![IT.ie]

# DATA PROTECTION

## Safeguarding Personal Information: A Guide for Employees

# INTRODUCTION

In today's digital world, safeguarding personal and company information is not just important, it's essential. Cyber threats are ever-increasing, and data breaches can have serious implications, both financially and reputationally. This guide is designed to provide employees with an understanding of how to protect personal and company information from such threats.

# SAFEGUARDING PERSONAL INFORMATION

## Understanding Personal Information

Personal information refers to any information relating to an identified or identifiable individual. This could include names, addresses, phone numbers, bank account numbers, email addresses, login credentials, PPS numbers, and other similar information.

## Importance of Safeguarding Personal Information

Safeguarding personal information is crucial to protect the individual's privacy, prevent identity theft, and ensure compliance with data protection regulations such as the GDPR. Furthermore, businesses also have a responsibility to protect customer and employee information from unauthorised access and data breaches.

# SAFEGUARDING YOUR PERSONAL INFORMATION

## Strong Passwords

Use complex passwords, combining upper and lower case letters, numbers, and special characters. Change your passwords regularly and avoid using the same password for multiple accounts

## Multi-Factor Authentication (MFA)

Where possible, enable 2FA. This adds an extra layer of security by requiring not only a password and username but also something that only the user has on them (like a mobile device).

## Phishing Awareness

Be aware of phishing attacks. Never click on suspicious links in emails, and never provide your personal information in response to an email request.

## Secure Networks

Use secure and trusted networks when accessing sensitive information. Avoid using public Wi-Fi for activities that require passwords or involve personal data.

# SAFEGUARDING COMPANY INFORMATION

**Data Minimization:** Only collect and process the data necessary for your job role.

**Data Storage and Transfer:** Store data securely using company-approved storage solutions. Only transfer data using secure and approved methods.

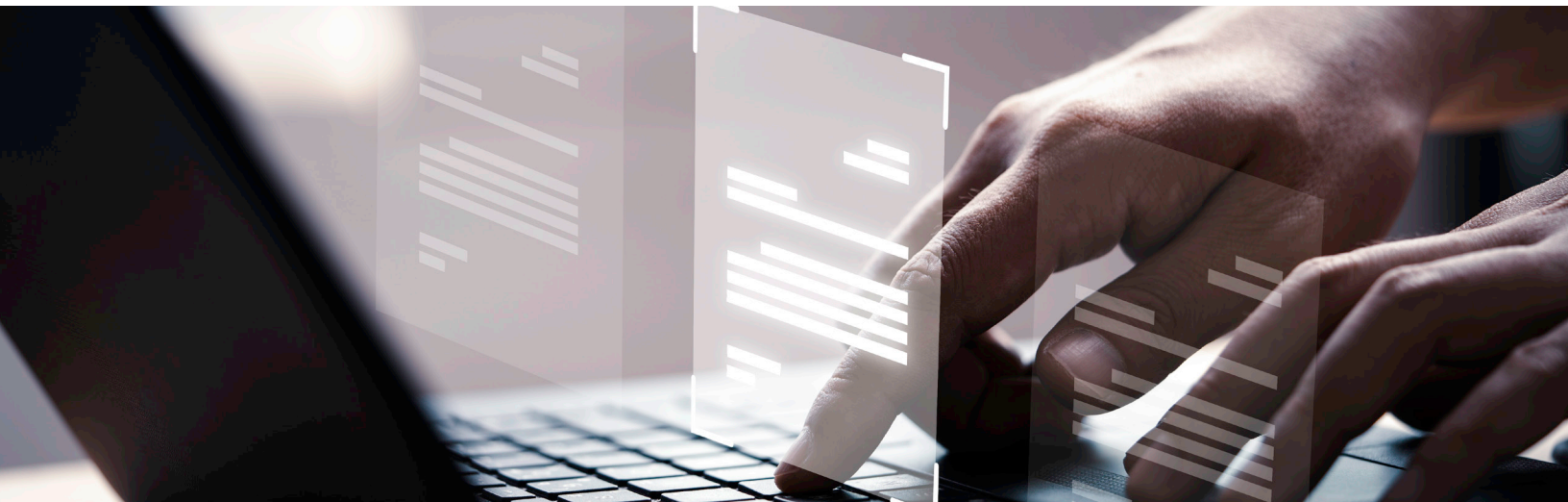**Data Sharing:** Only share data with those who need to know, and always ensure data is shared securely.

**Software Updates:** Regularly update software and devices. Updates often include patches for security vulnerabilities.

# A GUIDE FOR EMPLOYEES

## Reporting Incidents

If you suspect a data breach or a security incident, report it to your manager or your company's IT department immediately. Swift reporting can significantly mitigate the effects of a breach.

## Conclusion

Protecting personal and company data is everyone's responsibility. By adopting these practices and maintaining a proactive approach to security, you can significantly contribute to the safety and integrity of personal and company data.

**Remember: When in doubt about a data protection issue, always consult with your IT department or manager.**

**HELLO@IT.IE**

**1800 353 353**