Cyber Security Policy 2023

The COVID-19 pandemic has impacted the education sector as for the safety of the children and faculty members, all educational institutions have changed the mode of teaching to online from the traditional offline physical classes. Moreover, the National Education Policy of 2020 (NEP, 2020) has emphasized on the revamping of the teaching pedagogy and extensive usage of ICT tools. In this light, the DME Cyber Policy that was adopted on 11/01/2017 is hereby revised to accommodate the changing needs of the education sector while also further strengthening the policy of the institution currently in place.

Objectives:

1. To build a secure and resilient cyberspace for all staff members to secure a positive and progressive teaching-learning environment.
2. To ensure that there is appropriate use of IT and allied services to support learning, teaching, research, administrative, and service functions.
3. To raise awareness among students, faculty members, and staff about the importance of cyber security and to provide education on best practices to mitigate cyber threats.
4. To sensitize adolescents in schools about online behaviour and safety measures through workshops and campaigns.
5. To promote a culture of cyber security within the institution by encouraging students, faculty, and staff to take responsibility for their own cyber security and to be vigilant against cyber threats.
6. To provide opportunities for students and faculty members to develop cyber security skills and conduct research on cyber security topics, including participation in cyber security competitions and research projects.
7. To establish partnerships and collaborations with other institutions, government agencies, and industry experts to share knowledge, resources, and best practices on cyber security.

Ravikant Swami
Digitally signed by Ravikant Swami
Date: 2024.12.24 09:43:30 +05'30'

Delhi Metropolitan Education DME B-12, Sector-62, Noida

8. To establish a system of cyber proctoring for reporting and tracking cyber security incidents, including data breaches, malware infections, and other security breaches.
9. To continually improve the institution's stand on cyber security through ongoing education, training, and awareness initiatives, and through the adoption of new technologies and best practices.

Scope of activities:

DME shall strive towards:-

1. Making it compulsory for the students getting enrolled in any program across the three Schools run under the umbrella of DME to sign a 'Cyber Policy and Anti-Cyber Crime Undertaking' as part of the admission process.
2. Ensuring that there is appropriate use of ICT tools in consonance with NEP, 2020, to support its learning, teaching, research, administrative, and service functions.
3. Organization of awareness programs and workshops for students, faculty members and staff about cyber security, highlighting the importance of cyber security, and providing education on best practices to mitigate cyber threats.
4. Conducting workshops and campaigns to sensitize adolescents in schools about online behaviour and safety measures.
5. Providing opportunities for students and faculty members to develop cyber security skills, conduct research on emerging issues related cyber security and participate in cyber security related events and competitions.
   5.1 DME shall organize a yearly inter-college as well as intra-college event under the broad theme of cyber awareness and protection wherein different competitions will be organized for students such as quizzes, debate competition, poster-making competition, among others.
   5.2 The Cyber Cell shall mandatorily contribute to the DME Newsletter.
   5.3 The Cyber Cell shall establish and publish a blog to spread cyber literacy among institutional stakeholders. Students shall be encouraged to submit their articles on contemporary issues related to Cyber Security for the blog.
   5.4 Group discussions, debates and other such activities shall be carried out across all Schools/Departments on the current trends within the Cyber domain, to deliberate on such issues and find plausible solutions.

Delhi Metropolitan Education DME B-12, Sector 62, Noida

5.5 The faculty members shall be motivated and supported for conducting empirical research through surveys that can form the basis of a comprehensive book on cyber issues and solutions.

6. DME shall create a mechanism to record and monitor occurrences of cyber security issues through the combined efforts of the Cyber Cell and the institutional Proctoring body.
7. The Cyber Cell shall post a "Cyber Security Tip" once every month across all social media handles of DME as well as email it to all staff members as a reminder to keep their digital accounts safe and secure.
8. Enhancing the institutional preparedness on cyber security through guest talks, training of students through workshops by experts in the cyber domain, value added courses on cyber security awareness, and through the adoption of new technologies and best practices.
9. Sessions in collaboration with governmental bodies shall be organized from time to time to sensitize teaching and non-teaching staff on protection from cyber and digital scams.
10. The IT in-charge of the institution shall run antivirus check on the laptops and computer systems of all the staff at DME periodically.

Ravikant Swami

Digitally signed by Ravikant Swami
Date: 2024.12.24 09:43:48 +05'30'

Delhi Metropolitan Education DME Plot-12, Sector-62, Noida