



BHAKTA KAVI NARSINH MEHTA UNIVERSITY, JUNAGADH

(Established vide Government of Gujarat Act No. 23/2015)

ભક્તકવિ નરસિંહ મહેતા યુનિવર્સિટી, જૂનાગઢ

(ગુજરાત અધિનિયમ નં. ૨૦૧૫ દ્વારા સ્થાપિત)

Ref. No./BKNMU/IT-CELL/008/2026

DATE : 15/01/2026

:: પરિપત્ર ::

વિષય : Student Cybersecurity Training Program માટે સાયબર ક્લબ વોલન્ટીયર તરીકે વિદ્યાર્થીઓની વિગતો મોકલવા બાબત.

સંદર્ભ : (1) ઉચ્ચ શિક્ષણ કમિશ્નરશ્રીની કચેરી, ગાંધીનગર (પત્ર ક્રમાંક : ઉશિક/પીઆરઓ/2026/19, તા.13/01/2026

(2) શિક્ષણ વિભાગ, ગુજરાત સરકાર (UNICEF - Agenda for the Volunteer Training)

શ્રીમાન,

ઉક્ત વિષય અન્વયે તથા સંદર્ભ પત્રથી, ભક્તકવિ નરસિંહ મહેતા યુનિવર્સિટી જૂનાગઢ સંલગ્ન તમામ કોલેજોના આચાર્યશ્રીઓ, અનુસ્નાતક કેન્દ્રોના ઇન્ચાર્જશ્રીઓ, માન્ય સંસ્થોના વડાઓ તેમજ અનુસ્નાતક ભવનોના તથા અધ્યક્ષશ્રીઓને જણાવવાનું કે ગુજરાત સરકારના શિક્ષણ વિભાગના કવચ કેન્દ્ર અંતર્ગત એક દિવસીય "Student Cybersecurity Training Program" યુનિસેફ સાથે સંકલનમાં આયોજન કરવાનું થાય છે. આ પ્રોગ્રામનો ઉદ્દેશ્ય કવચ કેન્દ્ર અંતર્ગત કામ કરતા સ્ટુડન્ટ વોલન્ટીયરને સાયબર સલામતી, ડિજિટલ જવાબદારી, ઘટના પ્રતિભાવ અને સંસ્થાકીય તૈયારીની વ્યવહારુ સમજથી સજ્જ કરવાનો છે, જેથી તેઓ તેમની સંસ્થાઓમાં જાણકાર કવચ કેન્દ્ર વોલન્ટીયર તરીકે કાર્ય કરી શકે.

"Student Cybersecurity Training Program" માં ગુજરાત રાજ્યની તમામ ઉચ્ચ તથા ટેકનીકલ શિક્ષણની સરકારી કોલેજો, બિન-સરકારી કોલેજો, બિન-સરકારી અનુદાનિત કોલેજો અને સ્ટેટ યુનિવર્સિટીઓમાંથી કવચ કેન્દ્ર અંતર્ગત આપની સંસ્થામાં સાયબર ક્લબ વોલન્ટીયર તરીકે ૦૫ વિદ્યાર્થીઓ કાર્ય કરે છે. તેમાંથી ૦૨ વિદ્યાર્થીઓની માહિતી "Student Cybersecurity Training Program" માટે જણાવેલ ગુગલ લિંકમાં તા.૧૬/૦૧/૨૦૨૬ રોજ સવારે: ૧૨:૦૦ કલાક સુધીમાં ભરીને મોકલી આપવા જણાવવામાં આવે છે.

ગુગલ લિંક: <https://forms.gle/mTSkw1z8jGvfXiQ99>

આપના સહયોગ બદલ આભાર.

• બીડાણ :

(1) સંદર્ભ પત્રની નકલ

(2) Agenda for the Volunteer Training

પ્રતિ,

ભક્તકવિ નરસિંહ મહેતા યુનિવર્સિટી સંલગ્ન તમામ કોલેજોના આચાર્યશ્રીઓ, અનુસ્નાતક કેન્દ્રોના ઇન્ચાર્જશ્રીઓ, માન્ય સંસ્થોના વડાઓ તેમજ અનુસ્નાતક ભવનોના અધ્યક્ષશ્રીઓ તરફ...

• નકલ સાદર રવાના :

માનનીય કુલપતિશ્રી / કુલસચિવશ્રીના અંગત સચિવશ્રી

• વેબસાઈટ પર પ્રસિદ્ધ તથા યોગ્ય કાર્યવાહી અર્થે :

આઈ.ટી. સેલ


Registrar
Bhakta Kavi Narsinh Mehta
University, Junagadh



ઉચ્ચ શિક્ષણ કમિશનરશ્રીની કચેરી
જનસંપર્ક શાખા, બ્લોક નં. ૧૨/૨, બીજો માળ, ડૉ. જીવરાજ મહેતા ભવન,
ગાંધીનગર, ગુજરાત રાજ્ય.

ક્રમાંક:ઉશિક/પીઆરઓ/૨૦૨૬/૧૮

તા.૧૩/૦૧/૨૦૨૬

પ્રતિ,
રજીસ્ટ્રારશ્રી/ આચાર્યશ્રી અને સાયબર ક્લબ કો-ઓર્ડિનેટર
ઉચ્ચ તથા ટેકનીકલ શિક્ષણની સરકારી કોલેજો,
બિન-સરકારી અનુદાનિત કોલેજો,
ગ્રામવિધાપીઠો, સ્ટેટ યુનિવર્સિટીઓ
(ગુજરાત રાજ્યની તમામ)

વિષય: Cybersecurity Awareness And Creative Handholding (CAWACH) Kendra અંતર્ગત
"Student Cybersecurity Training Program" માટે ૦૨ વિદ્યાર્થીઓની માહિતી આપવા
બાબત.

શ્રીમાન,

ઉપરોક્ત વિષય અન્વયે જણાવવાનું કે, ગુજરાત સરકારના શિક્ષણ વિભાગના કવચ કેન્દ્ર અંતર્ગત એક દિવસીય "Student Cybersecurity Training Program" યુનિસેફ સાથે સંકલનમાં આયોજન કરવાનું થાય છે. આ પ્રોગ્રામનો ઉદ્દેશ્ય કવચ કેન્દ્ર અંતર્ગત કામ કરતા સ્ટુડન્ટ વોલન્ટીયરને સાયબર સલામતી, ડિજિટલ જવાબદારી, ઘટના પ્રતિભાવ અને સંસ્થાકીય તૈયારીની વ્યવહારુ સમજથી સજ્જ કરવાનો છે, જેથી તેઓ તેમની સંસ્થાઓમાં જાણકાર કવચ કેન્દ્ર વોલન્ટીયર તરીકે કાર્ય કરી શકે.

"Student Cybersecurity Training Program" માં ગુજરાત રાજ્યની તમામ ઉચ્ચ તથા ટેકનીકલ શિક્ષણની સરકારી કોલેજો, બિન-સરકારી અનુદાનિત કોલેજો, ગ્રામવિધાપીઠો અને સ્ટેટ યુનિવર્સિટીઓ માંથી કવચ કેન્દ્ર અંતર્ગત આપની સંસ્થામાં સાયબર ક્લબ વોલન્ટીયર તરીકે ૦૫ વિદ્યાર્થીઓ કાર્ય કરે છે. તેમાંથી ૦૨ વિદ્યાર્થીઓની માહિતી "Student Cybersecurity Training Program" માટે જણાવેલ ગુગલ લિંકમાં તા. ૧૬-૦૧-૨૦૨૬ રોજ સવારે: ૧૨:૦૦ કલાક સુધીમાં ભરીને મોકલી આપવા જણાવવામાં આવે છે. ગુગલ લિંક: <https://forms.gle/mTSkw1z8jGyfXIQ99>

માન. ઉચ્ચ શિક્ષણ કમિશ્નરશ્રી અને સી.ઈ.ઓ., કેસીજી ની મળેલ મંજૂરી અન્વયે.

સંયુક્ત કમિશ્નરશ્રી,
ઉચ્ચ શિક્ષણ કમિશ્નરશ્રીની કચેરી
ગાંધીનગર



CAWACH Kendra – Student Cybersecurity Training Program (Final Draft)

1. Program Overview

The **Student Cybersecurity Training Program** is a one-day intensive capacity-building initiative under **CAWACH Kendra**, Education Department, Government of Gujarat, **planned in coordination with UNICEF**. The program aims to equip selected students with practical understanding of cyber safety, digital responsibility, incident response, and institutional preparedness, enabling them to act as informed **CAWACH Kendra Volunteers** within their institutions.

The training aligns with national priorities on digital safety, the **Digital Personal Data Protection Act, 2023**, and ongoing cybercrime awareness initiatives, while remaining student-centric and practice-oriented.

2. Target Audience

- **Student Volunteers / CAWACH Kendra Volunteers**

3. Pre-Training Assessment

A **pre-session online survey** will be shared at least one week prior to the training to:

- Assess baseline understanding of cyber safety themes
- Identify common challenges faced by students
- Adapt session emphasis based on real student experiences

4. Training Agenda (09:00 AM – 4:30 PM)

Time	Section	Description
09:00 – 10:00 AM	Registration & Breakfast	
10:00 – 10:15 AM	Welcome & Icebreaker	• Overview of CAWACH Kendra and program objectives

		• Introduction of facilitators and partner representatives • Context-setting: Why student leadership matters in cyber safety • Icebreaker activity: Common scams, recent platform changes, or cyber concerns encountered by students
10:15 – 11:00 AM	Section 1: Looking Back to Move Forward – Core Digital Safety Foundations	This session serves as a structured recap rather than re-teaching. Key Focus Areas: • Digital citizenship: rights, responsibilities, and ethical online behaviour • Common online threats affecting students: phishing, internship/job scams, scholarship frauds, cyberbullying, harassment • Cyber hygiene practices: strong passwords, 2FA, device security, app permissions • Healthy vs unhealthy digital behaviours: misinformation verification, emotional manipulation online, screen-time balance Emphasis: What has intensified, what has changed, and where students feel uncertain in real-life situations.
11:00 – 11:45 AM	Section 2: When Something Goes Wrong – Introductory Digital Forensics & Incident Response	A hands-on, non-technical session focused on first-response thinking. Participants will learn: • What qualifies as digital evidence • Importance of screenshots, metadata, logs, and timelines • Common mistakes after a cyber incident • How to preserve information safely without escalating harm Outcome: Students understand their role as first-level responders, not investigators, and know when and how to escalate issues responsibly.

11:45 – 12:30 PM	Section 3: Manipulated Realities – Misinformation, Deepfakes & Influence Tactics	This session examines how false and harmful content is deliberately created and amplified. Key Topics: • Design and spread of misinformation campaigns • Role of algorithms, virality, and emotional triggers • Deepfakes and AI-generated media: creation, impact, and risks • Gendered harassment, political misinformation, and AI voice scams Practice Component: Breaking down content critically without shaming, panic, or overcorrection, especially in youth-facing conversations.
12:30 – 1:30 PM	Lunch Break	
1:30 – 2:15 PM	Section 4: What Happens After a Breach – Dark Web, Leaked Data & Stolen Information	This session moves beyond the “do not click links” narrative. Key Concepts: • What the dark web is and is not • Lifecycle of leaked data from student portals, exam databases, and placement systems • How stolen data is sold, reused, and combined over time • Why old data breaches continue to pose risks years later Outcome: Students understand long-term impacts of breaches and the importance of prevention and response.
2:15 – 3:00 PM	Section 5: From Individual Safety to Institutional Responsibility – Law, Policy & Preparedness	This session zooms out from individuals to systems. Coverage Includes: • Student-relevant overview of the Digital Personal Data Protection Act, 2023 • Institutional responsibilities in handling student and staff data • What Cyber Hygiene Policies do (and do not do)

		• Introduction to Cyber Crisis Management Plans (CCMP): triggers, roles, and escalation pathways Clarification: Clear distinction between student responsibilities and institutional authority.
3:00 – 3:45 PM	Section 6: Activity Space – Drafting a Student-Friendly Cyber Safety Policy	Core synthesis activity of the training. Group Task: Draft a simple, realistic Cyber Safety & Incident Response Policy covering: • Cyber hygiene expectations • Incident reporting and escalation flow • Data handling and privacy principles • Social media conduct and communication norms • Roles of students, staff, volunteers, and institutions Focus: Practical usability over legal complexity.
3:45 – 4:00 PM	Closing Reflection & Way Forward	• Reflection on transition from awareness-building to informed support roles • Reinforcing boundaries, responsibility, and ethical conduct • Positioning students as CAWACH Kendra Volunteers and referral points • Overview of post-training engagement opportunities under CAWACH Kendra
4:00 - 4:30 PM	Tea & Coffee	

5. Expected Outcomes

- Improved cyber safety awareness and confidence among students
- Creation of a trained pool of student **CAWACH Kendra Volunteers**
- Stronger linkage between students and institutional cyber response mechanisms
- Enhanced culture of responsible and ethical digital behaviour

6. Certification

Participants who complete the training and activities will receive a “**Certified Student Cyber Safety Volunteer – CAWACH Kendra**”

7. Conclusion

The **CAWACH Kendra Student Cybersecurity Training Program** provides a structured, practical, and future-ready approach to student capacity building. By combining awareness, response readiness, and institutional understanding, the program strengthens cyber safety ecosystems across educational institutions in Gujarat.