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

UNIVERSITY ETHICAL COMMITTEE (NON-RESEARCH)

MINUTES OF THE NINTH MEETING

Meeting No.: UEC/09/2024-25
Academic Year: 2024–2025

Date

18 March 2025

Time

11.00 A.M.

Venue

MGR 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, highlighting the successful implementation of programmes on Gender Equality, POSH awareness, Human Values, Anti-Ragging initiatives, counselling services, and student wellbeing activities.

Agenda

1. Confirmation of the Minutes of the Eighth Meeting.
2. Review of the Action Taken Report (ATR).
3. Discussion on Digital Ethics and Responsible Digital Citizenship.
4. Review of Cyber Security Awareness and Information Security Practices.
5. Ethical Use of Artificial Intelligence (AI) in Teaching, Learning, Administration, and Assessment.
6. Review of Data Privacy, Data Protection, and Cyber Risk Management.
7. Digital Governance and Responsible Use of Social Media.
8. Capacity Building on Cyber Hygiene and Digital Literacy.

9. Alignment with **NAAC**, **NIRF**, **IQAC**, Digital India initiatives, Outcome-Based Education (OBE), and **QS World University Rankings**.
10. Any other matter with the permission of the Chair.

Proceedings of the Meeting

The Chairperson emphasized that rapid digital transformation in higher education has increased the need for ethical and responsible use of technology. Members agreed that digital ethics, cyber security, Artificial Intelligence (AI), and data protection have become essential components of institutional governance and academic excellence.

The Committee reviewed the University's Digital Ethics Policy and discussed the responsibilities of students, faculty members, and administrative staff in ensuring responsible use of digital technologies. Members stressed that ethical behaviour should extend to online learning platforms, digital communication, virtual classrooms, academic collaborations, and social media interactions.

The Information Technology Cell presented an overview of the University's cyber security infrastructure, including network security, firewall management, antivirus protection, data backup procedures, secure authentication mechanisms, and access control policies. Members appreciated the existing cyber security measures and recommended periodic vulnerability assessments, penetration testing, and security audits to strengthen institutional resilience against cyber threats.

The Committee deliberated extensively on the ethical use of Artificial Intelligence (AI) in higher education. Members recognized that AI-powered technologies can enhance teaching, personalized learning, student assessment, academic administration, and decision-making. However, it was unanimously agreed that AI should be used responsibly, maintaining academic integrity, originality, transparency, fairness, and accountability. Faculty members were encouraged to guide students on the appropriate use of AI tools without compromising independent learning or ethical standards.

The Committee also reviewed institutional practices concerning data privacy, confidentiality, and protection of personal information. Members emphasized compliance with applicable data protection regulations and recommended strengthening awareness among students and employees regarding password security, phishing attacks, cyber fraud, identity theft, responsible email communication, and secure handling of institutional data.

The role of social media in academic and professional communication was discussed. Members advised students and employees to maintain professionalism, respect institutional values, avoid misinformation, protect confidentiality, and uphold ethical behaviour while using social media platforms.

The Committee recommended conducting regular cyber security awareness programmes, workshops on Artificial Intelligence ethics, digital literacy sessions, and faculty development

programmes on emerging educational technologies. It was also suggested that digital governance policies be reviewed periodically to address evolving technological challenges.

The Chairperson highlighted that systematic documentation of cyber security training, digital ethics awareness programmes, AI governance initiatives, information security audits, and digital literacy activities would strengthen institutional quality under **NAAC**, **NIRF**, **IQAC**, Digital India initiatives, Outcome-Based Education (OBE), and **QS World University Rankings**.

Resolutions Passed

The Committee unanimously resolved to:

1. Strengthen Digital Ethics and Responsible Digital Citizenship initiatives across the University.
2. Conduct regular cyber security awareness programmes for students, faculty members, and administrative staff.
3. Develop institutional guidelines for the ethical and responsible use of Artificial Intelligence (AI) in academic and administrative activities.
4. Enhance institutional data privacy, information security, and cyber risk management practices.
5. Promote responsible use of social media and digital communication platforms.
6. Conduct periodic cyber security audits and information security assessments.
7. Organize digital literacy and cyber hygiene training programmes every semester.
8. Align digital governance initiatives with **NAAC**, **NIRF**, **IQAC**, Digital India initiatives, Outcome-Based Education (OBE), and **QS World University Rankings**.

Action Points

Sl. No.	**Action Item**	**Responsibility**	**Timeline**
1	Organize Cyber Security Awareness Programmes	IT Cell	Every Semester
2	Develop AI Ethics Guidelines and implementation framework	University Ethical Committee & IQAC	April 2025
3	Conduct Information Security Audits	IT Cell	Half-Yearly

Sl. No.	Action Item	Responsibility	Timeline
4	Organize Digital Literacy and Responsible Social Media workshops	Student Affairs & IQAC	Quarterly
5	Review Data Privacy and Institutional Information Security Policies	IT Cell & Legal Cell	Annual Review
6	Submit Digital Governance Compliance Report	Member Secretary	Quarterly

Expected Outcomes

The Committee expects the following outcomes:

- Enhanced awareness of Digital Ethics and Responsible Digital Citizenship.
- Strengthened cyber security infrastructure and improved protection of institutional information assets.
- Ethical adoption of Artificial Intelligence in teaching, learning, examinations, and administration.
- Improved compliance with data privacy, information security, and digital governance policies.
- Increased digital literacy, cyber hygiene, and responsible online behaviour among students and employees.
- Better preparedness to address emerging technological and cyber security challenges.
- Improved institutional performance under **NAAC**, **NIRF**, **IQAC**, Digital India initiatives, Outcome-Based Education (OBE), and **QS World University Rankings**.

Conclusion

The Chairperson appreciated the valuable contributions made by all members and emphasized that ethical digital practices are essential for safeguarding institutional integrity in an increasingly technology-driven academic environment. Members unanimously agreed to strengthen digital governance, cyber security, Artificial Intelligence ethics, and data protection measures through continuous awareness, training, monitoring, and policy implementation.

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 2025