Annexure to HQ AWES Letter No. B/46031/CS/AWES Dated 06 Dec 2024

Digital Safety and Best Practices

Overview

As we increasingly rely on digital tools and platforms in our educational journey, maintaining a secure and safe digital presence is essential. This document outlines key best practices in digital safety and security, applicable to all students and educators across our entire community of APS and APPS. Following these guidelines will help protect personal information, maintain the integrity of school resources, and create a safer online environment for everyone.

By understanding and adhering to these practices, we collectively contribute to a secure digital experience for our entire school community. Please take a moment to review each of the points carefully and integrate them into your daily digital interactions.

01

Internet and Safe Browsing

A

Best Practices

- Choose a well-known browser like Google Chrome, Firefox or Safari
- Regularly Update your Browser and Plugins
- Go a Step further by using privacy first browsers like DuckDuckGo
- Avoid accessing sites without HTTPS
- Use an Ad Blocker and avoid clicking on Pop-Ups
- Clear Cache and Cookies
- Use a password manager
- Enable "Do Not Track" in your browser

B

At Home

- Change your router's default administrative username and password
- Choose a Strong **Wi-Fi Network Password** and enable WPA2 or WPA3 (Avoid WEP)
- Turn Off Remote Management on your router (WPS and UPnP)
- Setup a Separate "Guest Network" for your guests
- Advanced Users can also turn off Network Name Broadcasting

C

Outside Home or Public Wi-Fi

- Avoid using Public Wi-Fi as much as possible
- Use Private Browsing or Incognito mode when using a public network

Get a Paid VPN, if possible

02

Passwords

ONLINE APPS

- Use different passwords for different accounts
- Configure and Use 2FA/MFA wherever possible
- Use a Strong Password (12-16 Characters)
- Use Passphrases as passwords
- Use a Password manager like 1Password, Bitwarden, KeePass etc.
- Change or rotate your password maximum every 90 days

DEVICE PASSWORD

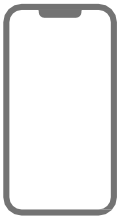
- Don’t share your passwords
- Use a strong password, enable Biometric Protection if available

03

Devices

LAPTOP

- Add a Webcam Cover
- Encrypt your Hard Drive
- Backup your Data on an external source every 90 days
- Install Antivirus
- Use a Privacy Screen
- Avoid Pirated Materials and Apps
- Avoid leaving Laptop unattended in public places or vehicles
- Use a Laptop Lock with Kensington slot
- Use Protective Casing and etch your name or stickers for identification



MOBILE

- Set a strong passcode and don’t share it with others
- Always keep your phone locked when not in use
- Turn on OS and Apps to be updated automatically
- Only download Apps from trusted sources
- Limit Location sharing with both Apps and People Only grant apps the permissions they really need Enable “Find my device” to locate phone if lost/stolen Use an Antivirus if possible
-
-
-
-

Avoid USB charging in public places

-
-
-
-

04

Email ID

- Avoid logging to your email from Public W-Fi
- Enable 2FA using Authenticator Apps or TOTP
- Add/Update your Email Account Recovery Options
- Always log out of your email account after use
- Keep an eye for Security Notifications
- Avoid opening, replying or forwarding to unwanted Emails
- Check the From Name as well as the Email ID to confirm the sender
- Regularly check your account for suspicious logins and devices

05

Social Media

- Avoid sharing personal or sensitive information especially address, mobile numbers and location
- Keep privacy settings of your social media profile at highest restrictions
- Avoid accepting friend/follow requests from people you don't know, as they are commonly used to gather information or spread malware
  Avoid phishing messages which may come in as offers, deals etc and may contain suspicious links
  Avoid granting permissions to third-party apps that request access to your social media accounts
  Think before you post anything
  Avoid geotagging and be careful about sharing travel information, vacation photos etc.
  Regularly monitor your account for any unusual account activity such as unfamiliar posts, likes, messages or login
  Report and flag accounts, comments, or messages that appear spammy, abusive, or inappropriate

-

-

06

WhatsApp

- Enable Two-Step Verification from Account Settings
- Ensure WhatsApp is always updated to the latest version
- Enable “Disappearing Messages” for sensitive chats
- Control Groups Settings to avoid being add to random/suspicious groups
- Regularly review linked devices and delink any unused devices
- Use App Lock for additional security
- Avoid downloading unknown files or media
- Report and Block suspicious contacts
- Limit location sharing to trusted contacts only for limited duration

07

Data and Privacy

- Limit personal data and information shared online
- Use encrypted storage for sensitive information
- Monitor permissions for Apps and Services
- Regularly backup your data both online and offline
- Ensure you do not upload PII Documents like Aadhaar, Pan Card etc on untrusted sites / Public Computers / Printing Shops or delete them post the work is complete.
- Review and limit data collection by Smart Devices like Smart Watches, Home Assistants etc.
- Educate yourself on Data Privacy Laws

08

Cyber Frauds

Report incidents to **https://cybercrime.gov.in/** or call **1930**

Avoid answering any phone/video calls from unknown contacts Think before you click

Avoid sharing any sensitive information with online strangers even if they claim to be investigation officers

If you receive any calls about arrest or investigation, visit the nearest police station

-
-
-
-

09

Beware of Common

2024 Scams

A

Custom Office Scam

You may receive a call from an unknown number claiming that a courier with objectionable items (e.g., SIM cards, drugs) has been sent using your ID proof. They will ask you to log a complaint with cybercrime and offer to transfer your call. The second person will ask for your full address and other personal details, which can be misused.

B

Indian Post Scam

You might receive an SMS, WhatsApp, or iMessage claiming to be from India Post, stating that you have a package at the post office. They will ask you to verify your details by uploading your Aadhar, PAN, and other documents on a fake website. This information can be misused.

C

iCloud Scam

You may receive a message claiming suspicious activity on your Apple ID, prompting you to change your password via a fake link. This can lead to your information being compromised.

D

Police Impersonation Scam

A person with a police profile picture may call you, claiming that a close relative has committed a crime and is under arrest. They may share AI-morphed images taken from social media of that person to convince you and demand money to release and remove the charges. Most of the calls are made from +92 (Pakistan) country code, but they may also call from +91 (India).

E

Digital Arrest Scam

Scammers may call you through WhatsApp, FaceTime, or any video conferencing medium, claiming to be from government authorities. They will insist that you do not disconnect the video call until the case is resolved and that you stay at home. They will create unnecessary pressure to convince you to transfer money in the form of Amazon coupons, UPI transfers or Money transfer. They may reference your recent trip images and connect them to a crime,

showing AI-generated images of that area.