

Arup Roy
India

Date: February 18, 2022

Dear **Arup Roy**,

It was a pleasure meeting you to explore a career opportunity for you with ITC Infotech India Limited.

Based on our discussion, we are pleased to offer you the position of **Associate IT Consultant** at grade **IS1**

1. Your annual gross salary along with the break-up of salary is enclosed at the end.
2. You are required to join us on or before **February 16, 2022** and the offer stands withdrawn thereafter, unless the date is extended by us and communicated to you in writing.
3. You are requested to report at 9.30 AM to complete the joining formalities. Your initial place of posting will be at **Kolkata**. At the time of joining you are requested to submit the copies of documents as per the checklist enclosed.
4. For any further clarifications, request you to communicate with the concerned recruiter contact.

Your appointment is subject to

- Your passing the Company's medical examination successfully. The decision of Company's medical team in this regard will be final.
- The Company receiving appropriate and satisfactory replies from your referees. The decision of the Company in this regard will be final.
- Your producing acceptable certified documentary evidence of your date of birth. This evidence must be a Birth Certificate or School Leaving Certificate, Copy of your passport or an Affidavit attesting your date of birth and sworn by your father, mother or a close relative. This date once accepted will be used for all purposes in connection with your employment and no cognisance will be taken for any alterations in the future.



- Your producing acceptable certified documentary evidence of your academic and professional qualifications.
- The Company receiving appropriate and satisfactory report on your background check i.e. past employment and education details.

Welcome to ITC Infotech India Limited and look forward to a long and mutually beneficial association.

Yours faithfully,
ITC Infotech India Limited

Jaismon Emmanuel

Sr VP – Business Excellence

Designation: Associate IT Consultant

Grade: IS1

Location: Kolkata

Qualification: B.tech

Experience: 1.4 yrs

Date of Birth: March 10, 1994

Date of Joining: February 16, 2022

Monthly Components	Proposed Salary (Rs pm)
Basic/Consolidated Salary	7500
House Rent Allowance	3750
Supplementary Allowance	21408
SUB- TOTAL I	32658
Annual Components	
PF	1800
L.T.A.	917
Bonus	2021
ITC Products & Services	104
SUB- TOTAL II	4842
TOTAL	37500
Grand Total PA	450000

Explanatory Notes:

- Medical Insurance for Self/Family (Spouse, 2 dependent children up to age of 24 years) will be covered under Company's Health Insurance scheme, with a sum insured value of **Rs.5,00,000/-** per annum.

You will also be covered under the Group Accident Insurance scheme, with a sum insured value of **Rs.15 Lakhs/-** per annum.

Option to cover parents / parents-in-law on payment of premium by employee with attractive benefits. Option has also been provided to cover your family under the Critical Illness Program, additional Group Accident Insurance for yourself and Group Medical Insurance for your family by paying a nominal top up premium by yourself.

- Leave Travel Allowance of Rs. 11000/- is paid as per company policy, Prorata for the previous financial year along with April salary of the following financial year.
- ITC Products & Services - this scheme provides you an opportunity to avail and enjoy ITC's world class products and services, governed by the following policy.
 - a) You are eligible to claim reimbursement towards the purchase up to **Rs. 1250 /-** per annum, prorated in case where there is no full year of service).
 - b) The Reimbursement amount are based on assumption that you are availing the benefit upto the entitlement as per the respective policy. If you do not avail the benefit, the amount mentioned is non-encashable / not carried forward to the next financial year.
- Bonus - You are entitled to the indicated Bonus amount as per the Payment of Bonus Act or the STI amount as per the policy, whichever is higher. In case you have joined the Company during January - March, you will be eligible for STI from the following accounting year.
- You will also be eligible for Gratuity as per the Payment of Gratuity Act.

Yours faithfully,
ITC Infotech India Limited

Jaismon Emmanuel

Sr VP – Business Excellence

Privacy Notice Employees

This notice is applicable to all employees of ITC Infotech India Limited, its branches and subsidiaries (ITC Infotech Group) who are in the UK, European Union (EU) and the European Economic Area (EEA) whose Personal Data is collected and/or processed in the UK, EU and the EEA in the context of the employment relationship (known through this document as “you” or “your”).

ITC Infotech Group is committed to protecting the privacy and security of your Personal Data.

For the purposes of your employment with ITC Infotech Group (hereinafter referred to as “ITC Infotech” or “Company” or “we” or “our” or “us”) , we collect, hold, process and transfer Personal Data and sensitive Personal Data about you as necessary for the administration, management and performance of your employment or otherwise in the legitimate interests of the Company.

The purpose of this notice is to provide you information about how we collect, store and process your Personal Data.

1. Your Personal Data and Sensitive Personal Data

Personal Data means any information which is relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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. The processing of personal data is governed by the EU General Data Protection Regulation (the “EU GDPR”), UK GDPR and other laws.

The Personal Data is collected and processed by the Company for the following employee administration and management purposes:

- Identification Information including name, gender, age, date of birth, email address, home address, contact details, government-issued identification numbers, photographs, demographic information, citizenship, nationality, marital status, date of marriage, dependent names, relationship, age or date of birth, domicile or residence data.
- Educational and Professional Details including highest education, certifications, previous employment history with all supporting documents and proofs.
- Employment, credit checks, criminal checks, drug test report and other requirements as part of background verification.
- Past or current compensation and benefits information including details of salary and benefits, bank account details, salary reviews, records relating to holiday and other leaves, working time records

- Information about your performance at work, including references obtained from your previous place of work, performance evaluations, as well as opinions expressed by your colleagues, individuals who you manage or have managed, supervisors, and clients.
- Travel and Expenses Information including passport, visa details, corporate card transactions, expense details, supporting bills, claims reimbursed, and locations visited, supporting proofs carrying your Personal Information.
- Learning and Development Information including training, certifications, attendance & and assessment records of past or present engagements.
- Information collected as part of Surveillance and Monitoring such as video surveillance data, physical access logs, activity logs from systems and communication channels etc.

The sensitive personal data collected may include:

- Information relating to your Health: such as physical examination results, accident and injury reports, disability status, medical records, doctor's certificates.
- As part of diversity surveys or equal employment opportunities, we may also collect information related to racial, ethnic origin or religious beliefs.

This information would be collected by us either directly from you or indirectly through our authorized third party service providers who are authorized to collect such information in a number of legally allowed ways, through multiple channels, while joining our organization and over time during the course of your employment.

Apart from personal information relating to you, you may also provide ITC Infotech with personal information of your dependents and other family members, for purposes of HR administration and management, including the administration of insurance, benefits etc. and someone to contact in an emergency. Before you provide such dependents personal information to ITC Infotech, you must first inform them of any such information that you intend to provide and of the processing to be carried out by ITC Infotech, as detailed in this notice.

2. Purpose of processing your Personal Data and Sensitive Personal Data and legal basis for processing

We use your Personal Data to enable us to run our operations, meet with our legal obligations and manage our relationship with you effectively, during and after your employment with the Company. This includes using your Personal Data to enable us to comply with your employment contract, to comply with any legal requirements, pursue our legitimate interests and protect or defend our legal position in the event of legal proceedings. If you do not provide requisite Personal Data or Sensitive Personal Data, we may be unable in some circumstances to comply with our obligations or fulfil our contractual obligations with you.

The key processing activities shall include:

- Pay your salary and register you for benefits in accordance with your

employment contract. If you do not provide the information requested, we will be unable to pay your salary, provide or register you for benefits.

- Deduct and Pay taxes on your earnings as required under laws.
- Carry out background verification checks as per the customer needs or in accordance with applicable law and as per Company's laid down process.
- Note your expression of wish for death benefits. By completing and returning your expression of wish you consent to us storing your expression of wish and referring to it in the event of your death in service. If you do not provide the information requested, we will not have an indication of your wishes in the event of your death in service.
- General HR administration. We keep employment records in line with industry practice including information relating to employment history, CV, references, absences (for example, annual leave and sickness or injury), accidents and equal opportunities monitoring. We keep a copy of your employment contract and any correspondence with you in the event of your cessation of employment. It is in our legitimate business interests to process these records.
- Operate and keep a record of employee performance review processes and in relation to compensation, reward and benefits. We also keep employee learning and development records to plan for employee career development. It is in our legitimate business interest to process these records.
- Engage travel and immigration vendors to facilitate corporate travel, location transfers, validate corporate card expenses and relevant supporting in line with our travel, mobility and expense policies, as detailed in the company handbook/intranet.
- Operate and keep a record of disciplinary, grievance and dismissal processes to ensure acceptable conduct within the work place.
- Monitoring and Surveillance processing of biometric and other personal data for the purpose of ensuring safety and security of the Company and its staff and in certain cases to comply with legal requirements, manage and comply with information security practices required by our customers. In particular, we monitor computer [and telephone/mobile telephone] use and may also carry out CCTV monitoring of key areas, as detailed in our Interception and Surveillance policy, available on CafeXpress
- We may also keep records of your hours of work by way of our access control system for responding to requests by legal authorities or courts.
- Audit Compliance – We may process personal data as part of our audit controls and processes directly or through third party auditors, from time to time.
- Insurance Administration – We may process your medical, dental or any other insurance as per the coverage provided.
- Exit Administration and post-employment related activities including providing references on request for current, future or former employers.
- Complying with laws and regulations, including disclosing your personal data to

third parties in order to comply with legal obligations, including where necessary to abide by law, regulation or contract (for example administer pension, compliance of health and safety law), or to respond to a court order, administrative or judicial process, including but not limited to, a subpoena, government audit.

We process your data to pursue our legitimate business interests, for example providing services to our clients, to prevent fraud, verifying compliance to policies, administrative purposes or reporting potential crimes, information security compliance, compliance with law, availability of reference records and other legitimate business or compliance purposes that may arise from time to time.

Where necessary, we may process sensitive personal information relating to your health, or limitations, special abilities in order to comply with our health and safety and occupational health obligations, for providing insurance based on your eligibility where applicable or to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate.

We need such data to also administer and manage statutory and company sick pay, pension health insurance or life insurance benefits.

The Company shall process such information subject to your consent or as otherwise legally permitted, for example, where it is necessary for carrying out obligations or exercising rights under employment law, to protect your vital interests, for the establishment or defense of legal claims, to facilitate medical diagnosis/ assistance/ treatment and/or for the assessment of your working capacity. Please note that withdrawal of such consent may in some circumstances affect our ability to fulfil certain responsibilities to you and we will tell you about the implications of that decision.

We may also process sensitive personal information relating to your racial or ethnic origin, religious beliefs in each case, for the purposes of monitoring the existence or absence of equality of opportunity or assertive action required by law or other lawful purposes. Such processing shall only be carried out based on your consent and you have the right to withdraw that consent at any time. Please note that withdrawal of such consent may in some circumstances affect our ability to fulfil certain responsibilities to you.

In the future, if we intend to process your personal data for a purpose other than those mentioned above or related to those mentioned above, we will provide you with required notice and obtain your consent where it is necessary to do so.

3. Monitoring

We have industry standard security measures to keep our systems and premises secure. The security measures implemented for the processing of personal data either routinely or occasionally (as appropriate), include:

- Email security – We have email security measures in place that involve automated scanning of incoming and outgoing emails for potential threats.

Threats, such as phishing emails or malware may be escalated to the IT Department for consideration.

- Activity logs – We have audit trail capabilities as part of our automated systems to track who accesses and amends data. This means that we have access to information about your usage of login credentials, websites and applications, which may be referred to in the event of need.
- CCTV – We may operate CCTV to help keep our premises secure. Images of you may be captured as part of the CCTV operation, however, we only view images where an incident has occurred or necessary for monitoring.
- We may also perform aggregated non-anonymous system scans to help improve our services, tools and compliance. Any such scan will be proportional to our specific legitimate business interests and will be consistent with applicable local law.

This processing is necessary for the purposes of the legitimate interests pursued by us to keep our customer's data, our business data and your Personal Data or Sensitive Personal Data secure and confidential and in some cases to protect or defend our legal rights or obey orders of courts or authorities.

4. Who we may share your Personal Data with (the recipients or categories of recipients of the personal data)

- Your information may be shared internally, including with members of the HR and recruitment team, compensation and benefits (including payroll), Finance team, managers, management of the Company, legal, disciplinary or ethics or compliance team, IT staff or other functionaries if access to the data is necessary for the performance of their roles either in the country of data collection or outside the country of data collection. We have offices and operations in a number of international locations and we share information between our group companies for business and administrative purposes.
- We may share your Personal Data or Sensitive Personal data with third parties in order to carry out certain activities
 - to help us to run our business (such as payroll processing, cloud service providers, IT support vendors, external audits),
 - to provide you with certain benefits as required under law (such as pension, social security or health insurance schemes etc.,),
 - to facilitate your corporate travel and expense (corporate card vendors, travel and immigration vendors, foreign exchange suppliers and other third parties connected with a legitimate purpose related to travel),
 - to carry out background verification (background verification agencies and local authorities) and to facilitate audits (third party auditors).

Some of these organizations will process your personal data on our behalf and in accordance with our instructions. Other organizations will be responsible to you directly as a data controller for their use of the personal data that we share with them. Information on the data controllers and their contact information will be made available to you on request. The data controllers will process your personal data in accordance with their own data protection policies (which will apply to their use of your data).

Where required or permitted by law, information may be provided to others, such as regulators and law enforcement agencies.

- Where required for your role, your business contact details may be shared with our clients, other business partners and suppliers.
- We may also share your CV's and background verification status to customers, upon request, to comply with our contractual obligations.
- From time to time, we may consider corporate transactions such as a merger, acquisition, reorganization, asset sale, or similar. In these instances, we may transfer or allow access to information to enable the assessment and undertaking of that transaction. If we buy or sell any business or assets, personal data may be transferred to third parties involved in the transaction.
- To comply with our statutory and other obligations and for the proper management of the business operations of the Company and our service providers or customers, we may also provide information to other third parties, including, but not limited to, auditors, accountants, lawyers and other professional advisers, as well as to administrative authorities, courts, law enforcement and/or regulatory authorities, arbitrators, experts, adverse parties and/or their advisors.

5. International transfers of Personal Data

We may transfer your Personal Data or Sensitive Personal Data to countries outside the European Union (EU) for the purposes mentioned in this notice. Our parent or subsidiaries and branches may receive such Personal Data or Sensitive Personal Data. Details of our subsidiaries and branches can be found on our website www.itcinfotech.com.

We may also transfer your Personal Data or Sensitive Personal Data to our third party suppliers outside the European Union where necessary for processing activities mentioned in section 2 of this notice.

Where we transfer personal data outside of European Union or the European Economic Area, we either transfer personal data to countries that provide an adequate level of protection (as determined by the European Commission) or where we have appropriate contractual safeguards in place.

If you would like more information on the any of the data transfer mechanisms on which we rely please contact us at HR.GDPR@itcinfotech.com.

6. Security of Personal Data and Sensitive Personal Data

We have implemented industry standard security measures to keep your Personal Data and Sensitive Personal Data secure and confidential, including and not limited to the following:

- Limiting access to any personal data that may be submitted by you, to those employees or third parties strictly on a need to know bases, such as to respond to your inquiry or request.

- Physical, electronic, administrative, technical and procedural safeguards that comply with applicable laws and regulations to protect your Personal Data and Sensitive Personal Data from unauthorized or inappropriate access, alteration, disclosure and destruction. It is also important for you to protect yourself and your computers/smartphones, iPads or documents against unauthorized access to your password and to your computer.
- Employees who misuse Personal Data or Sensitive Personal Data are subject to strict disciplinary action.

7. Location and Period of retention

Your Personal Data and Sensitive Personal Data may be received, processed and retained in England, European Union countries, the US, and India. These may also be accessed electronically from these locations.

We store Personal Data and Sensitive Personal Data in line with legal, regulatory, financial and best-practice business requirements. Your Personal Data will be retained in accordance with our *data retention policy* and/or legal or regulatory requirement.

8. The existence of Automated Profiling and Decision Making

We may use any automated decision making (including profiling) tool to process your Personal Data or Sensitive Personal Data, however in the event that such automated decision making tool or software is implemented, we shall use the same within the legal framework of personal data protection applicable and for legitimate purposes.

9. Your rights

- You may have certain rights relating to your Personal Data under applicable law, such as the right to request access to your personal data and the processing activities performed.
- Request that your personal data is rectified if it is inaccurate or incomplete.
- Request erasure of your personal data in certain circumstances.
- Request that the processing of your personal data is restricted in certain circumstances.
- Object to the processing of your personal data in certain circumstances.
- Receive your personal data provided to us as a controller in a structured, commonly used and machine-readable format in certain circumstances.
- Lodge a complaint with supervisory authority.
- Object to, and not to be subject to a decision based solely on, automated processing (including profiling), which produces legal effects or significantly affects you.
- Withdraw your consent provided at any time by contacting us.

Please ensure that the information that we hold about you is accurate and up to date by keeping us informed of any changes that you become aware of.

You have access to view/ extract/ rectify certain aspects of your personal data via the Café Express and other associated portals. In order to receive more details or carry out any specific rectifications to your personal data please contact HR.GDPR@itcinfotech.com.

To exercise the rights outlined above in respect of your personal data you may also contact ITC Infotech Data Protection Officer at the email address DPO@itcinfotech.com.

10. Effective Date

This Notice is effective as of 25th May 2018 and we will notify you of changes we may make to this Notice.

11. Questions

If you have any questions about this Notice or wish to

- (i) access or review your Personal Data and Sensitive Personal Data or learn more about who has access to your Personal Data (i.e., enforce your privacy rights), or
- (ii) make another type of request related to your Personal Data and Sensitive Personal Data, including the rectification of any inaccurate data or to object, at any time and for free to the processing of your data for direct marketing purposes,

Please contact the Data Protection Officer at the email address DPO@ITCInfotech.com

12. Complaints

Any complaints received about the use of Personal Data and Sensitive Personal Data should be promptly directed to the Data Protection Officer at the email address DPO@ITCInfotech.com

Acknowledgement:

I agree with the Company using my Personal Data and Sensitive Personal Data as per the above statements.

Agreed and Accepted:

Name:

Designation:

Place:

Date: