

_____ **GROUP MOBILE TELEPHONY POLICY No. 18 dated July 27th 2015**

Author:

Name	Position / Role	Date	Signature
Stefano Stopponi	IT Operations Manager	22/04/2013	

Reviewer:

Name	Position / Role	Date	Signature
Davide Magnone	Organization & People Development and HR IT Manager	16/07/2015	

Approver:

Name	Position / Role	Date	Signature
Giovanni Daconto	Group IT Manager	22/07/2015	
Luca Mezzopera	Group HR&O Director	22/07/2015	
Leonardo Senni	C.E.O.	22/07/2015	

Table of contents

1.	Purposes and applications.....	3
2.	Risks and Sanctions	3
3.	Company Mobile Phone	4
4.	Company Smartphone	4
4.1	Assignment & withdrawal	4
4.2	Data traffic.....	5
4.3	Usage.....	5
4.4	Recap.....	6
4.5	Personal device with personal SIM card.....	7
5.	Use of Company content on personal devices	8

1. Purposes and applications

This policy aims to give all the Employees of the companies belonging to *Ariston Thermo Group* (hereunder the Company) guidelines and rules on the following subjects:

- Company mobile telephony devices/services assignment, use and management;
- Company Data access (e.g. emails, documents, systems) using personal devices (e.g. smartphones)

The rules listed in this document aim at preserving the security of the Company asset and information.

The Company considers each Employee trustworthy and fully responsible for ensuring the observance of the present guidelines and rules on behalf of:

- himself as individual/Employee;
- his staff as Manager coordinating other people.

The rules listed in this Policy are valid for all the employees of the companies controlled either directly or indirectly by Ariston Thermo S.p.A.

Any disregard of the present rules will expose the Company to a series of risks which could harm its business, its image, its tangible and intangible assets and could cause extremely extensive damage as well as sanctions of different kinds.

For anything related to the correct usage of the devices and services, please refer to the "Group IT Policy".

Compliance with the rules stated into this document must be ensured within the end of 2015.

2. Risks and Sanctions

The observance of the guidelines contained in this document is an essential part of the contractual obligations to which employees must comply with in the performance of their working activities.

Any disregard of the present guidelines and rules and/or any behavior openly in contradiction with them will represent violation of employment relationship obligations and disciplinary offence which will be subject to disciplinary procedure in accordance with the Employment contract and with the Labor Law (i.e. Collective Bargaining agreements, Company Agreements, etc.) of each Country where the company employing the transgressor has its registered office.

The disciplinary procedure will be defined according to the seriousness of the violation and to the risks to which the Company has been exposed. It will be fixed by the HR Business Partner together with the Group HR&O Director and the Country Manager or the Matrix Manager as for Corporate functions.

3. Company Mobile Phone

Mobile Phone is generally a basic device for placing/receiving voice calls and using SMS without any App or data traffic capabilities (internet connection). The data traffic has to be disabled by telephony contract.

The request to assign a mobile phone to an employee has always to be drawn up in writing in compliance with the Company local and/or Group procedures and has to be authorized by the Line Manager and the Country Manager or the Matrix Manager as for Corporate functions and has to be transmitted to the Local Mobile Telephony Responsible of the Area/Country.

The withdrawal of the Mobile Phone assigned to an end user usually happens in case of a company change or resignation which must be communicated to the Local Mobile Telephony Responsible of the Area/Country by the Local HR Manager.

In Case the Mobile Phone is assigned to the employee as a “**contract benefit**”:

- The Company shall pay for all voice calls/SMS

In case the Mobile Phone is assigned to the employee as a “**working tool**” only:

- The Company shall pay only for professional voice calls/SMS.
- The Employee shall pay for personal voice calls/SMS (if personal calls/SMS cannot be charged to employee, it is forbidden to place personal calls/SMS).

It is allowed to use Company Mobile Phone SIM card on personal devices.

In case the device is lost or stolen, the Local Mobile-Telephony Responsible must be informed as soon as possible in order to disable the SIM card. The theft must also be reported to the competent authorities within 24 hours. A copy of this report has to be given to local mobile telephony responsible.

4. Company Smartphone

Smartphone shall be a medium-range device for using Apps with an internet connection. Company smartphone model is decided by Corporate IT. Any variation must be agreed in advance with the Corporate IT.

4.1 Assignment & withdrawal

The request to assign a Smartphone to an employee with a band of reference (Ariston Thermo Group Banding System) from A to E has always to be drawn up in writing in compliance with the Group Policy by the *N.ORG.MD022Tt-“Smartphone Assignment Module”* and has to be transmitted

to the Local Mobile Telephony Responsible of the Area/Country and in copy to the HR Business Partner.

The request to assign a Smartphone to an employee with a band of reference from F to I has always to be drawn up in writing in compliance with the Group Policy and has to be authorized by the HR Business Partner, by the First Line Director and by the Group HR&O Director by the *N.ORG.MD022Tt-“Smartphone Assignment Module”* and has to be transmitted to the Local Mobile Telephony Responsible of the Area/Country.

The Local Mobile Telephony Responsible of the Area/Country has to archive the assignment module with the signatures requested.

The withdrawal of the Smartphone assigned to an end-user usually happens in case of a company change or resignation which must be communicated to the Local Mobile Telephony Responsible of the Area/Country by the Local HR Manager.

4.2 Data traffic

A data traffic limit has to be defined by contract for both national and roaming, when overpassed the data traffic has to be blocked.

National data traffic limit has to be set to 1GB/month for any Smartphone user.

National data traffic does not need any further approval.

Roaming data traffic limit has to be set to 500MB/month for employees with a band of reference from A to B and 200MB/month for employees with a band of reference from C to I.

Roaming data traffic for A-B bands does not need any approval.

Roaming data traffic for C-I bands has always to be drawn up in writing in compliance with the Company local and/or Group procedures and has to be authorized by the HR Business Partner, by the First Line Director and by the Group HR&O Director and has to be transmitted to the Local Mobile Telephony Responsible of the Area/Country. In case roaming data traffic is not granted, it has to be disabled by telephony contract.

4.3 Usage

In case the Smartphone is assigned to an employee as a “**contract benefit**”:

- The Company shall pay for all voice calls/SMS and data costs

In case the Smartphone is assigned to an employee as a “**working tool**” only:

- The Company shall pay only for professional voice calls/SMS and data traffic,
- The employee shall pay for personal voice calls/SMS (if personal calls/SMS cost cannot be charged to employee, it is forbidden to place personal calls/SMS).

Whether the smartphone is assigned as “contract benefit” or “working tool”, “BYOD Engagement Letter” (see chapter 6) has to be signed by the employee.

A personal User-ID can be used for official App Stores services from Google, Microsoft and Apple; other App installation channels are forbidden.

It is allowed to use Company Smartphone SIM card on personal devices.

The Company gives support only on Company Smartphones and only for the working Apps related to Company email, calendar and contacts.

It is mandatory to setup a device access password to be asked after device inactivity of 5 minutes.

In case the device is lost or stolen, the Local Mobile-Telephony Responsible must be informed as soon as possible in order to disable the SIM card, remotely remove all the device content and change the mailbox password for security reason. The theft must also be reported to the competent authorities within 24 hours. A copy of this report has to be given to Local Mobile-Telephony Responsible.

In case of employee resignation or in case of risky situations (e.g. virus), the company can remotely delete all the device content for security reason.

4.4 Recap

Smartphone BYOD letter to be signed		
Model	Banding	Authorization
Decided by Corporate IT; any variation to be agreed	A-E	none
Decided by Corporate IT; any variation to be agreed	F-I	HR Business Partner + First Line Director + Group HR&O Director

National data traffic		
Limit	Banding	Autorization
1GB/month; blocked when overpassed	A-I	none

Roaming data traffic		
Limit	Banding	Autorization
500MB/month; blocked when overpassed	A-B	none
200MB/month; blocked when overpassed	C-I	HR Business Partner + First Line Director + Group HR&O Director

4.5 Personal device with personal SIM card

In case the telephony service is granted to an employee as a “**contract benefit**”, the employee adopts his/her own device and contract subscription and the Company will provide a reimbursement against expenses actually incurred, up to a defined monthly cap¹ which is defined by the Local HR Manager according to the level and role of the Employee. Both traffic contract and device are directly owned and managed by the employee. Only one number per employee is allowed.

The Company allow the use of Company email system on personal devices with personal SIM card signing the BYOD letter (see chapter 5).

¹ The monthly cap cannot be higher than the actual costs incurred by the Company for the individual contract fees (traffic costs excluded)

5. Use of Company content on personal devices

In case the employee intends to use personal devices for storing/managing working documents (mainly emails on personal smartphones), he/she has to confirm that the device he will use:

















- is his exclusive property and/or availability;
- will not be used by third parties, or where third parties can use it, access to applications for office use will be subject to password only known by the employee;
- will always be set up with access password of at least 8 alphanumeric characters or the maximum allowed;
- will have the password changed every 90 calendar days;
- will always have barred access via password when idle for more than 5 minutes;
- Will not contain programs (or other material) not properly bought and/or licensed;
- will always be kept with the greatest care in order to preserve it from theft and / or loss.

In addition, the employee has to declare that he/she:

- will immediately delete any content referable to the Company as soon as it is no longer necessary;
- will promptly notify the Company (Local IT Support - Helpdesk) in case of loss and / or theft by providing, in the second case, the report released by the competent authorities;
- will respect, even compared to the personal equipment, any company policy that is compatible;
- will promptly change the password for accessing the equipment and/or office applications/documents in case a family member or a third party, they become aware of it.
- knows and agrees that in the event of loss or theft of the equipment or in the event of termination of employment, the Company can remotely erase all data on the equipment itself. The company can also perform remote wipe-out of all data even in presence of viruses in the device or other at-risk situations, having duly informed the employee in advance. For such a cancellation (in both cases) nothing can be requested by the employee to the Company on whatever basis;
- will not require (pretend) any corporate technical support.

The "BYOD Engagement Letter" N.ORG.MD018Tt-00 has always to be signed by the employee for having the permission of storing/managing working documents on personal devices.

Recap of Options and allowances

Option	Voice / SMS Professional	Voice / SMS Personal	Data (email)	Personal device	Company support	BYOD required
Smartphone as Benefit				allowed	only for company device	Yes
Smartphone as working tool				allowed	only for company device	Yes
Phone as benefit → Company device with direct payment			not available	allowed	only for company device	No
Phone as working tool			not available	allowed	only for company device	No
Personal device with personal SIM card as benefit → Personal device/contract reimbursed with cap				always	No	Yes
Personal device with personal SIM card				always	No	Yes



Paid by the Company



Paid by the Employee



Reimbursed to employee with cap