises.

4.3 Monitoring activities are likely to be continuous and ongoing. However, they will always be proportionate, for legitimate purposes and as required or permitted by applicable law. Before undertaking any monitoring activities, we will consider your reasonable expectations of privacy and assess whether there are any less invasive options.

4.4 You should be aware that any message, files, data, document, facsimile, telephone conversations, social media post or instant message communications, or any other types of information transmitted to or from, received or printed from, or created, stored or recorded on our IT and communications systems and devices are presumed to be business-related and may be monitored by us in accordance with applicable law.

5. Who we share your personal information with

5.1 Shield takes care to allow access to personal information only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it. Whenever we permit a third party to access personal information, we will implement appropriate measures to ensure the information is used in a manner consistent with this Notice and that the confidentiality and integrity of the information is maintained.

5.2 We will share your personal information for legitimate business purposes (such as IT services/security, tax & accounting purposes, general business management).

5.3 We make certain personal information available to third parties who provide services to us. We do so on a "need to know basis" and in accordance with applicable data protection law. For example, some personal information will be available to third-party companies who provide us with services such as: payroll support, resourcing software, general software/IT troubleshooting.

5.4 We may also disclose personal information to other third parties on other lawful grounds, including:

5.4.1 To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process, or

to meet national security or law enforcement requests, including, but not limited to, a subpoena or search warrant;

5.4.2 With your consent;

5.4.3 As necessary to establish, exercise or defend against potential, threatened or actual litigation;

5.4.4 Where necessary to protect the vital interests of another person; and

5.4.5 In connection with the sale, assignment or other transfer of all or part of our business.

6. Data retention periods

6.1 Personal information will be stored only as long as is necessary to carry out the purposes described in this Notice or as otherwise required by contractual agreements with third parties, law or other Shield policies.

7. Your data protection rights

7.1 Data Subject Rights are explained in more detail in Shield's Data Subject Rights Handling Policy (a copy of which is available from your Shield Account Manager).

7.2 If Shield is relying on your consent to process your personal information, you have the right to withdraw your consent at any time. This will not however affect the lawfulness of the processing before your consent has been withdrawn.

8. Updates to this notice

8.1 This Notice may be updated periodically to reflect any necessary changes in our privacy practices. Where such changes will materially affect your privacy rights, we will inform you and indicate at the top of the Notice when it was most recently updated. We encourage you to check back on this Notice periodically so that you are aware of the most recent version of it.

9. Questions and comments

9.1 In the first instance, you may wish to raise any questions or concerns with your Shield Account Manager.

9.2 Please address any questions or requests relating to this Notice to emma.hulme@shieldhospitality.co.uk

9.3 You have a right to lodge any complaints with the Information Commissioner's Office although we ask that you raise any issues internally in the first instance via emma.hulme@shieldhospitality.co.uk