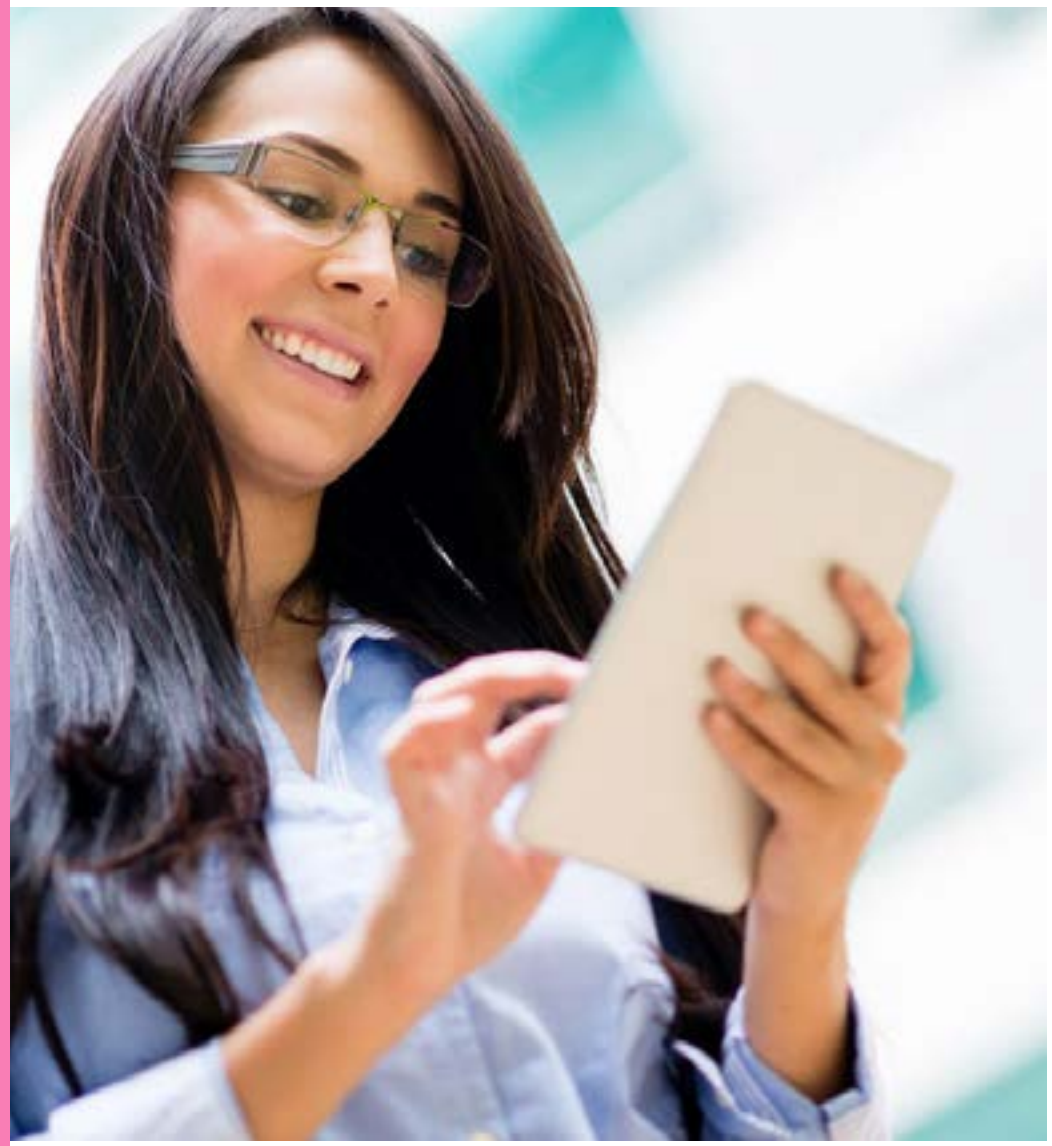
Use of Information Technology (1 of 2)



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, software, digital services, and equipment to carry out their role.

Employees are permitted to use Unilever Equipment for personal use if this does not expose Unilever to cyber risk or harm, or materially impact Unilever systems or operational resiliency. Material impact examples includes excessive storage, network usage, mobile data usage, storing non public data on personal storage or voice utilisation which may have an impact on the performance of the environment. Cyber risk is defined as an action that could expose Unilever systems or data or damage the Unilever brand.

To the extent permitted by law:

- All information processed by or stored on Unilever issued or owned systems and equipment (and Unilever information on personal devices) may be monitored, inspected or removed by Unilever without prior notification
- Unilever may log, diagnose, investigate, and assess activity and data on Unilever systems to ensure this policy is being followed and Unilever's technical environment is optimised and risk managed. Unilever reserves the right to remove any software that is non compliant / unapproved

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
- Lock any device, used to access Unilever Information, when unattended (e.g. password, PIN or biometrics)
- 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 process to install any software or applications on Unilever equipment and not install unapproved applications
- Only store Unilever data on approved storage platforms unless an exception has been sought and approved by Cyber Security

Must nots

Employees **must not**:

- Try to disable, defeat or circumvent Unilever security controls, including but not limited to browser configuration, antivirus, privileged access, firewalls and 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
- Run or engage in any form of private business using Unilever IT equipment
- Access Unilever Systems or Information after leaving Unilever employment
- Use removable media (USB storage) unless an exception has been sought and approved.
- Use a Unilever device for any activity that would be considered illegal by any operating countries Computer Misuse Acts
- Expose Unilever information by:
  - Using non-public Unilever information for anything other than Unilever business
  - Sharing or synchronising non-public Unilever information other than your own personal information (e.g. payslips), to personal accounts (e.g. email or storage) or devices not managed by Unilever
  - Sharing Unilever access credentials with anyone, including work colleagues (other than in defined circumstances pre- authorised by Cyber Security), friends and family
  - Using Unilever email addresses as an identity for non-business related activity
  - Using Unilever passwords anywhere else
  - Intentionally accessing Unilever Systems or Unilever Information that is not intended for their role