DSCI
PROMOTING DATA PROTECTION
A **nasscom** Initiative

DATA PRIVACY DAY | #DPD2025 | JANUARY 28, 2025

PRIVACY AI
IN THE AGE OF

FROM CITIZENS TO NETIZENS

UNDERSTANDING PRIVACY IN THE AGE OF AI

AI is transforming our world but it also raises new privacy concerns.

This guide provides some essential best practices to help you protect your personal information in the age of AI.

PERSONAL DATA PROTECTION IN CONSUMER AI

(AI ASSISTED DEVICES)

AI is everywhere,
from listening to your favourite album
on AI assisted smart speaker to tracking
your daily steps on your smart watch, it's
crucial to understand how your data is
collected, stored, and used.

AI USAGE BEST PRACTICES

Review and adjust your device and app privacy settings to align with your data-sharing preferences.

Turn off unnecessary features like ad personalization and activity tracking.

Disable microphone access for apps that do not need it to operate.

Regularly check and delete unwanted voice recordings from your smart speaker's activity log.

Restrict or manually activate voice recording features when not in use to prevent unintended recordings.

Avoid using virtual assistants for sensitive tasks, such as banking, unless the platform is verified secure.

DID YOU KNOW?
The virtual assistants market is expecected to reach a value of **$58.17 billion** by 2028 driven by increasing reliance on AI for task automation and smart device integration.
(Source: https://www.g2.com/articles/artificial-intelligence-statistics?)

DIGITAL FOOTPRINT

IN THE AGE OF AI

As AI becomes more integrated into our daily life, every click, search, and interaction contributes to your digital footprint. While AI has enhanced the functionality, convenience, and efficiency of our lives, it's equally important to understand how we can minimize our online footprint.

KEEP IT CLEAN

Regularly review and clean your online presence by deleting old accounts and minimizing shared personal information.

Linking multiple accounts can provide access to many platforms through just one account.

Delete unused or inactive online accounts to reduce your digital footprint.

Regularly clean out unnecessary data and apps to minimize digital clutter.

Log out from previously used apps to safeguard your privacy.

Delete history and cookies of online service providers to reduce the trace of your digital identity.

DID YOU KNOW?

By 2025, it is estimated that the average person will interact with connected devices nearly **4,800 times per day.**

(Source: https://www.statista.com/statistics/948840/worldwide-data-interactions-daily-per-capita/#:~:text=This%20statistic%20shows%20the%20daily,interactions%20per%20day%20by%202025.)
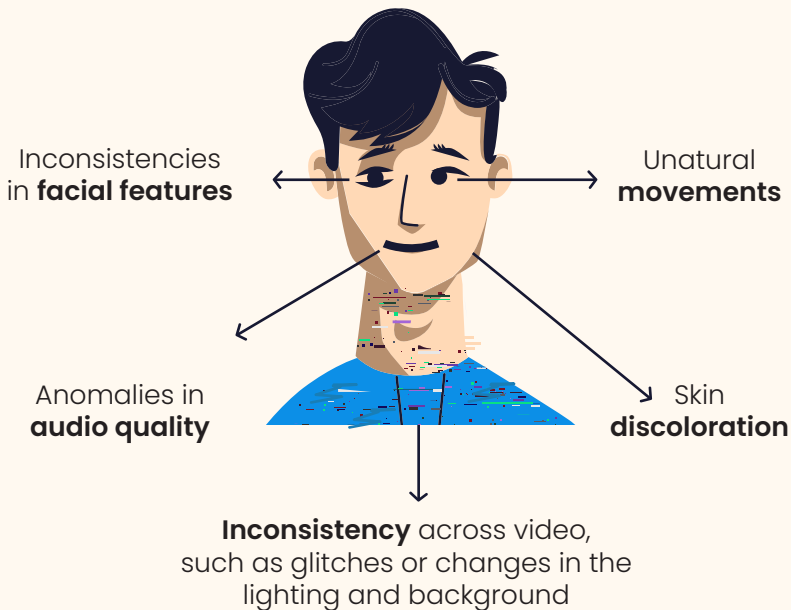
AI-GENERATED
CONTENT & PRIVACY
(DEEPFAKE)

WHAT IS DEEPFAKE?

A video or sound recording that replaces someone's face or voice with that of someone else, in a way that appears real. Deepfake technology uses AI to create hyper-realistic audio, video, and images that can manipulate appearances and voices to deceive viewers.

HOW TO SPOT DEEPFAKES?

Inconsistencies in **facial features**

Unatural **movements**

Anomalies in **audio quality**

Skin **discoloration**

Inconsistency across video, such as glitches or changes in the lighting and background

DID YOU KNOW?

The global market for deepfake technology is projected to exceed **$3 billion** by 2027 as its applications in entertainment, marketing, and cybercrime expand.
(Source: https://www.marketsandmarkets.com/Market-Reports/deepfake-ai-market-256823035.html)

HOW TO AVOID BEING MISLED?

Check credibility of suspicious content from multiple reliable sources.

Look for visible watermarks labels indicating use of AI.

Consider the context before believing content Stay informed on deepfake technology.

Spread awareness and educate others against misleading deepfakes.

Report suspicious content to platforms or websites.

Think before you share or believe.

CHILDREN'S PRIVACY IN
AI WORLD

In today's digital age, kids often use AI-powered devices like smart toys, apps, and games. While these offer fun and learning, they also pose privacy and security risks. Both parents and children must stay vigilant to safeguard data and prevent misuse.

RECOMMENDATIONS FOR PARENTS

Customize privacy settings on apps and devices to control & limit access to personal data collection.

Add an extra layer of security to accounts by enabling multi-factor authentication where possible.

Explain to your child why it's important to keep personal information private and how to spot suspicious online activity.

Make sure the apps your child uses are designed for their age.

Select toys, apps, and devices that prioritize privacy and are transparent about their data practices. Always read privacy policies before purchasing AI-powered products for your children.

As a parent, think carefully before sharing photos or personal details about your child on social media. Once posted, it can be hard to control where that information goes. Remember, their story is theirs to tell.

RECOMMENDATIONS FOR CHILDREN

Don't share sensitive details like your name, address, phone number, or school online.

Limit the permission you give to apps and social media platforms, such as access to contacts or location.

Set privacy to the highest levels on devices, apps, and social media to protect your info.

Tell a trusted adult if you see anything strange or receive messages from strangers on digital platforms.

Create unique, hard-to-guess passwords for each site using a mix of letters, numbers, and symbols to protect it from any kind of intrusion.

AI is cool but it is not a real person. Remember, AI is smart, but it's no substitute for real connections. Explore a variety of activities both online and offline, and be less dependent on digital devices for entertainment.

DID YOU KNOW?

A 2023 study found that **72% of parents** are concerned about the privacy of their children's data collected by smart toys and educational AI applications.
(Source: https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/)