Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.

Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

DATE:09-02-2026

To
The principal
Government Degree College,
Chintapalli,
Alluri Sitharama Raju Dist.,

Sir

Sub: Request to grant thee permission to conduct a Certificate Course on Cyber Security

Ref: Proceedings from the State project director PM-USHA-Procs RC No:2519744/rusa-13022/16/2024 dated 21/06/2025.

I hereby submit you that PM USHA GIEI Scheme the college is going to conduct a certificate Course on **Cyber Security** Course Training from **09/1/2026 to 13/2/2026** as per the reference cited above. Through this Certificate course we are going to aware the girl students about the Cyber Security methoda and techniques to them through experts. So, we request you to grant the permission to conduct a 05 Day certificate course on **Cyber Security** Training.

Thanking you sir

Yours Sincerely

In charge of PM-USHA

Government Degree College,

Chintapalli,

Alluri Sitarama Raju Dist.

Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.
Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

PM USHA
UNDER
GIEI SCHEME

Certificate Course

on

CYBER SECURITY

AWARENESS PROGRAMME FOR WOMEN

2025-2026

Date of Activity : 09/02/2026 TO 13/02/2026

Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.

Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

From
The principal
Government Degree College
Chintapalli,
Alluri Sitharama Raju Dist.,

To
Company : EXCELR
vijayawada
Andhra Pradesh

Respected Sir,

Subject: Request to be the Resource Person for Fifteen -Day Certificate Course on "**CYBER SECURITY** Course Training.

Respected Sir,

Greetings from Government Degree College, Chintapalli.

We are pleased to inform you that our college is organizing a Five -Day Certificate Course on "**CYBER SECURITY**" **09/02/2026 to 13/02/2026** at our college. The program aims to create awareness among girl students regarding their Cyber Security to them with the knowledge to face challenges with confidence.

Considering your expertise and distinguished contribution in the field of texttiles, we would be honoured if you could kindly accept our invitation to be the Resource Person for this Certificate Course. Your guidance and insights will greatly benefit our students in increasing their ability for tech development.

We look forward to your valuable presence and request you to kindly confirm your availability at your earliest convenience.

Thanking you in anticipation.

With regards

Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.

Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

CIRCULAR

Date: 09.02.2026

We are pleased to inform to all the faculty members and students that our college is going to conduct a Certificate Course on "**CYBER SECURITY** under PM-USHA GIEI Scheme from 09.02.2026 to 13.02.2026 at College. We are inviting Sri **S.SARATH BABU**, CYBER SECURITY expert, Visakhapatnam. Your active participation is highly encouraged. So let us come together to make this event a impactful one.

With regards,

Principal,

Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.
Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

BRIEF REPORT ON CYBER SECURITY

05-day Certificate Course on "CYBER SECURITY "

Held from **09th FEBRUARY 2026 to 13th FEBRUARY 2026**

INTRODUCTION:

The 5-day Certificate Course on web development with pages, organized at Government Degree College, ChintaPalli from **09th FEBRUARY 2026 to 13th FEBRUARY 2026**, **What is Cyber Security** **Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from threats like hacking, malware, and phishing. Also known as Information Security (INFOSEC), Information Assurance (IA), or System Security.**

- **Protects systems, networks, and personal information**
- **Uses security tools, policies, and safe online practices**
- **Prevents data theft, system damage, and unauthorized access**

Day 1 :

ypes of Cybersecurity

There are seven types of cyber security, each explained below in detail with uses and functions:

1. Network Security

It focuses on securing computer networks from unauthorized access, data breaches, and other network-based threats. This involves implementing technologies such as **Firewalls**, **Intrusion detection systems** (IDS), Virtual private networks (VPNs), and Network segmentation as well as deploying antivirus software

- Using public Wi-Fi in locations like cafes and malls poses significant security risks. Malicious actors on the same network can potentially intercept your online activity, including sensitive information.
- If you use payment gateways on these unsecured networks, your financial data could be compromised because these open networks don't have proper security layers, which means anyone even hackers can watch what you're doing online.
- So, use a secure private network or VPN to protect your internal network from outside threats

2. Application Security

Concerned with securing software applications and preventing vulnerabilities that could be exploited by attackers. It involves secure coding practices, regular software updates and patches, and application-level firewalls.

- Most of the Apps that we use on our cell phones are Secured and work under the rules and regulations of the Google Play Store.
- There are 3.553 million applications in Google Play, Apple App Store has 1.642 million, and Amazon App Store has 483 million available for users to download. With so many choices, it's easy to assume all apps are safe—but that's not true.
- Some apps pretend to be secure, but once installed, they collect personal data and secretly share it with third-party companies.
- The app must be installed from a trustworthy platform, not from some 3rd party website in the form of an APK (Android Application Package).

3. Information or Data Security

Focuses on protecting sensitive information from unauthorized access, disclosure, alteration, or destruction. It includes Encryption, Access controls, Data classification, and Data loss prevention (DLP) measures.

- Incident response refers to the process of detecting, analyzing, and responding to security incidents promptly.
- Promoting security awareness among users is essential for maintaining information security. It involves educating individuals about common security risks, best practices for handling sensitive information, and how to identify and respond to potential threats like phishing attacks or social engineering attempts.
- Encryption is the process of converting information into an unreadable format (ciphertext) to protect it from unauthorized access.

DAY 2 :

Cloud Security

It involves securing data, applications, and infrastructure hosted on cloud platforms, and ensuring appropriate access controls, data protection, and compliance. It uses various cloud service providers such as **AWS**, **Azure**, **Google Cloud**, etc., to ensure security against multiple threats.

- Cloud-based data storage has become a popular option over the last decade. It enhances privacy if configured and managed correctly and saves data on the cloud, making it accessible from any device with proper authentication.
- These platforms offer free tiers for limited usage, and users must pay for additional storage or services
- It is a cloud service provider that offers a wide range of services, including storage, computing, and security tools.

5. Endpoint Security

Refers to securing individual devices such as computers, laptops, smartphones, and IoT devices. It includes antivirus software, intrusion prevention systems (IPS), device encryption, and regular software updates.

- **Antivirus** and **Anti-malware**software that scans and detects malicious software, such as **Viruses**, **Worms**, Trojans, and Ransomware. These tools identify and eliminate or quarantine malicious files, protecting the endpoint and the network from potential harm.
- Firewalls are essential components of endpoint security. They monitor and control incoming and outgoing network traffic, filtering out potentially malicious data packets.
- Keeping software and operating systems up to date with the latest security patches and updates is crucial for endpoint security.

Day 3:

perational Security

Refers to the processes and policies organizations implement to protect sensitive data from internal threats and human errors.

- **Access Controls** ensure that only authorized personnel can access critical systems and sensitive information. This includes role-based access, multi-factor authentication (MFA), and least privilege principles.
- **Risk Management** involves identifying, analyzing, and mitigating security risks within an organization. It includes regular security assessments, vulnerability testing, and compliance audits.

- **Employee Training** is crucial for preventing insider threats and social engineering attacks. Organizations conduct cybersecurity awareness programs to educate employees on phishing scams, password security, and data handling best practices.
- **Monitoring & Incident Response** includes tracking user activity, detecting suspicious behavior, and responding to security incidents in real time. Security Information and Event Management (SIEM) tools help organizations analyze and mitigate threats effectively.

7. Internet of Things (IoT) Security

Refers to protecting internet-connected devices such as smart home gadgets, industrial sensors, medical equipment, and wearable technology from cyber threats. IoT security ensures that these devices do not become entry points for hackers to exploit networks and steal sensitive data.

- **Device Authentication & Encryption** ensures that only authorized devices can connect to networks. Encryption protects data transmitted between IoT devices and servers from interception.
- **Firmware & Software Updates** are crucial to patch security vulnerabilities. Regular updates help prevent exploitation by cybercriminals who target outdated IoT firmware.
- **Network Segmentation** isolates IoT devices from critical systems, reducing the risk of widespread attacks if one device is compromised. This approach limits unauthorized access and lateral movement within a network.
- **IoT Security Standards & Compliance** include implementing industry security frameworks like Zero Trust Architecture (ZTA) and following best practices such as strong password policies, secure APIs, and endpoint protection to enhance IoT device security.

Day 4:

Major Cybersecurity Threats & Attacks

Hackers use advanced techniques to find weaknesses in systems, steal or change data, and break into networks without permission. Below are the most common cybersecurity threats that target businesses, cloud storage, and personal devices:

Read complete article, here: Types of Cyber Attacks

1. Malware Attacks

- Malware is a type of harmful software created to enter, attack, and compromise systems. It includes trojans, rootkits, and spyware.
- Hackers use payload obfuscation, polymorphic techniques, and zero-day exploits to bypass intrusion detection systems (IDS) and endpoint protection platforms (EPP).

2. Phishing & Spear Phishing Attacks

- Phishing uses tricks and manipulation to steal login details, session tokens, and financial information. Spear phishing is a more targeted version that uses open-source intelligence (OSINT) to create personalized fake messages.
- Hackers use domain spoofing, homograph attacks, and malicious macros to bypass security and trick users into revealing sensitive data.

3. Ransomware Attacks

- Ransomware locks important system files by encrypting them using **asymmetric cryptography** (like RSA, ECC) or hybrid encryption (AES-RSA). It then demands a ransom, usually in cryptocurrency, to unlock the data.

- More advanced types, like double extortion ransomware, first steal sensitive data before encrypting it. Hackers then threaten to leak the stolen data on dark web sites if the ransom isn't paid.

4. Distributed Denial-of-Service (DDoS) Attacks

- DDoS attacks overload a network by flooding it with massive amounts of traffic at different levels volumetric, protocol, or application-layer causing servers to crash and making services unavailable.
- Hackers use botnets, amplification techniques to increase attack size, and HTTP flood requests to overwhelm websites. These methods help attackers bypass rate-limiting defenses and take down their targets.

5. SQL Injection (SQLi) & NoSQL Injection

- SQL injection attacks take advantage of weak web application queries by inserting malicious SQL code to modify database records, steal login credentials, or run admin-level commands.
- NoSQL injection targets document-based databases like MongoDB and Firebase by altering query parameters, allowing attackers to bypass authentication and gain unauthorized access to sensitive data.

Day 5

Rising Cyber Threats: How Hackers Exploit Weak Security

Cybercriminals exploit weak security using tactics like phishing, ransomware, social engineering, and AI-driven attacks to steal data, disrupt systems, and cause financial loss.

- Weak passwords, outdated software, and unsecured networks are easy targets
- Phishing and social engineering trick users into sharing sensitive information
- Ransomware and AI-powered bots automate and scale attacks
- Cybersecurity is critical to protect personal and financial data

Example: While shopping online, a fake email posing as Flipkart or Amazon may lure users with an offer; entering saved details can let hackers steal card and personal information, leading to financial loss.

Consequences of Cyber Attacks

Cyber attacks cause severe financial, reputational, and personal damage to both businesses and individuals.

- Businesses face financial losses, legal penalties, and loss of customer trust
- Small businesses are more vulnerable due to weaker security
- Individuals risk identity theft, fraud, and personal data leaks
- Ransomware can lock devices and wipe out bank accounts
- Long-term impacts include emotional stress and financial instability

Cybersecurity Trends in 2025

Cybersecurity has progressed from basic antivirus defenses to today's AI-driven, highly targeted attacks involving ransomware, deepfakes, zero-days, supply chain breaches, and nation-state cyber warfare.

1. Rise of AI and Machine Learning: More cybersecurity tools are using artificial intelligence (AI) and machine learning to detect and respond to threats faster than humans can. AI in cybersecurity helps recognize patterns, block suspicious behavior, and even predict future threats making it one of the most powerful tools to protect sensitive information.

2. Increase in Ransomware Attacks: Ransomware, where hackers lock you out of your data until you pay a ransom, is becoming more common. Companies and individuals alike need to back up their data regularly and invest in security measures to avoid falling victim to these attacks.
3. Cloud Security: As more businesses move their data to the cloud, ensuring this data is secure is a top priority. This includes using strong authentication methods and regularly updating security protocols to protect against breaches.
4. Internet of Things (IoT) Vulnerabilities: With more devices connected to the internet, like smart home gadgets and wearable tech, there's an increased risk of cyberattacks. Ensuring these devices have updated security features is crucial.
5. Zero Trust Security: This approach assumes that threats could come from inside or outside the network, so it constantly verifies and monitors all access requests. It's becoming a standard practice to ensure a higher level of security.
6. Cybersecurity Skills Gap: There is a growing need for skilled cybersecurity professionals. As cyber threats become more sophisticated, the demand for experts who can protect against these threats is higher than ever.
7. Regulatory Compliance: New regulations are being introduced worldwide to protect personal data. Companies must stay informed about these laws to ensure they comply and avoid hefty fines.

How to Stay Safe?

There are several steps you can take to protect yourself from cyber threats, including:

- **Use strong passwords:** Use unique and complex passwords for all of your accounts, and consider using a password manager to store and manage your passwords.
- **Keep your software up to date:** Keep your operating system, software applications, and security software up to date with the latest security patches and updates.
- **Enable two-factor authentication:** Enable two-factor authentication on all of your accounts to add an extra layer of security.
- **Be aware of suspicious emails:** Be cautious of unsolicited emails, particularly those that ask for personal or financial information or contain suspicious links or attachments.
- **Educate yourself:** Stay informed about the latest cybersecurity threats and best practices by reading cybersecurity blogs and attending cybersecurity training programs.

Challenges of Cybersecurity and Tips to Avoid

- **Constantly Evolving Threat Landscape**: Cyber threats are constantly evolving, and attackers are becoming increasingly sophisticated. This makes it challenging for cybersecurity professionals to keep up with the latest threats and implement effective measures to protect against them.

ENCLOSURES :

1.PHOTOS

2. ATTENDANCE SHEET

Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.

Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

PM USHA UNDER GIEI SCHEME

Invites You to a Certificate Course on

"WEB DEVELOPMENT WITH PAGES "

Chief patron :

Dr.Narayan Bharath Gupta, IAS — Director of Collegiate Education, Govt. of Andhra Pradesh

Dr. P. V. Krishnaji — RJDCE of Zone-I

Dr.M.Vijaya Bharathi — principal

Date :

09th Feb

To

13th Feb

Resource person

S.SARATH BABU

Company : Excelr

Vijayawada

Program Highlights

- Expert training session on Technology for women & girls
- Overview of key-topics related to web development with pages

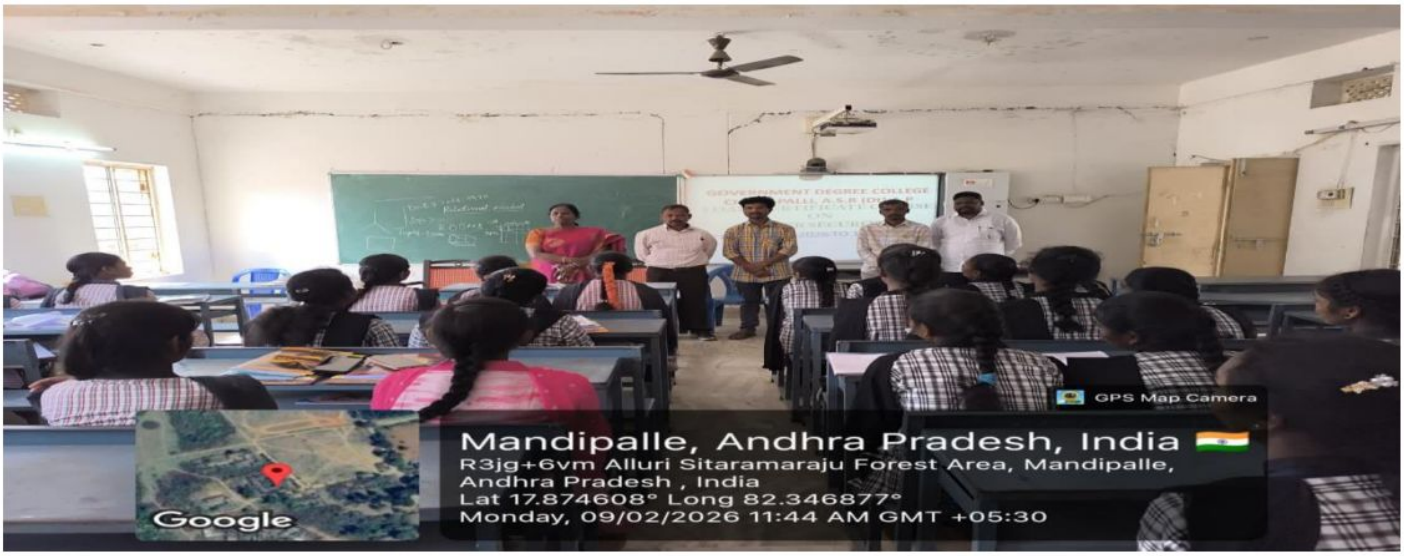
Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.

Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

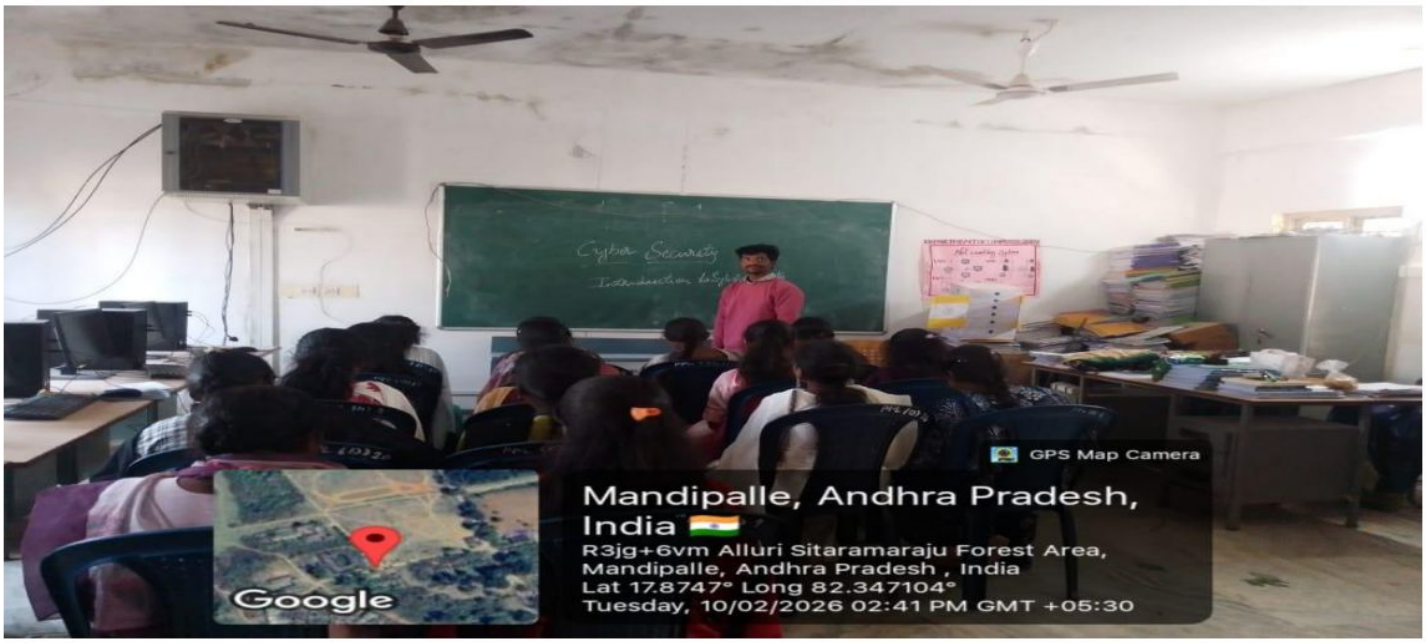
PM USHA Coordinator	Dr.V.Ramana ,lecturer in Zoology
Organizing secretaries	Dr.D.Kejiya,lecturer in English Sri I.Raveendra naik , lecturer in chemistry
Programme convenors	T.B.V.V.S. PRASAD ,Lecturer in COMPUTER APPLACTION S.SARATH BABU lecturer in Computer science
Students representatives	k.Anu (2nd bsc comp science) B.Bhargavi (1st BA (HISTORY)

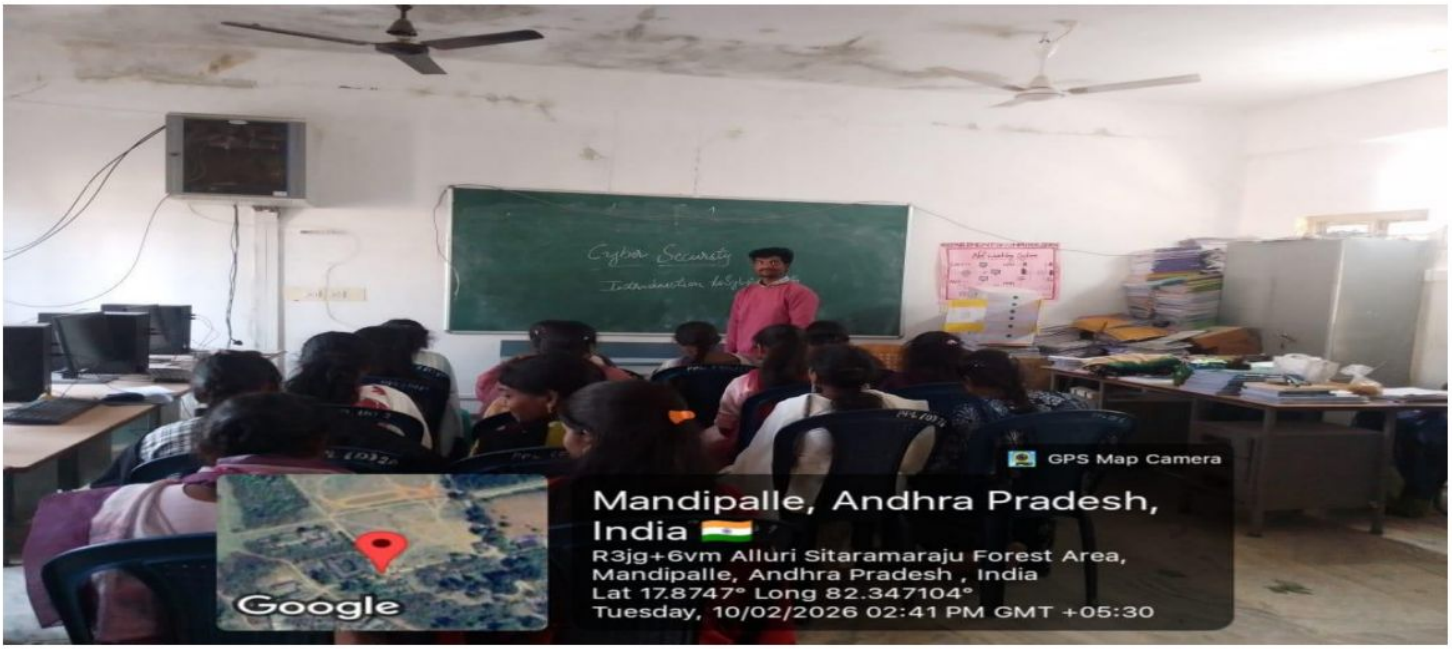
PHOTO GALLERY

DAY -1



DAY:02


Cyber Security
GPS Map Camera
Mandipalle, Andhra Pradesh, India
R3jg+6vm Alluri Sitaramaraju Forest Area, Mandipalle, Andhra Pradesh , India
Lat 17.8747° Long 82.347104°
Tuesday, 10/02/2026 02:41 PM GMT +05:30
Google


Cyber Security
GPS Map Camera
Mandipalle, Andhra Pradesh, India
R3jg+6vm Alluri Sitaramaraju Forest Area, Mandipalle, Andhra Pradesh , India
Lat 17.8747° Long 82.347104°
Tuesday, 10/02/2026 02:41 PM GMT +05:30
Google

DAY:03


GPS Map Camera
Mandipalle, Andhra Pradesh, India
R3jg+6vm Alluri Sitaramaraju Forest Area, Mandipalle, Andhra Pradesh , India
Lat 17.874178° Long 82.348202°
Wednesday, 11/02/2026 12:21 PM GMT +05:30
Google


GPS Map Camera
Mandipalle, Andhra Pradesh, India
R3jg+6vm Alluri Sitaramaraju Forest Area, Mandipalle, Andhra Pradesh , India
Lat 17.874344° Long 82.347391°
Wednesday, 11/02/2026 12:21 PM GMT +05:30
Google

DAY:04

DAY 5


GPS Map Camera
Mandipalle, Andhra Pradesh, India
R3jg+6vm Alluri Sitaramaraju Forest Area, Mandipalle, Andhra Pradesh , India
Lat 17.874412° Long 82.346771°
Friday, 13/02/2026 04:07 PM GMT +05:30
Google

Government Degree College, Chintapalli
Affiliated to Andhra University
Chintapalli, Alluri Sitharama Raju -District, AP.

Phone no: 9666739207. Email.ID: gdcchintapalli@gmail.com

WEB DEVELEOPMENT WITH PAGES TRAINING

5 Days Certificate course on web development with pages

Schedule for Day by Day syllabus

Day	Topic	Sub -topic
1	Introduction to Web Technologies	Internet and World Wide Web, Web browsers and web servers, Website architecture, Basics of HTTP and URLs
2	HTML – Creating Web Pages	Structure of HTML documents, Text formatting, lists, tables, and links, Images, audio, and video embedding, Forms and input elements
3	CSS – Styling Web Pages	Selectors, Properties, and Values, Layout Techniques, Responsive Design and Media Queries
4	JavaScript – Adding Interactivity	Introduction to JavaScrip, Variables, Functions, and Events, Form Validation
5	Web Publishing and Project	Web Hosting and Domains, Uploading Websites, Website Maintenance, Mini Project Development