1. INTENT

Our Company, that is IWL, IGESL, RESCO,IWEL and Inox FMCG Private Limited together referred to herein after as the Company, is committed to all aspects of personal data protection. This policy sets out how the Company shall deal with employees' personal data, including personnel files and data subject access requests; and employees' obligations in relation to personal data. The Company recognizes that employees have rights in relation to their own personal data processed by the Company, and as employees of the Company they have responsibilities for the personal data of others (i.e. clients, customers and colleagues) which they process in the course of their work.

The Company expects its employees and the third parties to hold themselves to the high standards of legal and ethical compliance to which the company holds itself.

2. PURPOSE

The purpose of this policy is to highlight practices that are followed at the Company for confidentiality of employee's personal information and make everyone in the organization familiar with how we collect, use, protect and disclose the information. Personal information received from our employees shall be used, entirely or partly, for the following purposes:

a) to carry out recruitment process i.e. to communicate with the applicant and do selection between different candidates
b) for employment contract or the related agreement
c) when the Company is required by laws and regulations to provide personal information.
d) for Performance reviews
e) for administration of Employee Payroll
f) to process of Employee Benefit claims like: Medical Insurance etc
g) to comply with all applicable labor and employment legislation
h) to notify information regarding events such as exhibitions and seminars
i) where the company is required to comply with the valid court orders, warrants or other valid processes
j) in an emergency to protect the physical safety of any employee
k) for other related works or services in relation to the services described above

The Company may use personal Information for a purpose other than originally stated purpose is required by law or where the Company has obtained consent in writing from the affected individual for each new purpose

3. SCOPE & APPLICABILITY

This policy applies to all employees associated with the Company (globally) and all affiliates and subsidiaries of the Company at all levels and grades, including directors, senior executives, officers, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, casual workers, volunteers, interns, agents, or any other person associated with the Company who deal with personal information of employees on behalf of the company

Part of the company's commitment to prevent misuse of confidential information of employee personal data is to ensure that the people acting on our behalf also do so in compliance with effective data privacy policies. Accordingly, where we engage "Third Parties" such as any individual or organization, who/which come into contact with the Company or transact with the Company and also includes actual and potential clients, suppliers, business contacts, consultants, intermediaries, representatives, subcontractors, agents, advisers, joint ventures and government & public bodies (including their advisers, representatives and officials, politicians and political parties).

4. DEFINITION AND CATEGORIES OF PERSONAL INFORMATION ASKED

a) Definition of Personal Data

"Personal data" is any information that relates to an identified or identifiable living individual. This includes where living individuals can be directly or indirectly identified using information such as a name as well as other identifiers such as unique personal identifiers (e.g. payroll and National Insurance numbers), location data or other online identifiers, as well as physical, physiological, genetic mental, economic, cultural or social identity.

b) Definition of Processing

"Processing" is defined very broadly and encompasses any action performed on or with personal data, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (that is, the marking of stored data with the aim of limiting its processing in the future, erasure and destruction. In effect, it is any activity involving personal data.

c) Definition of "Special categories of personal data"

It means personal data which reveals a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data, and information relating to a data subject's sex life or sexual orientation. Examples of special categories of personal data are as follows –

- racial or ethnic origin - political opinions
- religious or philosophical beliefs
- the processing of genetic data
- the processing of biometric data in order to uniquely identify a person - mental or physical health - sexual life and orientation
- trade union membership

d)"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

The Company shall collect relevant and necessary Personal Information, and shall process such information only for the purpose it has been collected. The purpose of collection shall be specified not later than at the time of data collection. Such personal data can generally be divided into the following categories:

- Identifying data, such as name, password (when applying via our home page), citizenship, and date of birth;
- contact details, such as address and telephone number;
- recruitment-related information, such as previous work experience information (including previous employer references), qualifications and work history, educational qualification, appraisal record, disciplinary records, UAN Number, bank account number
- any kind of application form or declaration as required
- communication information, such as content in e-mail conversations as required

5. DISCLOSURE AND DATA SHARING TO THIRD PARTIES

a. The Company shall not sell, share, rent or otherwise distribute/ trade sensitive personal information, collected by the Company by documentation or by any online mode.

b. Personal data may occasionally be transferred to third parties who act for or on behalf of the Company, or are in connection with the business of the company, for further processing in accordance with the purpose for which the data was originally collected.

c. The Company shall not try to collect any of the Special Category Personal Data

d. The Company may ask from an employee hos criminal records, but shall have no right to disclose such data to any external agencies if not asked by any agency of a gubernatorial nature

e. The Company may also share information with third party service providers contracted to provide services on our behalf for processing personal information, to conduct marketing campaigns, trainings and related services. Where disclosure of sensitive personal data to a third party is likely or necessary for whatever reason, the company will, wherever possible, endeavor that the disclosure and intended use of the data are clearly indicated. All such parties provide the same level of protection as the company and, where appropriate, we will contractually require them to process data transferred only for the purposes expressly authorized by the company

6. RETENTION & DISPOSAL OF PERSONAL INFORMATION:

Any personal information collected by the Company shall be retained by the Company during the period of active employment of the individual and not more than three (3) years from the date of leaving.

Personal Information that is no longer needed for its stated purpose shall be destroyed, erased or made anonymous. The Company shall ensure that all practices and procedures relating to the disposal of Personal information shall respect the fundamental policy of confidentiality. All personal information disposal procedures, including the disposal of computerized data storage devices shall ensure the complete destruction of personal information so that there is no risk of subsequent unauthorized disclosure of personal information.

The Third Party has no right to keep a copy of any data provided by the Company in any format, and all physical and logical access to such Personal Data or other data shall be deleted. The Third Party shall provide the Company with a written declaration whereby the third party warrants that all Personal Data or other data mentioned above has been returned or deleted according to the Company's instructions and that the third party has not kept any copy, print out or kept the data on any medium.

7. OBLIGATION OF EMPLOYEES/ MANAGERS

a. As part of the on-going move to employee self-service, managers can view their immediate reports contact information including emergency contact details (where provided) and employment information integral to staff management

b. Employees with access to and responsibility for personal data are expected to:
   i. access only data that they have authority to access and only for authorised purposes;
   ii. comply at all times with the City Corporation's IT, Security and email use policies; and in particular not use a non corporation email system for the transmission of personal data;
   iii. use data responsibly and in accordance with the data protection principles and should be cautious about disclosing personal data both within and outside the City Corporation, and about using it in email and via the internet or intranet;
   iv. complete mandatory data protection and related training to comply fully with corporate and local guidance, procedures and practice regarding the processing of personal data and check their authority to take any action involving personal data with their manager;
   v. report any loss or compromise of their own or others personal information to the Departmental Head and the Corporate HR.

c. Where personal information is to be disposed of, employees should ensure that it is destroyed permanently and securely. This may involve the permanent removal of the information from the server so that it does not remain in an employee's inbox, deleted items folder or recover deleted items folder. Hard copies of personal information must be confidentially shredded or placed in confidential waste bins provided. Employees should be careful to ensure that personal information is not disposed of in a wastepaper basket / recycle bin. It must be remembered that the destruction of personal data is of itself "processing" and must be carried out in accordance with the data protection principles.

d. If an employee acquires any personal data in error by whatever means, they shall inform their Departmental Head and Corporate HR representative immediately and, if it is not necessary for them to retain it, destroy the personal data without any further processing of it.

e. An employee must not send other people's personal data from a Company laptop, desktop, tablet or mobile phone to a personal email account i.e. an account not owned or controlled by the City Corporation, except where it is legally permitted to do so.

f. Where employee personal data needs to be taken off site the responsible employee must ensure that appropriate steps are taken to protect it; be it in hard copy, stored on a laptop or other electronic device. For the removal of hard copy information, prior consent should be obtained from their line manager or senior officer. Care must also be taken when observing personal data in hard copy or on-screen so that such information is not viewed by anyone who is not legitimately privy to it.

g. If an employee is in any doubt about what they may or may not do with personal data, they should seek advice from their Departmental Head or the Corporate HR representative before taking any action.

8. COMPLIANCE

All the employees and the third parties having care over personal information must comply with the policies, procedures and practices as described in the policy. Breach of any term or condition of this privacy policy, whether intentional or unintentional, including but not limited to the unauthorized disclosure of personal information is grounds for disciplinary action up to and including the immediate termination from employment/contract of any or all responsible employee/third party.

All employees are expected to sign a declaration form (Annexure I – Declaration) giving their consent to share Personal Data as per this Guideline.
All third parties are expected to sign a declaration form (Annexure II – Confidentiality and Non-Disclosure Agreement) for before any Personal Data/ Information is shared by the Company.

9. POWER TO AMEND

a. Any Changes of the Guidelines have to be approved by the Head GCHR. b. The management has the overriding right to withdraw and /or to amend guidelines at its own discretions as it deems fit time to time. The decision of management shall be final and binding.

Annexures

1. Employee Declaration – Annexure 1 2. Confidentiality and Non-Disclosure agreement with service providers and third party – Annexure 2

Annexure I – DECLARATION OF CONSENT BY AN EMPLOYEE

I, Mr/Ms……Employee Code…….confirm that I have gone through the Guideline on Confidentiality of Personal Information of the Company and having understood the same and by signing this declaration of consent, I authorize the Company to process my personal data in regard to my employment with the Company and its affiliated companies. The personal data processed by the Company is name, any national identification number, date of birth, address, telephone, work telephone, cell phone, email address, employment contract, area of work, job title, date of hire, application, resume, diplomas, visa, car, familial relationships, sick days, taxes, bank account, private economy such as the calculation of net salary, and similar purely private conditions.

I authorize the Company to use and process my personal data within the Company and its affiliated companies, and only if and when it is deemed necessary and relevant in regard to my employment with the Company.

I authorize processing of my personal data shall take place by electronic and manual means. This processing involves transfer, registration, storage, printing, and deletion of information. The specific processors are email and server provider, CRM system, online banking system, payroll system, digital transaction manager, accountant, legal representative, recruiter, encryption provider and insurance company.

I authorize the Company to share my personal data shall only be available to relevant, designated persons in the Company and affiliated companies, and shall not be shared or transferred to anyone other than these unless required by law.

I authorize the Company retains my personal data for three (03) years after my resignation.

I, the undersigned, hereby give my consent for the Company to process information about me, including my personal data, as described in the above.

……. ……..

Employee Name Employee Signature

DATE:

PLACE:

Back To Index

Annexure - 2

Data Processing and Confidentiality Agreement
between
The Company and Third Party and/or Agencies where employee Personal Data is involved

This agreement is signed between the ……..having its registered office at …….(hereinafter referred to as the "Company") and ……..having its registered office at ……(hereinafter referred to as the "Processor")

1. Purpose and definitions

The purpose of this Data Processing Agreement is to regulate the Processor's processing of personal data on behalf of the Company whilst providing Support & Consulting Services to the Company. This Data Processing Agreement governs the Processor's rights and obligations, in order to ensure that all Processing of Personal Data is conducted in compliance with applicable data protection legislation. Processing of Personal Data (as defined below) is subject to requirements and obligations pursuant to applicable law. The parties agree to amend this Data Processing Agreement to the extent necessary due to any mandatory new requirements under the Law of the Land.

a) Definition of Personal Data - "Personal data" is any information that relates to an identified or identifiable living individual. This includes where living individuals can be directly or indirectly identified using information such as a name as well as other identifiers such as unique personal identifiers (e.g. payroll and National Insurance numbers), location data or other online identifiers, as well as physical, physiological, genetic mental, economic, cultural or social identity.

b) Definition of Processing - "Processing" is defined very broadly and encompasses any action performed on or with personal data, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (that is, the marking of stored data with the aim of limiting its processing in the future, erasure and destruction. In effect, it is any activity involving personal data.

2. Processor's responsibilities

2.1 Compliance - The Processor shall comply with all provisions for the protection of Personal Data set out in this Data Processing Agreement and in applicable data protection legislation with relevance for Processing of Personal Data. The Processor shall comply with the instructions and routines issued by the Company in relation to the Processing of Personal Data.

2.2 Restrictions on use - The Processor shall only Process Personal Data on, and in accordance with, the instructions from the Company. The Processor shall not Process Personal Data without a prior written agreement with the Company or without written instructions from the Company beyond what is necessary to fulfil its obligations towards the Company under the Agreement.

2.3 Information Security - The Processor shall by means of planned, systematic, organizational and technical measures ensure appropriate information security with regard to confidentiality, integrity, and accessibility in connection with the Processing of Personal Data in accordance with the information security provisions in applicable data protection legislation. The measures and documentation regarding internal control shall be made available to the Company upon request. Discrepancies and data breach notifications Any use of the information systems and the Personal Data not compliant with established routines, instructions from the Company or applicable data protection legislation, as well as any security breaches, shall be treated as a discrepancy. The Processor shall have in place routines and systematic processes to follow up discrepancies, which shall include re-establishing of the normal state of affairs, eliminating the cause of the discrepancy and preventing its recurrence. The Processor shall immediately notify the Company of any breach of this Data Processing

Agreement or of accidental, unlawful or unauthorized access to, use or disclosure of Personal Data, or that the Personal Data may have been compromised or a breach of the integrity of the Personal Data.

Back To Index

The Processor shall provide the Company with all information necessary to enable the Company to comply with applicable data protection legislation and enabling the Company to answer any inquiries from the applicable data protection authorities. It is the Company's responsibility to notify the applicable Data Protection Authority of discrepancies in accordance with applicable law.

3. Confidentiality

The Processor shall keep confidential all Personal Data and other confidential information. The Processor shall ensure that each member of the staff of the Processor, whether employed or hired employee, having access to or being involved with the Processing of Personal Data under this Agreement (i) undertakes a duty for confidentiality and (ii) is informed of and complies with the obligations of this Data Processing Agreement. The duty of confidentiality shall also apply 3 year after termination of the Agreement.

4. Security audits

The Processor shall on a regular basis carry out security audits for systems and similar relevant for the Processing of Personal Data covered by this Data Processing Agreement. Reports documenting the security audits shall be available to the Company. The Company has the right to demand security audits performed by an independent third party at the Processors choice. The third party will provide a report to be delivered to the Company upon request.

5. Use of sub-contractors (sub-processors)

The Processor is entitled to use sub-contractors and the Company accepts the use of sub-contractors. The Processor shall, by written agreement with any sub-contractor ensure that any Processing of Personal Data carried out by sub-contractors shall be subject to the same obligations and limitations as those imposed on the Processor according to this Data Processing Agreement. If the Processor plans to change sub-contractors or plans to use a new sub-contractor, Processor shall notify the Company in writing 4 months prior to any Processing by the new sub-contractor, and the Company may within 1 month of the notice object to the change of sub-contractors. Should the Company object to the change, Company may terminate the Agreement upon 3 months' notice. To the extent Company does not terminate the Agreement, the change of subcontractor shall be regarded as accepted.

4. Non-disclosure of Personal Information

4.1 Each of the parties to this Agreement intends to disclose information (the Confidential Information) to the other party for the purpose of Support and Consulting services related to Employee Services only.
4.2 The Processor undertakes not to use the Confidential Information disclosed by the Company for any purpose except the Purpose, without first obtaining the written agreement of the other party.
4.3 The Processor undertakes to keep the Confidential Information disclosed by the Company secure and not to disclose it to any third party, except to its employees and professional advisers who need to know the same for the Purpose, who know they owe a duty of confidence and are bound by obligations equivalent to those in this Agreement.
4.4 The undertakings in clauses above apply to all of the information disclosed by each of the parties to the other, regardless of the way or form in which it is disclosed or recorded, but they do not apply to: a) any information which is or in future comes into the public domain (unless as a result of the breach of this Agreement); or b) any information which is already known to the Processor and which was not subject to any obligation of confidence before it was disclosed to the Processor by the other party.
4.5 Nothing in this Agreement will prevent the Processor from making any disclosure of the Confidential Information required by law or by any competent authority.
4.6 The Processor will, on request from the Company, return all copies and records of the Confidential Information disclosed by the Company to the Processor and will not retain any copies or records of the Confidential Information disclosed by the other party.

Back To Index

4.7 Neither this Agreement nor the supply of any information grants the Processor any license, interest or right in respect of any intellectual property rights of the other party except the right to copy the Confidential Information disclosed by the other party solely for the Purpose.
4.8 The parties shall ensure that each member of the staff of the parties, whether employed or hired employee, having access to or being involved in performing the Services, undertakes a duty of confidentiality and is informed of and complies with the obligations of this Non-disclosure Agreement. The duty of confidentiality shall also apply 1 year after termination of this Agreement.
5. Entire Agreement - This Agreement constitutes the entire agreement between the parties hereto pertaining to the subject matter hereof and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions, whether oral or written, of the parties hereto in this connection.

6. Severability - If any provision in this Agreement is determined to be invalid, void or unenforceable by the decision of any court of competent jurisdiction, which determination is not appealed or appealable for any reason whatsoever, the provision in question shall not be deemed to affect or impair the validity or enforceability of any other provision of this Agreement and such invalid or unenforceable provision or portion thereof shall be severed from the remainder of this Agreement.

7. Modification - No modification or amendment of any of the provisions of the Agreement shall be binding unless it is in writing and mutually agreed.

8. Survival - Notwithstanding that the Company or the Processor may decide to terminate the Agreement , the provisions of the Agreement shall remain in force and survive for a period of 3 (three) years from the date the employee ceases to be in employment with the Company.

9. Indemnity - The Processor agrees to indemnify and hold the Company harmless from any cost, expenses, loss damages, claims or liability (including legal fees and the cost of enforcing this indemnity) arising out of or resulting from any unauthorized use or disclosure by the Processor of the Personal Information or other violation of this Agreement.

10. Arbitration - Without limitation to the Company's right set forth above, In the event of any dispute or difference amongst or between the Parties hereto either during the subsistence of this Agreement or afterwards arising from or relating to or in any way connected with this Agreement, which cannot be resolved by the parties acting in good faith, shall be referred to the Arbitration of a Single Arbitrator to be nominated by the management of the Company authorized in this behalf whose decision shall be final and binding on the Parties. The provisions of the Indian Arbitration and Conciliation Act or any statutory modification or re-enactment thereof for the time being in force shall be applicable. The venue of arbitration shall be NCT of Delhi only.

11. Jurisdiction and Applicable law - The courts at New Delhi alone will have exclusive jurisdiction in all matters arising from or connected with this Agreement and it shall be governed according to the substantive laws in India.

IN WITNESS WHEREOF the parties hereto have, themselves or through their duly authorized representatives, set and subscribed their respective hands the day, month and year first above written.

Signed and Delivered
For Company

Authorized Signatory
Name:
Date :
Place :

Signed and Delivered

Signature
Name:
Date :

Back To Index