Vikram Solar (Vikram Solar Limited and its subsidiaries, the "Company", "we" or "our")

IT AND COMMUNICATIONS SYSTEMS POLICY

6th of July, 2018

1 ABOUT THIS POLICY

1.1 Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take if these standards are not met.

1.2 This policy applies to all employees, officers, consultants, third party contractors/vendors, volunteers, interns, casual workers, agency workers and anyone who has access to our IT and communications systems.

1.3 Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy may be dealt with under our disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2 PERSONNEL RESPONSIBLE FOR THE POLICY

2.1 Our IT Department has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been assigned to the Head of the IT Department and the Legal Department.

2.2 Managers have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for their supporting colleagues and ensuring its success.

2.3 The IT Department will deal with requests for permission or assistance under any provisions of this policy, and may specify certain standards of equipment or procedures to ensure security and compatibility.

3 EQUIPMENT SECURITY AND PASSWORDS

3.1 You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this policy.

3.2 You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence.

(i) Anyone who is not authorised to access our network will be allowed to access internet only via the Company guest network.

(ii) Anyone who is required to work on a Company device will be allowed to work under the supervision of the Company authority only.

3.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without consulting the IT Department.

3.4 You should use passwords on all IT equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by Head of department. On the termination/retirement of employment, you must provide details of your passwords to the IT Department and return any equipment, key fobs or cards.

3.5 If you have been issued with a laptop, tablet computer, BlackBerry, smartphone or other mobile device ("**Business Device**"), you must ensure it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure confidential data are protected in the event of loss or theft. Please be aware that when using Business Devices away from the workplace, documents may be read by third parties, for example, passengers on public transport.

3.6 If you lose any of your Business Device(s) or it is stolen, you must immediately inform the Head of your concerned department and IT department. In case of unavailablity of Head of your concerned department, you must inform the concerned Admin department and also the IT department.

4 SYSTEMS AND DATA SECURITY

4.1 You should not delete, destroy or modify existing systems, programs, information or data except as authorised in the proper performance of your duties.

4.2 You must not download or install software from external sources without authorisation from the IT Department. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Any external files and data should always be virus-checked by the IT Department before they are downloaded. If in doubt, staff should seek advice from IT Department.

4.3 You must not attach any external device such as USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way without authorisation from the IT Department.

4.4 The Company uses Google Apps for basic suite for email and Google services. The emails are automatically scanned for viruses by Google. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious. You must inform the IT Department immediately if you suspect your computer may be infected by virus. The IT department reserve the right to delete or block access to emails or attachments in the interests of security.

4.5 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

4.6 You must be particularly vigilant if you use the Company IT equipment outside the workplace and take such precautions to protect it from viruses. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our IT Code of Conduct.

5 EMAIL

5.1 Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. The disclaimer is already included by the Company e-mail administrator. Hard copies of emails if required, should be maintained appropriately. If you receive any suspicious e-mails, you should not open any attachments or click on any link and must immediately inform the IT department.

5.2 As a best practice, you should access your emails regularly, stay in touch by remote access when travelling in connection with business, and use an out of office response when away from the office for more than a day. You should endeavour to respond to emails marked "high priority" at the earliest.

5.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. Anyone who feels that they are being or have been harassed or bullied, or is offended by material received from a colleague via email, should inform the Head of the Human Resources Department.

5.4 You must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it were forwarded to colleagues or third parties, or found its way into the public domain.

5.5 Email messages are required to be disclosed in legal proceedings in the same way as paper documents.

5.6 In general, you should not:

(a) Send, forward or read private emails at work which you would not want a third party to read.

(b) Send or forward chain mail, junk mail, cartoons, jokes or gossip.

(c) Contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list.

(d) Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals.

(e) Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter.

(f) Download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear the owner of such works allows this.

(g) Send messages from another person's email address or under an assumed name.

(h) Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

5.7 If you receive an email in error you must inform the sender.

5.8 Do not use your own personal email account to send or receive email for the purposes of our business. Use only the email account we have provided for you.

5.9 We do not permit access to web-based personal email owing to additional security risks.

6 USING THE INTERNET

6.1 Internet access is provided primarily for business purposes.

6.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in Paragraph 9.1, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature. This is further considered under Paragraph 9.

6.3 You must not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in your country may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

6.4 Except as authorised in the proper performance of your duties, you must not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

6.5 The following must never be accessed from our network for personal purposes: online radio, audio and video streaming, instant messaging, webmail such as Gmail or Hotmail and social networking sites (including, but not limited to, Facebook, Twitter, YouTube, Google+, Instagram, SnapChat, Pinterest, Tumblr, Second Life). This list may be modified from time to time.

7 PERSONAL USE OF OUR SYSTEMS

7.1 Personal use must meet the following conditions:

(a) Personal use must not interfere with business or office commitments.

(b) Personal emails should be avoided from the Company e-mail address.

(c) Personal use must not commit us to any marginal costs.

(d) Personal use must comply with this policy (see in particular Paragraph 5 and Paragraph 6) and our other policies including the IT Code of Conduct.

7.2 You should be aware that personal use of our systems may be monitored (see Paragraph 8) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see Paragraph 9). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

8 MONITORING

8.1 Our systems enable us to monitor telephone, email, voicemail, internet usage, file activity and data transfer. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

8.2 A CCTV system monitors the entry and exit points, common area, emergency exit, data centre, meeting rooms, shop floors, canteen area and all other critical locations of the office, plants, warehouse, branch offices etc., for 24 hours a day. This data is also recorded and it can be retrieved for investigation purpose.

8.3 We reserve the right to retrieve the contents of email messages, internet usage (including pages visited and searches made), File activity and log monitoring as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(a) To monitor whether use of the email system, the internet and other applications is legitimate and in accordance with this policy.

(b) To find lost messages or to retrieve messages lost due to computer failure.

(c) To assist in the investigation of alleged wrongdoing.

(d) To comply with any legal obligation.

9 Prohibited Use of Our Systems

9.1 Misuse of our telephone or email system, internet, printing devices, mobile/ipad/tab etc will be dealt with under our disciplinary procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

(a) Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).

(b) Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients or customers.

(c) A false and defamatory statement about any person or organisation.

(d) Material which is discriminatory, offensive, derogatory or may cause embarrassment to others.

(e) Confidential information about us, our business, or any of our staff, clients or customers (except as authorised in the proper performance of your duties).

(f) Unauthorised software.

(g) Any other statement which is likely to create any criminal or civil liability (for you or us).

(h) Music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

9.2 Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our disciplinary procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

10 Collection, use and transfer of Personal Data

10.1 Personal Data means any information about an individual from which that person can be identified.

10.2 Collection, use and transfer of Personal Data shall be treated in accordance with our Data Retention Policy.

---------- END ----------