

# EMPLOYEE PRIVACY AWARENESS GUIDE

Protecting Company and Personal Data in the Workplace

## KEY QUESTIONS TO ASK YOURSELF WHILE WORKING DIGITALLY

### WHERE?

am I sharing my company data

While working remotely or using digital tools, carefully assess where you're entering information.

You're not just an employee - you're a guardian of company and client data. Every login, click and file share either protects or puts your organization at risk.

**Scenario:** You receive an email with a link to what appears to be your company's HR portal asking you to update your banking details.

**Before proceeding, verify:**

- Is this the official company portal or an internal system?
- Is it a verified third-party vendor approved by IT?
- Or is it an unfamiliar or suspicious website?



**Action:**

Always verify requests through official channels. Contact your IT department or supervisor before sharing sensitive information on unfamiliar platforms.



### WHY?

While working remotely or using digital tools, carefully assess where you're entering information.

is it important to know the purpose behind data collection?



**Did you know?**

Under the Digital Personal Data Protection Act (DPDP) 2023, you have rights as a data principal - even when sharing work-related information.

**Ask yourself:**

- Is this for legitimate business purposes like payroll, benefits administration, or project collaboration?
- Is it for performance tracking, training, or system access?
- Does the request align with your role and responsibilities?



**Red Flag:**

Be cautious of vague requests that don't clearly state business necessity. Legitimate business tools should have clear data usage policies.

### WHAT?

kind of information is being requested

Evaluate whether the data request is appropriate for the business context.

You're asked to install a project management tool that requests access to:

- Your work email and calendar ✓
- Your personal contacts ✗
- Your camera and microphone without video conferencing features ✗
- Your location 24/7 ✗



Only provide information necessary for your job functions. Report suspicious requests to your IT security team immediately.

### HOW?

is my data privacy protected?

#### Your Rights Under DPDP Act 2023

##### Right to Information about Personal Data

You can request information about what personal data your employer processes, how it's used, and with whom it's shared.

##### Right to Grievance Redressal

You can file complaints about personal data processing with your organization's Data Protection Officer or Grievance Redressal Officer.

##### Right to Correction and Erasure

You can request corrections to your personal data maintained by your employer, including updating outdated information or correcting inaccuracies.

##### Right to Nominate

You can nominate someone to exercise your data rights if you become incapacitated or pass away.



**Action:** Be aware of your company's privacy notice and understand how your personal data is handled at work.

### WORKPLACE PRIVACY BEST PRACTICES CHECKLIST

- ✓ Read privacy policies for all business tools and applications you're asked to use
- ✓ Use only company-approved software and platforms for work-related tasks
- ✓ Enable multi-factor authentication on all work accounts
- ✓ Be suspicious of unsolicited emails or messages requesting credentials or sensitive data
- ✓ Verify unusual requests directly with the sender using known contact information
- ✓ Check URLs carefully before entering login credentials - ensure HTTPS and correct domain
- ✓ Report security incidents immediately to your IT security team
- ✓ Use secure connections (company VPN) when working remotely
- ✓ Limit permissions for work apps to only what's necessary for business functions
- ✓ Lock your devices when stepping away from your workstation
- ✓ Separate personal and work accounts and devices when possible



Remember: Protecting data at work protects both the company and your personal information. When in doubt, ask your IT security team!