PRIVACY NOTICE – JOB APPLICANTS

WHO WE ARE – THE DATA CONTROLLER

'We' are Smarts NI Limited ("Smarts NI"), a company incorporated and registered in Northern Ireland with company number NI024211 whose registered office is at 157 High Street, Holywood, County Down, BT18 9HU.

We are the "Controller" for the purposes of data protection law. This means that we are responsible for deciding how we hold and use personal information about job applicants. This policy details how and why their personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides applicants with certain information that must be provided under the General Data Protection Regulation (*(EU) 2016/679*) (GDPR).

Please note that we may not necessarily hold, use or share *all* of the types of personal data described in this Privacy Notice in relation to all applicants, the specific types of data that we will hold, use and share will depend on the role for which applicants are applying, the nature of the recruitment process, how far applicants progress in the recruitment process and their individual circumstances.

DATA PROTECTION PRINCIPLES

We will comply with data protection law and principles, which means that job applicants' data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told applicants about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told applicants about.
- Kept securely.

WHAT INFORMATION DO WE HOLD AND HOW DO WE OBTAIN IT?

In connection with applications for work with us, we will collect, store, and use the following categories of personal information about applicants:

- The information provided to us by applicants including; CV content, photographs, employment history, qualifications/training (including educational, vocational, driving licences where appropriate), referees' names and contact details etc.
- Publicly available information about applicants, such as business social media presence (e.g. LinkedIn) and any personal blogs.
- Any information provided to us during an interview and the results of any written or online selection tests.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Equal opportunities monitoring data which could include information about race or ethnicity, religious beliefs, political opinions, sexual orientation and health. We use this information to report and monitor equality of opportunity and diversity in our recruitment process. Our legal ground for using this information is that it is necessary in the public interest for the purposes of equal opportunity monitoring and is in line with our Privacy Standard.
- Information about health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is personal information collected?

We collect personal information about candidates from the following sources:

- The job applicant.

- Any recruitment agency, involved in the recruitment process. The recruitment agency may provide us with copies of CVs and contact details.
- Any named referees, from whom we collect the following categories of data: references if the applicant is successful.

How we will use information about applicants

We will use the personal information we collect to:

- Assess skills, qualifications, and suitability for the role.
- Carry out background and reference checks, where applicable.
- Communicate with applicants during the recruitment process.
- Keep records related to our hiring processes.
- Make informed recruitment decisions.
- Comply with legal or regulatory requirements, e.g. the obligation on us not to discriminate during our recruitment process or employ someone who does not have the right to work in the UK.

It is in our legitimate interests to decide whether to appoint applicants to the role since it would be beneficial to our business to appoint someone to that role.

We also need to process personal information to decide whether to enter into a contract of employment with successful applicants and, in some instances, to comply with a legal obligation e.g. the obligation not to discriminate during our recruitment process, or the obligation not to employ someone who does not have the legal right to work in the UK.

Having received an application, we will then process that information to decide whether applicants meet the basic requirements to be shortlisted for the role. If they do, we will decide whether their application is strong enough to invite them for an interview. If we decide to call applicants for an interview, we will use the information provided to us at the interview to decide whether to offer the role. If we decide to offer the role, we may then take up references and (if necessary) carry out a criminal record check before confirming their appointment.

If applicants fail to provide personal information

If a job applicant fails to provide information when requested, which is necessary for us to consider their application (such as evidence of qualifications or work history), we will not be able to process their application. For example, if we require a credit check or references for a role and they fail to provide us with relevant details, we will not be able to take their application further.

HOW WE USE PARTICULARLY SENSITIVE INFORMATION

We will use particularly sensitive personal information in the following ways:

- We will use information about disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during interview.
- We will use information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure lawful and meaningful equal opportunity monitoring and reporting.

Information about criminal convictions

We may process information about criminal convictions where we are legally authorised to do so.

We will collect information about criminal convictions history if we would like to offer a role (conditional on checks and any other conditions, such as references, being satisfactory) in order to satisfy ourselves that there is nothing in an applicants criminal convictions history which makes them unsuitable for the role.

AUTOMATED DECISION MAKING

Applicants will not be subject to decisions that will have a significant impact on them based solely on automated decision-making.

DATA SHARING

Why might we share personal information with third parties?

We may share personal data that is relevant where appropriate, with our group company to enable them to input into the recruitment process and approve final recruitment decisions.

Our legal grounds for doing so are that: it is necessary for entry into a contract and it is in our legitimate interests to obtain our group company's approval of our recruitment decisions and to comply with the procedures applicable without our corporate group.

For the purposes of GDPR, we are resident in the United Kingdom and regulated by the Information Commissioner's Office.

Overseas transfer of personal data

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed, accessed or otherwise used in, a different country. For example, we may transfer personal data to our USA branch. Data Protection law restricts transfers of personal data to countries outside the European Economic Area (EEA) because the law in those countries might not provide the same level of protection to personal data as the law in the EEA. To ensure that the level of protection afforded to personal data is not compromised, therefore, we are only able to transfer personal data outside the EEA if certain conditions are met, as explained below.

We have put in place appropriate measures to ensure that any personal data transferred outside the EEA is treated in a way that is consistent with and which respects the EEA and UK laws on data protection and receives an adequate level of protection.

Recruitment agencies

We engage recruitment agencies to provide us with details of suitable candidates for our available vacancies, to communicate to those candidates and to handle administration in connection with the recruitment process. If we have received an initial application from a recruitment agency, we will share with them any personal data that is necessary to enable them to fulfil their functions for us.

Medical / occupational health professionals

We may share information relevant to any request for adjustments to the recruitment process as a result of an underlying medical condition or disability with medical / occupational health professionals to enable us to identify what, if any, adjustments are needed in the recruitment process and, potentially, in the workplace. Our legal basis for sharing this information is that it is necessary for entry into a contract; it is in our legitimate

interest to consider adjustments to enable job applicants to participate fully in the recruitment process and it is necessary to comply with our legal obligations.

Legal / Professional advisers

We may share personal data that is relevant, where appropriate, with our legal and other professional advisers, in order to obtain legal or other professional advice about matters related to dealing with legal disputes. Our legal grounds for sharing this personal data are that it is in our legitimate interests to seek advice to clarify our rights and obligations and appropriately defend ourselves from potential claims; it is necessary to comply with our legal obligations / exercise legal rights in the field of employment and it is necessary to establish, exercise or defend legal claims.

Home Office

We may share right to work documentation with the Home Office, where necessary, to enable us to verify an applicant's right to work in the UK. Our legal ground for sharing this personal data is to comply with our legal obligation not to employ someone who does not have the right to work in the UK.

DATA SECURITY

We have put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. These include physical and administrative security measures at our offices, firewalls and continuously updated anti-virus programmes and encrypted storage. In addition, we limit access to personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process personal information on our instructions and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify applicants and any applicable regulator of a suspected breach where we are legally required to do so.

Our Company data is stored in the following locations:

- On servers in our offices in the United Kingdom
- Across several sites connected by a secure communications system
- By a secure cloud storage provider
- Locked filing cabinets

Data retention

How long will we use applicant's information for?

We will keep personal data throughout the recruitment process.

If an applicant is successfully recruited, when they start working for us they will be issued with an Employee Privacy Notice which will include information about what personal data we keep from the recruitment process and how long we keep personal data whilst working for us and after leaving.

If an applicant is unsuccessful, we will retain their personal information for a period of twelve months from the date they are notified of our decision. We retain personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy personal information.

We wish to retain an applicant's personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider them for that.

In all cases, we will not keep personal data for longer than we need it for our legitimate purposes.

REFERENCES

If we receive details of referees, we require applicants to inform them what personal data of theirs is being given to us. They must also give them our contact details and let them know that they should contact us if they have any queries about how we will use their personal data.

APPLICANTS RIGHTS

Under certain circumstances, by law applicants have the right to:

- **Request access** to their personal information (commonly known as a "data subject access request"). This enables them to receive a copy of the personal information we hold about them, and, to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about them. This enables applicants to have any incomplete or inaccurate information we hold corrected.

- **Request erasure** of their personal information. This enables applicants to ask us to delete or remove personal information where there is no good reason for us continuing to process it. They also have the right to ask us to delete or remove personal information where they have exercised their right to object to processing (see below).

- **Object to processing** of personal information where we are relying on a legitimate interest (or those of a third party) and there is something about an applicant's particular situation which makes the applicant want to object to processing on this ground. They also have the right to object where we are processing personal information for direct marketing purposes.

- **Request the restriction of processing** of personal information. This enables applicants to ask us to suspend the processing of personal information, for example if they want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of personal information to another party.

Note too that applicants 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. Details of how to contact the ICO can be found on its website: http://ico.org.uk