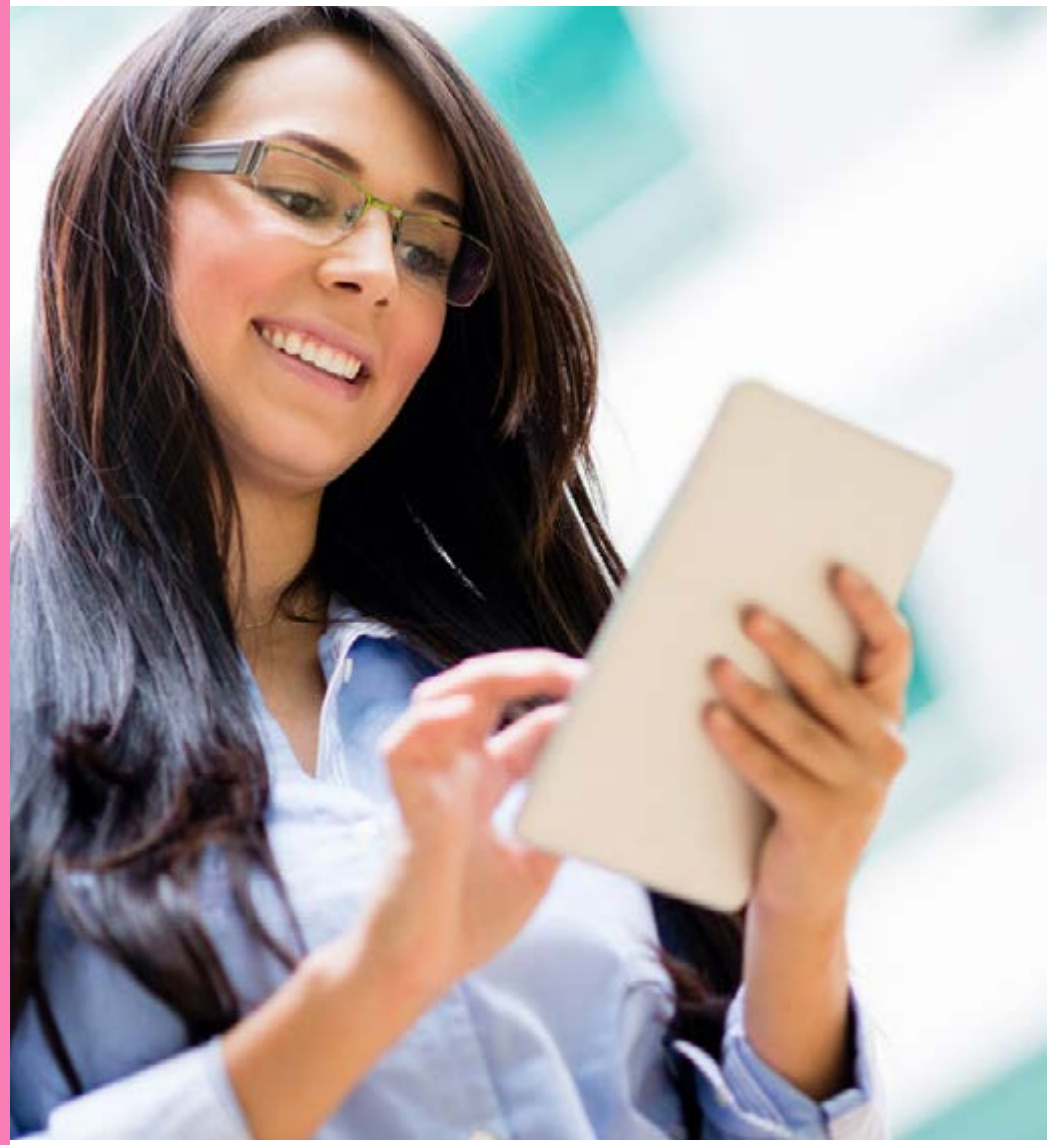
# Use of Information Technology (1 of 2)



This Code Policy explains how employees should use Unilever equipment and systems, or personal devices to access information at Unilever, responsibly and securely in compliance with all relevant laws and regulations

Employees are provided with access to Unilever systems and equipment to carry out their role.

Employees are permitted to use Unilever Equipment for personal use if this does not cause material impact to Unilever. Material impact includes excessive storage, network usage, mobile data usage, or voice utilisation which may have an impact on the performance of the environment.

All Unilever business information processed by or stored on Unilever or personal systems and equipment is not private and may be monitored, inspected or removed by Unilever, regardless of whether it is work-related or 'personal'.

Unilever may log, diagnose and assess activity on Unilever systems and equipment to the extent permitted by law, to ensure this policy is being followed and Unilever's technical environment is optimised.

# Use of Information Technology (2 of 2)

## Musts

When using Unilever's Systems and Equipment, employees **must**:

- Ensure Unilever equipment is used appropriately and protected from damage, loss or theft
- Use a password or PIN to lock unattended Unilever equipment, or any personal device used to access Unilever information
- Immediately report to the IT Service Desk the loss or theft of any Unilever equipment, or any personal device used to access or store Unilever Information
- Ensure any removable Unilever IT equipment is secured when left in the office overnight, is locked away or put out of sight when left unattended at home, in a hotel or in a vehicle. When travelling, keep it with you at all times
- Comply with copyright law and respect all applicable licenses for any graphics, documents, media and other materials stored on or accessed with Unilever systems or equipment
- Follow the appropriate IT request process to install any software or applications on their Unilever equipment

## Must nots

Employees **must not**:

- Try to disable, defeat or circumvent Unilever security controls, including but not limited to firewalls, browser configuration, privileged access, anti-virus and the deletion of system logs
- Use Unilever systems or Unilever equipment to intentionally access, store, send, post or publish material that is:
  - Pornographic, sexually explicit, indecent or obscene, or
  - Promotes violence, hatred, terrorism or intolerance, or
  - Is in breach of local, national or international laws
- Use Unilever systems or Unilever equipment to intentionally defame, slander or lower the reputation of any person or entity or their goods or services
- Expose Unilever information by:
  - Using non-public Unilever information for anything other than Unilever business
  - Forwarding emails containing non-public Unilever information to personal email accounts
  - storing or synchronising Unilever information from personal devices
  - Sharing their Unilever access credentials with anyone else, including work colleagues (unless formally approved by Information Security), friends and family
  - Using their Unilever password for non-Unilever IT Systems
  - Using their Unilever email address for non-business related websites or online activity
  - Intentionally accessing Unilever Systems or Unilever Information that is not intended for them
- Run or engage in any form of private business using Unilever IT equipment
- Access Unilever Systems or Information after leaving Unilever employment