GDPR POLICY

COMPANY NAME: **STAFF GIANT SERVICES LTD**
DOCUMENT DP3: **DATA PROTECTION POLICY**
TOPIC: **DATA PROTECTION**

CONTENTS

All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their personal data whilst imposing certain obligations on the organisations that process their data.

As a recruitment business the Company collects and processes both personal data and sensitive personal data. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how the Company implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure.

DATA PROTECTION POLICY: DEFINITIONS

In this policy the following terms have the following meanings:

'consent' means any freely given, specific, informed, and unambiguous indication of an individual's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of persona data relating to him or her;

'data controller' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data;

'data processor' means an individual or organisation which processes personal data on behalf of the data controller;

'personal data'* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;

'processing' means any operation or set of operations performed on personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

'sensitive personal data'* means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

* For the purposes of this policy we use the term 'personal data' to include 'sensitive personal data' except where we specifically need to refer to sensitive personal data.

'Supervisory authority' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

DATA PROTECTION POLICY: DATA PROCESSING UNDER THE DATA PROTECTION LAWS

The Company processes personal data in relation to its own staff, work-seekers and individual client contacts and is a data controller for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is [ZA325655].

The Company may hold personal data on individuals for the following purposes:

• Staff administration;
• Advertising, marketing and public relations [please refer to Policy X: Marketing…etc];
• Accounts and records;
• Administration and processing of work-seekers' personal data for the purposes of providing work-finding services, including processing using software solution providers and back office support [./;]
• Administration and processing of clients' personal data for the purposes of supplying/introducing work-seekers [./; and];

1. The data protection principles

The Data Protection Laws require the Company acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
7. The data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Legal bases for processing

The Company will only process personal data where it has a legal basis for doing so (see Annex A). Where the Company does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Company will establish that it has a legal reason for making the transfer.

3. Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

• data minimisation (i.e. not keeping data for longer than is necessary);
• pseudonymisation;
• anonymization [./;]
• cyber security [./; and];

For further information please refer to the Company's Information Security Policy.

DATA PROTECTION POLICY: RIGHTS OF THE INDIVIDUAL

The Company shall provide any information relating to data processing to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

1. Privacy notices

Where the Company collects personal data from the individual, the Company will give the individual a privacy notice at the time when it first obtains the personal data.

Where the Company collects personal data other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month. If the Company intends to disclose the personal data to a third party then the privacy notice will be issued when the personal data are first disclosed (if not issued sooner).

Where the Company intends to further process the personal data for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further processing.

2. Subject access requests

The individual is entitled to access their personal data on request from the data controller.

3. Rectification

The individual or another data controller at the individual's request, has the right to ask the Company to rectify any inaccurate or incomplete personal data concerning an individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

4. Erasure

The individual or another data controller at the individual's request, has the right to ask the Company to erase an individual's personal data.

If the Company receives a request to erase it will ask the individual if s/he wants his personal data to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual's personal data at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other data controllers and data processors processing the personal data to erase the personal data, taking into account available technology and the cost of implementation.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to erase the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

5. Restriction of processing

The individual or a data controller at the individual's request, has the right to ask the Company to restrict its processing of an individual's personal data where:

- The individual challenges the accuracy of the personal data;
- The processing is unlawful and the individual opposes its erasure;
- The Company no longer needs the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to restrict the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however, the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

6. Data portability

The individual shall have the right to receive personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another data controller in circumstances where:

- The processing is based on the individual's consent or a contract; and
- The processing is carried out by automated means.

Where feasible, the Company will send the personal data to a named third party on the individual's request.

7.Object to processing

The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest. The individual will also be able to object to the profiling of their data based on a public interest or a legitimate interest.

The Company shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their personal data for direct marketing. Please refer to the Company's Marketing Policy for further information.

8. Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

9. Automated decision making

The Company will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the data controller and the individual;
- Is authorised by law; or
- The individual has given their explicit consent.

The Company will not carry out any automated decision-making or profiling using the personal data of a child.

DATA PROTECTION POLICY: PERSONAL DATA BREACHES

Reporting personal data breaches

All data breaches should be referred to the persons whose details are listed in the Appendix.

1. Personal data breaches where the Company is the data controller:

Where the Company establishes that a personal data breach has taken place, the Company will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the personal data breach happens outside the UK, the Company shall alert the relevant supervisory authority for data breaches in the effected jurisdiction.

2. Personal data breaches where the Company is the data processor:

The Company will alert the relevant data controller as to the personal data breach as soon as they are aware of the breach.

3. Communicating personal data breaches to individuals

Where the Company has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

The Company will not be required to tell individuals about the personal data breach where:

- The Company has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

DATA PROTECTION POLICY: THE HUMAN RIGHTS ACT 1998

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

DATA PROTECTION POLICY: COMPLAINTS

If you have a complaint or suggestion about the Company's handling of personal data then please contact the person whose details are listed in the Appendix to this policy.

Alternatively you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

DATA PROTECTION POLICY: ANNEX A

a) The lawfulness of processing conditions for personal data are:

- Consent of the individual for one or more specific purposes.
- Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
- Processing is necessary for compliance with a legal obligation that the controller is subject to.
- Processing is necessary to protect the vital interests of the individual or another person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.

b) The lawfulness of processing conditions for sensitive personal data are:

1. Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.

2. Processing is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.

3. Processing is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving consent.

4. In the course of its legitimate activities, processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the consent of the individual.

5. Processing relates to personal data which are manifestly made public by the individual.

6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

7. Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.

8. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee , medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.

9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.

10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

NOTES – DELETE THESE NOTES FROM THE TERMS GIVEN TO THE INDIVIDUAL

NOTE: 1

SECTION NUMBER

SENSITIVE PERSONAL DATA

EXPLANATION

The Data Protection Act 1998 (DPA) uses the term 'sensitive personal data' which includes information on an individual's physical and mental health, sexual orientation, race or ethnic origin, religious beliefs, trade union membership and criminal records.

The GDPR uses the term 'special categories of data' but expands on the definition of sensitive personal data under the DPA. Interestingly the GDPR does not include criminal records and provides that member states must make separate arrangements for the processing of such records. However we anticipate that the draft Data Protection Bill that criminal convictions will constitute sensitive personal data after 25 May 2018. The draft Data Protection Bill provides that organisations can continue to process criminal records as they do now provided they have appropriate processes and policies in place. At the time of writing that Bill is working its way through Parliament and so is still subject to change.

NOTE: 2

SECTION NUMBER

DATA PROCESSING UNDER THE DATA PROTECTION LAWS

EXPLANATION

You should insert your ICO registration number here.

The GDPR removes the requirement for data controllers to register with the supervisory authority in the territories in which it operates. However the UK Government has confirmed that data controllers operating in the UK will still need to register with the ICO. For more information see ICO – fees and registration changes.

NOTE: 3

SECTION NUMBER

MARKETING

EXPLANATION

If your organisation as a marketing policy refer to it here. The REC are currently in the process of creating a marketing policy.

NOTE: 4

SECTION NUMBER

DATA PROCESSING UNDER THE DATA PROTECTION LAWS

EXPLANATION

If your organisation processes any other personal data for purposes not listed already then you should insert such details here.

NOTE: 5

SECTION NUMBER

LEGAL BASES FOR PROCESSING

EXPLANATION

Where you act as a data processor or data controller you are only permitted to process personal data where you can establish a lawful basis to do so.

Annex A to this policy sets out the lawful reasons to process both personal data and sensitive personal data. If you cannot establish a lawful basis to process the personal data then you should cease processing the data immediately.

NOTE: 6

SECTION NUMBER

PRIVACY BY DESIGN AND BY DEFAULT

EXPLANATION

The GDPR will oblige organisations to take a 'privacy by design and by default' approach to data protection. This will require organisations to implement measures and procedures that adequately protect the privacy of the data subject and ensure that data protection is integral to all processing activities. You may wish to refer to your organisation's Information Security Policy to demonstrate your agency's approach to 'privacy by design and by default'. Alternatively, you may want to set this out in full here.

If your organisation has implemented any other measures to protect the privacy of data subjects insert those here.

See the ICO Guidance on Privacy by Design and by Default and the Article 29 Working Party's Guidance on data privacy impact assessments.

NOTE: 7

SECTION NUMBER

PRIVACY NOTICES

EXPLANATION

The GDPR obliges data controllers to provide specific information to data subjects when first collecting their personal data.

See REC Model Documents DP5A and DP5B - Privacy Notices.

NOTE: 8

SECTION NUMBER

SUBJECT ACCESS REQUESTS

EXPLANATION

Individuals will have the right to obtain information that an organisation holds on them under what is known as a subject access request.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

NOTE: 9

SECTION NUMBER

RECTIFICATION

EXPLANATION

Individuals will have the right to ask data controllers to rectify personal data that is either not correct or incomplete. Data controllers will also be obliged to inform any data processors of such requests.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

NOTE: 10

SECTION NUMBER

ERASURE

EXPLANATION

Individuals will have the right to ask data controllers to delete their personal data. Data controllers should only delete such personal data where they have no other lawful basis to retain such data (for example where there is a legal basis to retain the personal data). Data controllers will also be obliged to inform any data processors of such requests.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

NOTE: 11

SECTION NUMBER

RESTRICTION OF PROCESSING

EXPLANATION

Individuals will have the right to ask data controllers to restrict the processing of their personal data. Data controllers will also be obliged to inform any data processors of such requests.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

NOTE: 12

SECTION NUMBER

DATA PORTABILITY

EXPLANATION

Individuals will have the right to ask data controllers to receive and transmit their personal data in specific circumstances.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

See also the Article 29 Working Party's Guidance on data portability.

NOTE: 13

SECTION NUMBER

OBJECT TO PROCESSING

EXPLANATION

Individuals will have the right to ask data controllers to object to the processing of their personal data.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

NOTE: 14

SECTION NUMBER

ENFORCEMENT OF RIGHTS

EXPLANATION

The GDPR requires data controllers to respond to the requests from individuals in a set timeframe (one month on receipt of the request). Failure to respond within the set timeframes will result in a breach of the Data Protection Laws.

If it is necessary to extend the period to respond for a further two months then the data controller must inform the individual of any such extension within one month of receipt of the initial request, together with the reasons for the delay.

In certain circumstances a data controller may either refuse a request or charge a fee to comply with an individual's rights. Where this is the case it will be for the data controller to bear the burden of demonstrating that any request was manifestly unfounded or excessive.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

NOTE: 15

SECTION NUMBER

AUTOMATED DECISION MAKING

EXPLANATION

The GDPR provides that an individual has a 'right not to be subject to a decision based solely on automated processing, including profiling, except in certain circumstances.

If the data controller plans to use automated decision-making and profiling which will have legal or similarly significant effects, it must:
•tell the data subject;
•provide 'meaningful information about the logic involved'; and
•explain the significance and expected consequences of such processing for the data subject.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.
See also the Article 29 Working Party's Guidance on automated decision making and profiling.

NOTE: 16

SECTION NUMBER

PERSONAL DATA BREACHES WHERE THE COMPANY IS THE DATA CONTROLLER

EXPLANATION

Where the data controller is made aware of a personal data breach then it will be necessary to investigate the breach to determine if the ICO will need to be made aware of the breach.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.
See also Article 29 Working party's Guidance on personal data breaches.

NOTE: 17

SECTION NUMBER

PERSONAL DATA BREACHES WHERE THE COMPANY IS THE DATA CONTROLLER

EXPLANATION

Where the data processor is made aware of a personal data breach then it will be necessary to inform the relevant data controller and have regard to any contractual terms that are in place between the parties.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.
See also Article 29 Working party's Guidance on personal data breaches.

NOTE: 18

SECTION NUMBER

COMMUNICATING DATA BREACHES TO INDIVIDUALS

EXPLANATION

If a personal data breach has been identified then in certain circumstances the GDPR obliges data controllers to inform the individual of the breach.

See REC Model Document DP4 – Data Protection Procedure for further information on how to process such a request.

See also Article 29 Working party's Guidance on personal data breaches.

NOTE: 19

SECTION NUMBER

THE HUMAN RIGHTS ACT 1998

EXPLANATION

The Data Protection Laws will need to be assessed in light of the fundamental rights and freedoms individuals have under the Human Rights Act 1998. You may find it useful to refer to WP29's guidance on data processing at work which discusses individual's fundamental rights in more detail.

NOTE: 20

SECTION NUMBER

APPENDIX

EXPLANATION

A Data Protection Officer (DPO) is the individual responsible for all issues relating to the protection of personal data within his/her organisation. The GDPR will oblige both data controllers and data processors to hire a DPO in specific circumstances, such as:
·when the processing of data is conducted by a public authority or body;
·the core activities of the data controller revolves around processing operations which require regular and systematic monitoring of data subjects on a large scale; or
·the core activities of the data controller or data processor consist of processing sensitive personal data of data on a large scale and personal data relating to criminal convictions.

Where an organisation is not obliged to have a DPO they will still be able to have one if they so wish.

See the Article 29 Working Party's Guidance on Data Protection Officers.

NOTE: 21

SECTION NUMBER

ANNEX A

EXPLANATION

Although the GDPR does not define the term 'employee' European legislation tends to define this quite broadly. Therefore it is the REC's view that this would include temporary workers as well as internal employees of the Company.