Hardware Lifecycle Policy

Joe & the Juice A/S

Version of 12 February 2026

Purpose

This policy sets out how Joe & the Juice manages the lifecycle, replacement, repair, and return of company-provided laptops, phones, and tablets. The purpose is to ensure secure, efficient, and fair handling of company hardware, while respecting employee rights.

1. Scope

The policy applies to all employees who are issued company hardware, regardless of location, employment type, or seniority, unless a written exception is approved by Corporate IT and HR.

2. General Principles

Company hardware is issued to support employees in performing their roles and remains company property at all times.

Employees are expected to take reasonable care of all company-issued devices. The company bears the normal operational risk for hardware wear, defects, and ordinary accidents. Employees may only be held financially liable for loss or damage to the extent permitted under Danish employment law, including where the employee has acted intentionally or negligently and where liability is proportionate.

All decisions on repair, replacement, or any potential cost recovery are made following a documented assessment by Corporate IT in dialogue with HR.

3. Laptops

3.1 Lifecycle

The standard lifecycle for company laptops is five (5) years. Employees become eligible for replacement at the end of the lifecycle if the device is still functional and no security or operational reasons require earlier replacement.

3.2 Hardware Standardization

As part of the company's platform standardization and to ensure optimal integration with the Microsoft-based ecosystem, including Microsoft 365, Teams, and security management tools, Windows-compatible laptops are the standard company hardware. Employees currently using MacBooks will transition to an approved Windows laptop at the end of their lifecycle or earlier if required for security or operational reasons. Exceptions may be granted where a MacBook is objectively necessary for the role or as a reasonable accommodation.

3.3 Loss or Theft

Employees must report loss or theft without undue delay to Corporate IT and their manager. The company will replace a lost or stolen laptop where justified. If repeated loss occurs, Corporate IT

and HR will review the circumstances, including whether the loss arose from negligence and whether any preventative measures are needed.

3.4 Damage and Repairs

Damage must be reported as soon as reasonably possible to Corporate IT. Corporate IT evaluates all damage and determines whether it results from normal wear and tear or defects, or from avoidable or negligent handling. Repairs or replacements are arranged by Corporate IT. Any consideration of employee liability follows section 2 and applicable Danish law.

3.5 IT Evaluation

Corporate IT assesses the cause and nature of the damage or loss, whether the device can be repaired securely, and the appropriate remedy, including repair, replacement, or retirement.

4. Phones

4.1 Lifecycle

The standard lifecycle for company phones is three (3) years. Employees become eligible for replacement after the lifecycle provided the device remains functional and secure. Earlier replacement can only take place with written approval from the Head of IT. The company may replace devices earlier where required due to security updates, incompatibility, performance issues materially affecting work, or manufacturer end-of-support.

4.2 Loss or Theft

Loss or theft must be reported immediately to Corporate IT and the manager. Corporate IT may require remote wipe or SIM-blocking where needed. Repeated loss triggers a joint IT and HR review, including whether negligence played a role and what preventative steps should be taken.

4.3 Damage and Repairs

First-time accidental damage is generally treated as part of normal operational risk. Corporate IT evaluates repeated or severe damage case-by-case and determines the remedy. Any potential employee liability is assessed under section 2 and Danish law.

5. Tablets (iPads)

5.1 Lifecycle

The standard lifecycle for company tablets (iPads) is four (4) years. Employees become eligible for replacement after the lifecycle if the device remains functional and secure.

5.2 Loss or Theft

Loss or theft must be reported immediately to Corporate IT and the manager. Corporate IT initiates relevant security measures, including tracking, remote lock, or remote wipe. Repeated

loss is reviewed jointly by Corporate IT and HR. The employee must send a copy of the police report for theft to Corporate IT and HR in case of theft.

5.3 Damage and Repairs

Corporate IT evaluates all damaged tablets to determine whether the damage is due to normal wear and tear or defects, or avoidable or negligent handling. The remedy is decided by Corporate IT. Any potential employee liability follows section 2 and Danish law.

6. Hardware Returns

6.1 Return Requirements

All company hardware must be returned to Corporate IT when the lifecycle ends and replacement is issued, when the employee changes role and no longer needs the device, or when employment ends regardless of reason. Devices must be returned together with relevant accessories.

6.2 End of Employment

Devices must be returned no later than the last working day unless otherwise agreed in writing. If an employee fails to return company devices, Corporate IT and HR will contact the employee to arrange return. Where devices are not returned after reasonable follow-up, the company may seek compensation to the extent permitted by Danish law and based on the fair market value of the device at the time of non-return, taking depreciation into account.

6.3 Wiping and Resetting

Corporate IT is solely responsible for data wiping and factory reset. Employees must not factory-reset or wipe devices themselves unless explicitly instructed by IT in writing. This ensures GDPR-compliant deletion and documentation.

6.4 Verification and Handover

Corporate IT verifies upon return that the device is received and logged, data wiping is completed securely, the hardware condition is recorded, and accessories are returned or noted missing.

7. Personal Use, Privacy, and Security

7.1 Permitted Use

Reasonable incidental personal use is allowed unless otherwise instructed. Employees must avoid storing sensitive personal data on company devices beyond what is necessary for incidental use.

7.2 Security Requirements

Employees must follow the Acceptable Use of IT Equipment Policy, must not disable security tools, encryption, or device management, must report suspicious activity or compromise immediately, and must use only approved software.

7.3 Monitoring and GDPR

Devices are managed through enterprise security and management tools. Any monitoring is limited to what is necessary for security, compliance, and operational purposes and is carried out in line with GDPR and applicable Danish privacy rules. Further information is provided in the company's IT and Privacy Notices published in the Employee Guide.

8. Exceptions

Exceptions to lifecycle rules, device standards, or return processes require prior written approval from Corporate IT and HR.

9. Policy Governance

Corporate IT owns this policy and may update it as needed. Material changes will be communicated to employees.

10. Acknowledgment

Employees issued hardware must acknowledge in writing that they have read and understood this policy.

Corporate IT Approval:

Signed by:
Antonio Cappiello
12B4A9F8235F4BE...

2/17/2026