Privacy Pillar

Building a Privacy-Conscious Workplace Culture

Do and Don't for Mindful Use of Personal Data

A privacy-conscious workplace starts with everyday decisions made by employees. Your decisions play a key role in protecting personal data and building trust at work. This playbook outlines simple Do's and Don'ts to help employees handle personal data responsibly, respectfully, and securely at work.

DATA PRIVACY DAY

Think Before You Share

DO

Be mindful of the personal data you share, upload, or enter into workplace systems and digital tools.

HOW

Before entering any personal or sensitive information into internal systems, applications, or AI tools, pause and check whether the data is necessary for the task and authorised for use. Follow organisational policies, use only approved tools, and limit data sharing strictly to what is required for business purposes.

DON'T

Do not upload, share, or process personal data unnecessarily, casually, or on unapproved platforms, or disclose personal information out of convenience without checking whether it is required or permitted.

Respect People's Personal Data

DO

Treat personal data of colleagues, customers, and partners with respect and care.

HOW

Handle personal data as you would expect your own data to be handled access it only when required for work, keep it confidential, and follow organisational guidelines while using or storing it. Always double-check if sharing or processing of data is authorised and appropriate.

DON'T

Do not view, access, or use personal data out of curiosity, personal interest, or for reasons unrelated to your role or responsibilities. Always ensure no personal data is shared without authorization, or left exposed in documents, emails, or devices you use.

Use Digital & AI Tools Responsibly

DO

Use only approved systems and tools when working with personal data.

HOW

Follow internal IT and security guidelines while using software, AI tools, or digital platforms. Be cautious about what data you upload into tools, especially AI-based systems, and ensure privacy settings are reviewed where applicable. Always confirm that any tool or platform you use is authorised for the type of data you handle.

DON'T

Avoid uploading personal, confidential, or sensitive data into unapproved tools, public platforms, or external applications without proper authorisation. Do not share login credentials or bypass system controls, and never assume a platform is safe without confirmation.

Speak Up When Something Feels Wrong

DO

Report privacy concerns, mistakes, or suspected data incidents promptly.

HOW

If you notice incorrect data, accidental sharing, unauthorised access, or any activity that may impact privacy, inform the designated team (IT, HR, privacy, or compliance) immediately so that corrective actions can be taken. Provide all relevant details you have, and do not wait to confirm every fact involved, timely reporting helps prevent bigger issues.

DON'T

Do not ignore, hide, or delay reporting privacy-related issues out of fear, embarrassment, or uncertainty. Avoid trying to fix or investigate a suspected incident on your own without guidance, and make sure the issue is reported to the concerned team.

Keep Learning & Improving

DO

Stay informed and build awareness about privacy and data protection practices.

HOW

Participate in training sessions, read internal communications, and stay updated on organisational guidelines related to privacy, security, and responsible data use.

DON'T

Do not assume privacy is a one-time exercise, an optional task, or that it is someone else's responsibility. Ensure that the data handling practices are aligned with current privacy expectations.