University of Allahabad
WI-FI ACCESS TERMS AND CONDITIONS

This agreement sets out the terms and conditions on which wireless internet access ("the Service") is provided free of charge to you, a guest, vendor, board member or employee of the University of Allahabad ("The University").

Your access to the Service is completely at the discretion of The University. Access to the Service may be blocked, suspended, or terminated at any time for any reason including, but not limited to, violation of this Agreement, actions that may lead to liability for The University, disruption of access to other users or networks, and violation of applicable laws or regulations. The University reserves the right to monitor and collect information while you are connected to the Service and that the collected information can be used at discretion of The University, including sharing the information with any law enforcement agencies, The University partners and/or The University vendors.

The University may revise this Agreement at any time. You must accept this Agreement each time you use the Service and it is your responsibility to review it for any changes each time.

We reserve the right at all times to withdraw the Service, change the specifications or manner of use of the Service, to change access codes, usernames, passwords or other security information necessary to access the service.

IF YOU DO NOT AGREE WITH THESE TERMS, INCLUDING CHANGES THERETO, DO NOT ACCESS OR USE THE SERVICE.

1. DISCLAIMER

You acknowledge

that the Service may not be uninterrupted or error-free;

that your device may be exposed to viruses or other harmful applications through the Service;

that The University does not guarantee the security of the Service and that unauthorized third parties may access your computer or files or otherwise monitor your connection;

that The University's ability to provide the Service without charge is based on the limited warranty, disclaimer and limitation of liability specified in this Section and it would require a substantial charge if any of these provisions were unenforceable;

that The University can at any point block access to Internet Services that they deem violate the acceptable terms of use outlined in 2.1.

The service and any products or services provided on or in connection with the service are provided on an "as is", "as available" basis without warranties of any kind. All warranties, conditions, representations, indemnities and guarantees with respect to the content or service and the operation, capacity, speed, functionality, qualifications, or capabilities of the services, goods or personnel resources provided hereunder, whether express or implied, arising by law, custom, prior oral or written statements by The University, or otherwise (including, but not limited to any warranty of satisfactory quality, merchantability, fitness for particular purpose, title and non-infringement) are hereby overridden, excluded and disclaimed.

2. ACCEPTABLE USE OF THE SERVICE

2.1 You must not use the Service to access Internet Services, or send or receive e-mails, which:

- 2.1.1 are defamatory, threatening, intimidating or which could be classed as harassment;
- 2.1.2 contain obscene, profane or abusive language or material;
- 2.1.3 contain pornographic material (that is text, pictures, films, video clips of a sexually explicit or arousing nature);
- 2.1.4 contain offensive or derogatory images regarding sex, race, religion, colour, origin, age, physical or mental disability, medical condition or sexual orientation;
- 2.1.5 contain material which infringe third party's rights (including intellectual property rights);
- 2.1.6 in our reasonable opinion may adversely affect the manner in which we carry out our work;
- 2.1.7 are bulk and/or commercial messages;
- 2.1.8 contain forged or misrepresented message headers, whether in whole or in part, to mask the originator of the message;
- 2.1.9 are activities that invade another's privacy; or
- 2.1.10 are otherwise unlawful or inappropriate;

2.2 Music, video, pictures, text and other content on the internet are copyright works and you should not download, alter, e-mail or otherwise use such content unless certain that the owner of such works has authorised its use by you.

2.3 You must not use the service to access illegally or without authorization computers, accounts, equipment or networks belonging to another party, or attempting to penetrate security measures of another system. This includes any activity that may be used as a precursor to an attempted system penetration, including, but not limited to, port scans, stealth scans, or other information gathering activity.

2.4 You must not use the service to distribute Internet Viruses, Trojan Horses, or other destructive software.

2.5 The Service is intended for The University guest use only. Access to this Service must not be used for commercial activity.

2.6 We may terminate or temporarily suspend the Service if we reasonably believe that you are in breach of any provisions of this agreement including but not limited to clauses 2.1 to 2.5 above.
2.7 We recommend that you do not use the service to transmit or receive any confidential information or data and should you choose to do so you do so at your own risk.

3. CRIMINAL ACTIVITY

3.1 You must not use the Service to engage in any activity which constitutes or is capable of constituting a criminal offence, either in the United States or in any country throughout the world.
3.2 You agree and acknowledge that we may be required to provide assistance and information to law enforcement, governmental agencies and other authorities.
3.3 You agree and acknowledge that we will monitor your activity while you use this service and keep a log of the Internet Protocol ("IP") addresses of any devices which access the Service, the times when they have accessed the Service and the activity associated with that IP address
3.4 You further agree we are entitled to co-operate with law enforcement authorities and rights-holders in the investigation of any suspected or alleged illegal activity by you which may include, but is not limited to, disclosure of such information as we have (whether pursuant to clause 3.3 or otherwise), and are entitled to provide by law, to law enforcement authorities or rights-holders.

4. OTHER TERMS

4.1 Under no circumstances will The University, their suppliers or licensors, or their respective officers, directors, employees, agents, and affiliates be liable for consequential, indirect, special, punitive or incidental damages, whether foreseeable or unforeseeable, based on claims of the Guest or its appointees (including, but not limited to, unauthorized access, damage, or theft of your system or data, claims for loss of goodwill, claims for loss of data, use of or reliance on the service, stoppage of other work or impairment of other assets, or damage caused to equipment or programs from any virus or other harmful application), arising out of breach or failure of express or implied warranty, breach of contract, misrepresentation, negligence, strict liability in tort or otherwise.
4.2 You agree to indemnify and hold harmless The University and its suppliers, licensors, officers, directors, employees, agents and affiliates from any claim, liability, loss, damage, cost, or expense (including without limitation reasonable attorney's fees) arising out of or related to your use of the Service, any materials downloaded or uploaded through the Service, any actions taken by you in connection with your use of the Service, any violation of any third party's rights or an violation of law or regulation, or any breach of this agreement. This Section will not be construed to limit or exclude any other claims or remedies that The University may assert under this Agreement or by law.
4.3 This Agreement shall not be construed as creating a partnership, joint venture, agency relationship or granting a franchise between the parties. Except as otherwise provided above, any waiver, amendment or other modification of this Agreement will not be effective unless in writing and signed by the party against whom enforcement is sought. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding will not affect the validity of the other provisions of this Agreement.
4.4 The University' performance of this Agreement is subject to existing laws and legal process, and nothing contained in this Agreement shall waive or impede The University' right to comply with law enforcement requests or requirements relating to your use of this Service or information provided to or gathered by The University with respect to such use. This Agreement constitutes the complete and entire statement of all terms, conditions and representations of the agreement between you and The University with respect to its subject matter and supersedes all prior writings or understanding.

By agreeing to the terms of service, I confirm that I accept these terms and conditions as the basis of my use of the wireless internet access provided.

STATUTORY WARNINGS:
वैधानिक चेतावनी

Information and Communications Technologies (ICTs) have greatly enhanced our capacities to collect, store, process and communicate information, ironically these very capacities of technology which make us vulnerable to intrusions of our privacy on a previously impossible scale, on several accounts:
Firstly, data on our own personal computers can compromise us in unpleasant ways — with consequences ranging from personal embarrassment to financial loss.
Secondly, transmission of data over the Internet and mobile networks is equally fraught with the risk of interception — both lawful and unlawful — which could compromise our privacy.
Thirdly, in this age of cloud computing when much of "our" data — our emails, chat logs, personal profiles, bank statements, etc., reside on distant servers of the companies whose services we use, our privacy becomes only as strong as these companies' internal electronic security systems.
Fourthly, the privacy of children, women and minorities tend to be especially fragile in this digital age and they have become frequent targets of exploitation.
Fifthly, Internet has spawned new kinds of annoyances from electronic voyeurism to spam or offensive email to 'phishing' — impersonating someone else's identity for financial gain — each of which have the effect of impinging on one's privacy.
Although there are a number of technological measures through which these risks can be reduced, it is equally important to have a robust legal regime in place which lays emphasis on the maintenance of privacy. This note looks at whether and how the Information Technology Act that we currently have in India measures up to these challenges of electronic privacy.
The IT Act defines a 'computer resource'; expansively as including a "computer, computer system, computer network, data, computer database or software". As is evident, this definition is wide enough to cover most intrusions which involve any electronic communication devices or networks — including mobile networks.
Briefly, then IT Act provides for both civil liability and criminal penalty for a number of specifically proscribed activities involving use of a computer — many of which impinge on privacy directly or indirectly. These will be examined in detail in the following sub-sections.

Intrusions into computers and mobile devices

- accessing
- downloading/copying/extraction of data or extracts any data
- introduction of computer contaminant; or computer virus
- causing damage either to the computer resource or data residing on it
- disruption
- denial of access
- facilitating access by an unauthorized person
- charging the services availed of by a person to the account of another person,
- destruction or diminishing of value of information
- stealing, concealing, destroying or altering source code with an intention

The Act provides for the civil remedy of "damages by way of compensation" for damages caused by any of these actions. In addition anyone who "dishonestly" and "fraudulently" does any of these specified acts is liable to be punished with imprisonment for a term of up to three years or with a fine which may extend to five lakh rupees, or with both.

Children's privacy online

The newly inserted section 67B of the IT Act (2008) attempts to safeguard the privacy of children below 18 years by creating a new enhanced penalty for criminals who target children.
The section firstly penalizes anyone engaged in child pornography. Thus, any person who "publishes or transmits" any material which depicts children engaged in sexually explicit conduct, or anyone who creates, seeks, collects, stores, downloads, advertises or exchanges this material may be punished with imprisonment upto five years (seven years for repeat offenders) and with a fine of upto Rs. 10 lakh.
Secondly, this section punishes the online enticement of children into sexually explicitly acts, and the facilitation of child abuse, which are also punishable as above.
Viewed together, these provisions seek to carve out a limited domain of privacy for children from would-be sexual predators.
The section exempts from its ambit, material which is justified on the grounds of public good, including the interests of "science, literature, art, learning or other objects of general concern". Material which is kept or used for bona fide "heritage or religious purpose" is also exempt.
In addition, the newly released Draft Intermediary Due-Diligence Guidelines, 2011require 'intermediaries' to notify users not to store, update, transmit and store any information that is inter alia, "pedophilic" or "harms minors in any way". An intermediary who obtains knowledge of such information is required to "act expeditiously to work with user or owner of such information to remove access to such information that is claimed to be infringing or to be the subject of infringing activity". Further, the intermediary is required to inform the police about such information and preserve the records for 90 days.

Electronic Voyeurism

Responding to the growing trend of such electronic voyeurism, a new section 66E has been inserted into the IT Act which penalizes the capturing, publishing and transmission of images of the "private area" of any person without their consent, "under circumstances violating the privacy" of that person.
This offence is punishable with imprisonment of upto three years or with a fine of upto Rs. two lakh or both.

Phishing – or Identity Theft

The word 'phishing' is commonly used to describe the offence of electronically impersonating someone else for financial gain. This is frequently done either by using someone else's login credentials to gain access to protected systems, or by the unauthorized application of someone else's digital signature in the course of electronic contracts. Increasingly a new type of crime has emerged wherein SIM cards of mobile phones have been 'cloned' enabling miscreants to make calls on others' accounts. This is also a form of identity theft.
Two sections of the amended IT Act penalize these crimes:
Section 66C makes it an offence to "fraudulently or dishonestly" make use of the electronic signature, password or other unique identification feature of any person. Similarly, section 66D makes it an offence to "cheat by personation" by means of any 'communication device' or 'computer resource'.
Both offences are punishable with imprisonment of up to three years or with a fine of up to Rs. one lakh.

Spam and Offensive Messages

Although the advent of e-mail has greatly enhanced our communications capacities, most e-mail networks today remain susceptible to attacks from spammers who bulk-email unsolicited promotional or even offensive messages to the nuisance of users. Among the more notorious of these scams is/was the so-called "section 409 scam" in which victims receive e-mails from alleged millionaires who induce them to disclose their credit information in return for a share in millions.
Section 66A of the IT Act attempts to address this situation by penalizing the sending of:

- any message which is grossly offensive or has a menacing character
- false information for the purpose of causing annoyance, inconvenience, danger, insult, criminal intimidation, enmity, hatred or ill-will
- any electronic e-mail for the purpose of causing annoyance or inconvenience, or to deceive the addressee about the origin of such messages;
- This offence is punishable with imprisonment upto three years and with a fine

Hoax E-mails Section 66A – Punishment for sending offensive messages through communication service -

Lawful Interception and monitoring of electronic communications under the IT Act

In addition to violations of privacy by criminal and the mischievous minded, electronic communications and storage are also a goldmine for governmental supervision and surveillance. This section provides a brief overview of the provisions in the IT Act which circumscribe the powers of the state to intercept electronic communications.

The newly amended IT Act completely rewrote its provisions in relation to lawful interception. The new section 69 dealing with "power to issue directions for interception or monitoring or decryption of any information through any computer resource" is much more elaborate than the one it replaced, In October 2009, the Central Government notified rules under section 69 which lay down procedures and safeguards for interception, monitoring and decryption of information (the "Interception Rules 2009"). This further thickens the legal regime in this context.

In addition to section 69, the Government has been empowered under the newly inserted section 69B to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource".

"Traffic data" has been defined in the section to mean "any data identifying or purporting to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted." Rules have been issued by the Central Government under this section (the "Monitoring and Collecting Traffic Data Rules, 2009") which are similar, although with important distinctions, to the rules issued under section 69.

Thus, there are two parallel interception and monitoring regimes in place under the Information Technology Act. In the paragraphs that follow, we provide an overview of the regime of surveillance under section 69 — since they are more targeted towards the individual, and consequently the threats to privacy are more severe — while highlighting important differences in the rules drafted under section 69.

Circumstances under which a direction to intercept may be issued

Purposes for which interception may be directed

Under section 69, the powers of interception may be exercised by the authorized officers "when they are satisfied that it is necessary or expedient" to do so in the interest of:

- sovereignty or integrity of India,
- defense of India,
- security of the state,
- friendly relations with foreign states or
- public order or
- preventing incitement to the commission of any cognizable offence relating to above or
- for investigation of any offence.

Under section 69B, the competent authority may issue directions for monitoring for a range of "cyber security" purposes including, inter alia, "identifying or tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security".

What penalties accrue to intermediaries and subscribers for resisting interception?

Section 69 stipulates a penalty of imprisonment upto a term of seven years and fine for any "subscriber or intermediary or any person who fails to assist the agency" empowered to intercept.

Data Protection under the IT Act

Data Retention Requirements of 'Intermediaries'

Section 67C of the amended IT Act mandates 'intermediaries'to maintain and preserve certain information under their control for durations which are to be specified by law.

Any intermediary who fails to retain such electronic records may be punished with imprisonment up to three years and a fine.

Liability for body-corporates under section 43A

The newly inserted section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

It is only the narrowly-defined 'body corporates' engaged in 'commercial or professional activities' who are the targets of this section. Thus government agencies and non-profit organisations are entirely excluded from the ambit of this section.

"Sensitive personal data or information" is any information that the Central Government may designate as such, when it sees fit to.

The "reasonable security practices" which the section obliges body corporates to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central Government.

By defining both "sensitive personal data" and "reasonable security practice" in terms that require executive elaboration, the section in effect pre-empts the courts from evolving an iterative, contextual definition of these terms.

Common Cyber-crime scenarios and Applicability of Legal Sections

Let us look into some common cyber-crime scenarios which can attract prosecution as per the penalties and offences prescribed in IT Act 2000 (amended via 2008) Act.

- **Harassment via fake public profile on social networking site** A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labelled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim.*Provisions Applicable:- Sections 66A, 67 of IT Act and Section 509 of the Indian Penal Code.*
- **Online Hate Community** Online hate community is created inciting a religious group to act or pass objectionable remarks against a country, national figures etc.*Provisions Applicable: Section 66A of IT Act and 153A & 153B of the Indian Penal Code.*
- **Email Account Hacking** If victim's email account is hacked and obscene emails are sent to people in victim's address book.*Provisions Applicable:- Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.*
- **Credit Card Fraud** Unsuspecting victims would use infected computers to make online transactions.*Provisions Applicable:- Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.*
- **Web Defacement** The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.*Provisions Applicable:- Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.*
- **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs** All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information.*Provisions Applicable:- Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.*
- **Cyber Terrorism** Many terrorists are use virtual (GDrive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business.*Provisions Applicable: Conventional terrorism laws may apply along with Section 69 of IT Act.*
- **Online sale of illegal Articles** Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet*Provisions Applicable:- Generally conventional laws apply in these cases.*
- **Cyber Pornography** Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography is.*Provisions Applicable:- Sections 67, 67A and 67B of the IT Act.*
- **Phishing and Email Scams** Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information)*Provisions Applicable:- Section 66, 66A and 66D of IT Act and Section 420 of IPC*
- **Theft of Confidential Information** many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.*Provisions Applicable:- Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.*
- **Source Code Theft** A Source code generally is the most coveted and important "crown jewel" asset of a company.*Provisions applicable:- Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.*
- **Tax Evasion and Money Laundering** Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities.*Provisions Applicable: Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.*
- **Online Share Trading Fraud** It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.*Provisions Applicable: Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC*