VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES (VISTAS)

UNIVERSITY ETHICAL COMMITTEE (NON-RESEARCH)

MINUTES OF THE NINTH MEETING

Meeting No.: UEC/09/2025-26
Academic Year: 2025–2026

Date

18 March 2026

Time

11.00 A.M.

Venue

Ratan Tata Block

Chairperson

Member Secretary

Members Present

The Chairperson welcomed all members to the Ninth Meeting of the University Ethical Committee (Non-Research). The quorum being present, the meeting commenced. The Member Secretary presented the Action Taken Report (ATR) of the previous meeting and informed the Committee that Gender Sensitization programmes, Human Values workshops, POSH awareness sessions, counselling initiatives, Equal Opportunity activities, and student wellbeing programmes had been successfully organized across all Schools and Departments.

Agenda

1. Confirmation of the Minutes of the Eighth Meeting.
2. Review of the Action Taken Report (ATR).
3. Review of Digital Citizenship initiatives for students and faculty.
4. Discussion on Cyber Ethics and Responsible Use of Digital Technologies.
5. Review of Artificial Intelligence (AI) Governance and Ethical AI Practices.
6. Evaluation of Information Security, Cyber Security Awareness, and Data Protection Measures.
7. Discussion on Digital Privacy, Institutional Data Governance, and Cyber Risk Management.

8. Strategies to strengthen cyber resilience, digital literacy, and responsible technology usage.
9. Alignment with **NAAC**, **NIRF**, **IQAC**, National Education Policy (NEP 2020), Digital India initiatives, Data Protection Regulations, and **QS World University Rankings**.
10. Any other matter with the permission of the Chair.

Proceedings of the Meeting

The Chairperson emphasized that digital technologies have become an integral part of higher education and institutional administration. Members agreed that responsible digital citizenship, ethical use of technology, cybersecurity, data privacy, and Artificial Intelligence governance are essential for maintaining institutional integrity, protecting stakeholder information, and supporting quality education.

The Committee reviewed initiatives undertaken to promote **Digital Citizenship** among students, faculty, and staff. Reports indicated that awareness programmes had been conducted on responsible online behaviour, digital etiquette, cyber hygiene, ethical communication, prevention of cyberbullying, responsible social media usage, and digital professionalism. Members appreciated the University's efforts to cultivate responsible digital behaviour across the campus.

The Committee discussed **Cyber Ethics** and emphasized that all stakeholders should use digital resources responsibly while respecting privacy, intellectual property, institutional policies, and legal requirements. Members recommended strengthening awareness on ethical use of online resources, copyright compliance, software licensing, plagiarism prevention, responsible content sharing, and digital communication standards.

The Information Technology Division presented a report on **Information Security** and **Cyber Security** measures implemented across the University. Members reviewed cybersecurity awareness programmes, firewall protection, secure authentication mechanisms, password management policies, antivirus protection, network monitoring, data backup procedures, and incident response protocols. The Committee appreciated the University's proactive approach in strengthening cybersecurity infrastructure.

The Committee extensively reviewed **Artificial Intelligence (AI) Governance** and the ethical use of AI tools in teaching, learning, administration, and assessment. Members acknowledged that AI has significant potential to enhance academic quality, administrative efficiency, and while emphasizing that AI should be used responsibly, transparently, and under appropriate human oversight. Faculty members were encouraged to guide students on ethical AI usage, disclosure of AI-assisted work, and responsible decision-making.

The Committee also reviewed institutional **Data Protection** and **Digital Privacy** measures. Discussions focused on confidentiality of student records, faculty information, examination

records, financial transactions, and institutional databases. Members recommended strengthening access controls, data encryption, user authentication, cybersecurity audits, and awareness regarding data protection policies to safeguard institutional information.

The Committee discussed emerging cyber threats, phishing attacks, ransomware, identity theft, online fraud, and misinformation. Members recommended conducting periodic cybersecurity drills, phishing awareness campaigns, digital literacy workshops, and incident response training to improve institutional cyber resilience.

The Chairperson highlighted that digital governance, cybersecurity, ethical AI adoption, and information security contribute significantly to institutional quality under **NAAC**, **NIRF**, **IQAC**, National Education Policy (NEP 2020), Digital India initiatives, Data Protection Regulations, and **QS World University Rankings**. Members emphasized maintaining comprehensive documentation of cybersecurity audits, AI ethics programmes, digital literacy initiatives, information security policies, and compliance reports for accreditation and quality assurance.

Resolutions Passed

The Committee unanimously resolved to:

1. Strengthen Digital Citizenship awareness among students, faculty, and staff.
2. Promote Cyber Ethics and responsible use of digital technologies across the University.
3. Develop institutional guidelines for the ethical governance and responsible use of Artificial Intelligence (AI).
4. Strengthen Information Security, Cyber Security, and Digital Privacy measures.
5. Conduct regular cybersecurity awareness programmes, phishing simulations, and cyber safety training.
6. Strengthen institutional Data Protection policies and cyber risk management practices.
7. Maintain comprehensive documentation of cybersecurity initiatives, AI governance, digital literacy programmes, and compliance records.
8. Align all digital governance initiatives with **NAAC**, **NIRF**, **IQAC**, National Education Policy (NEP 2020), Digital India initiatives, Data Protection Regulations, and **QS World University Rankings**.

Action Points

Sl. No.	Action Item	Responsibility	Timeline
1	Organize Digital Citizenship and Cyber Ethics awareness programmes	IT Division & IQAC	Every Semester
2	Conduct Cyber Security training and phishing awareness campaigns	Information Technology Division	Quarterly
3	Develop institutional AI Governance Guidelines	University Ethical Committee & IQAC	April 2026
4	Conduct Information Security and Data Protection audits	IT Division	Every Semester
5	Strengthen digital privacy policies and secure data management practices	Registrar & IT Division	Continuous
6	Submit annual Cyber Security and AI Governance compliance reports	Member Secretary	June 2026

Expected Outcomes

The Committee expects the following outcomes:

- Enhanced awareness of Digital Citizenship and Cyber Ethics among all stakeholders.
- Strengthened institutional cyber security, information security, and digital privacy.
- Responsible and ethical adoption of Artificial Intelligence in academic and administrative activities.
- Improved protection of institutional data through robust cybersecurity measures.
- Increased digital literacy, cyber resilience, and responsible technology usage across the University.
- Comprehensive documentation supporting accreditation, statutory compliance, quality assurance, and institutional audits.
- Improved institutional performance under **NAAC**, **NIRF**, **IQAC**, National Education Policy (NEP 2020), Digital India initiatives, Data Protection Regulations, and **QS World University Rankings**.

Conclusion

The Chairperson appreciated the active participation of all members and emphasized that ethical digital governance is essential for the University's future growth and global competitiveness. Members unanimously agreed to strengthen cybersecurity, responsible Artificial Intelligence adoption, information security, and digital citizenship through continuous awareness, policy implementation, monitoring, and institutional collaboration.

The meeting concluded with a vote of thanks proposed by the Member Secretary.

Prepared by

Member Secretary

Reviewed and Approved by

Chairperson

Date: 18 March 2026