

# DRAFT PRIVACY POLICY

## 1. Privacy Policy

### 1.1 Policy Statement:

National Law University, Delhi is committed to protecting the privacy, confidentiality and accuracy of personally identifiable information in accordance with Indian law and international human rights norms. Other than as required by laws that authorize public access to certain types of information, or in response to court orders legal instruments that authorize disclosure, the university shall not part with any personally identifiable information.

This policy applies to any information collected through visits to <http://www.nludelhi.ac.in>, information gathered through the university logins by students, faculties and other staff of the university, CCTV feeds and other information that flows from these activities, which the university pledges to protect. The University's website provides links to other websites. When you leave the NLU-Delhi website, (www.nludelhi.ac.in), you will be visiting sites that are beyond our control. These other sites may send their own cookies to users, collect data, or solicit personal information. The privacy policies and procedures described for this University do not extend to any external links.

The information collected by the university will be within its control and in a manner consistent with applicable laws, existing regulations, University policies and principles which guide such collection.

### 1.2 Authority:

Approved by the Registrar and the Vice Chancellor of National Law University, Delhi.

### 1.3 Scope of the Policy:

This policy is applicable to all members of the NLU Delhi community and visitors to the University. It includes the students, faculty, lecturers/instructors, researchers, staff, third-party contractors, and others with access to the University's and restricted information.

## **2. Information Privacy:**

### **2.1 General Policy:**

NLU-D limits the collection, use, disclosure or storage of information to that which reasonably serves the University's academic, research, or administrative functions, or other legally required purposes. Email correspondences with the university divulge details of e-mail addresses of individual. The university shall not sell or trade the contact details of this nature to any other university or organization. The university shall only use personal information for the purpose for which it was collected. The university shall only use personal information for longer than is required for the purposes for which the information can lawfully be used, or as otherwise required under any other law. The individual concerned has the right to review the information provided, and to ask for inaccurate or deficient information to be corrected. Sensitive personal information of individuals shall not be disclosed by the university, except in accordance with the provisions of existing laws.

### **2.2 Exceptions:**

Such collection, use, disclosure and storage should comply with applicable laws and regulations, and University policies. The University may disclose information in the course of investigations and lawsuits, in response to court orders, for the proper functioning of the University, to protect the safety and well-being of individuals or the community, and as required by law.

## **3. Information Gathered in CCTV footages:**

### **3.1 Purpose:**

The UGC recommends installation of CCTV in the interests of student safety. The objects of ensuring general sense of security crime prevention and community policing initiatives have led to the presence of video surveillance cameras in certain places of the university.

### **3.2 Scope of the technology:**

Video monitoring for security purposes will be consistent with all existing University policies. Such technologies will be used to meet the University's objective to protect persons and property, while avoiding unnecessary intrusions upon academic freedom or individual civil liberties including privacy, freedom of expression and freedom of assembly.

### **3.3 Monitoring the footage and recordings:**

Any information collected through the use of video surveillance equipment is considered University's property and/or records. The Vice Chancellor/Registrar or her/his designee is authorized to determine the specific personnel in the university who shall have access to the video surveillance equipment and recordings.

Disclosure of information obtained from video surveillance to non-University officials or personnel will be subject to review by the Vice Chancellor/Registrar.

Security camera recordings will be retained for a minimum period of 14 days. Recordings from surveillance equipment may be preserved and retained longer than 14 days under specific circumstances. This retention may only occur:

- a. Upon receiving credible notification by law enforcement authorities for an alleged illegal activity;
- b. Upon receiving authorization from the Vice Chancellor for Administration indicating that such retention reasonably appears necessary to protect University operators;
- c. Where there is reasonable belief that the surveillance information may be related to illegal activity that has occurred, is occurring or is imminently about to occur.