



Number:

Title:

Title (EN):

Type:

Scope:

Area:

Country:


Previous Number:

Document Information

Revision:

Status:

Effective Date:

		Standard Operating Procedure Grünenthal, Stokenchurch, HP14 3FE, United Kingdom		
document no.	replaces document no.	from	page	of
GB-IT-904-0007-02	GB-IT-904-0007-01	17-FEB-2017	1	10
valid from	01-FEB-2019	attachments	1	
Acceptable Use of E-mail, Internet and Social Media UK & Ireland				

SDN05-GL-QA-094-A009-V11

Regulatory area(s) ☐ GCP ☐ GLP ☐ GMP ☐ GVP ☐ GDP ☐ MedDev

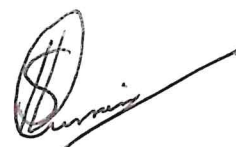
Other area(s) ☒ Information Technology

Language version ☒ Original ☐ Translation

Prepared by Shabbir Hussain
Senior Manager IT
GRT UK & Ireland

17-JAN-2019

Date



Signature

Reviewed by Thomas Spindler,
Finance Director,
GRT UK

17/01/19

Date



Signature

Reviewed by Emma McDermott,
HR Business Partner,
GRT UK & Ireland

18th JAN 19.

Date



Signature

Reviewed by John Fletcher,
Head of QRP,
GRT UK & Ireland

17 JAN 19

Date

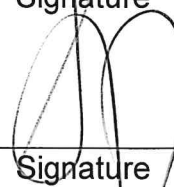
J. F. 19

Signature

Approved by Amanda Flanagan,
General Manager,
GRT UK

23/1/19

Date



Signature


Approved by Tom Coogan,
Country Manager,
GRT Ireland

Date

Signature

This document is the exclusive property of Grünenthal. It is to be treated as confidential and may not be reproduced either in its entirety or in part, nor may it be distributed to third persons without permission.

-/-

		Standard Operating Procedure Grünenthal, Stokenchurch, HP14 3FE, United Kingdom		
document no.	replaces document no.	from	page	of
GB-IT-904-0007-02	GB-IT-904-0007-01	17-FEB-2017	1	10
valid from		attachments	1	
Acceptable Use of E-mail, Internet and Social Media UK & Ireland				

SDN05-GL-QA-094-A009-V11

Regulatory area(s) ☐ GCP ☐ GLP ☐ GMP ☐ GVP ☐ GDP ☐ MedDev

Other area(s) ☒ Information Technology

Language version ☒ Original ☐ Translation

Prepared by Shabbir Hussain
Senior Manager IT
GRT UK & Ireland

Date

Signature

Reviewed by Thomas Spindler,
Finance Director,
GRT UK

Date

Signature

Reviewed by Emma McDermott,
HR Business Partner,
GRT UK & Ireland

Date

Signature

Reviewed by John Fletcher,
Head of QRP,
GRT UK & Ireland

Date

Signature

Approved by Amanda Flanagan,
General Manager,
GRT UK

Date

Signature

Approved by Tom Coogan,
Country Manager,
GRT Ireland

24.1.19

Date

Signature

This document is the exclusive property of Grünenthal. It is to be treated as confidential and may not be reproduced either in its entirety or in part, nor may it be distributed to third persons without permission.

-/-



	GB-IT-904-0007-02	page 2 of 10
---	-------------------	-----------------

Table of contents

1	Objective	3
2	Scope	3
3	Concerned roles	3
4	Terms	4
5	Process description	5
5.1	Company e-mail	5
5.2	Internet usage.	7
5.3	Social Media and Social Networks.	8
6	Cross references	9
6.1	References to standard procedural documents	9
6.2	Legal references	9
6.3	Other references (Available in GRT eRooms on the Group Intranet)	9
7	Attachments	10
8	Historical index	10

	GB-IT-904-0007-02	page 3 of 10
---	-------------------	-----------------

1 Objective

The objective of this document is to describe the acceptable and secure use of e-mail, Internet and Social Media professionally whilst conducting company business and privately during personal use.

2 Scope


This document applies to all Grünenthal UK & Ireland employees and to employees of external partners, agency workers or self-employed contractors.

3 Concerned roles

This section provides information about the concerned roles in the described process.


Concerned Role	Responsibility
Grünenthal employee	Usage of IT systems provided by Grünenthal appropriate to the rules defined in this guideline.
IT Help Desk	1st & 2nd Line Support for users of IT-Systems.
External Partner	Usage of IT systems provided by Grünenthal in correspondence to the rules outlined in this SOP and the agreement Terms on Execution of Remote Support. This agreement must be signed by all external partners prior to access to Grünenthal IT Systems.

See Section 5 for the responsibilities of concerned roles given above.

	GB-IT-904-0007-02	page 4 of 10
---	-------------------	-----------------

4 Terms

Term	Definition/Explanation
Grünenthal IT (GRT IT)	IT Department of Grünenthal companies (Global IT at Headquarters and local IT in subsidiaries).
User	Grünenthal employees as well as employees of external partners, consultants and contractors with access to IT systems provided by Grünenthal for work purposes.
Business critical data	Business critical data should be considered in the broadest sense to include research, intellectual property of Grünenthal, personally identifiable information, business and product development, clinical test and evaluation data, sales, marketing and business plans, customer and supplier information, supply chain, manufacturing, distribution, finance, human resources, consulting, partnerships, contracts and mergers and acquisitions. The criticality and the required protection level are derived from the result of its classification process.
Malware	Software that infiltrates and harms a computer system by bypassing the acceptance of the system owner (known as Viruses, Trojans and Worms).
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
McLaren	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Phishing	Criminal attempt to steal user data, credit card details and identity by means of fake e-mails and websites.
Man-in-the-middle attack	Attempt to redirect encrypted data traffic to a rogue/hackers server in order to break the encryption.
Social Media	Websites and applications that enable users to create and share content or to participate in social networking, e.g. Facebook, YouTube and Twitter.
Social Networking	The use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own.

	GB-IT-904-0007-02	page 5 of 10
---	-------------------	-----------------

5 Process description

All Grünenthal employees are responsible for using the IT systems provided to them in a secure and responsible manner. This includes the use of company e-mail, Internet usage and the use of Social Media.


A breach of the following rules violates the Grünenthal Code of Conduct and may result in disciplinary action and or legal proceedings (employment, civil or under criminal law).

5.1 Company e-mail

- It is forbidden to forward your Grünenthal work e-mail, either manually or by any automated means, to any private or external e-mail account. Doing so is deemed to be gross misconduct and anyone found to be in breach of this rule maybe liable for disciplinary action.
- E-mail with information which is meant exclusively for Grünenthal employees or of confidential nature must not be forwarded to any externals, third parties or private e-mail accounts. Doing so will be a breach and will also lead to disciplinary action.
- The Grünenthal work e-mail account must exclusively be used to conduct the company's business.
- Sending e-mails to everyone in the company or to a large collective e-mail group is the responsibility of the Leadership Team, HR, Compliance and the IT department which are authorised by the company to do so. Should a situation arise where an individual outside the functions mentioned above has to send an e-mail to the entire company, then they must seek the approval of a Leadership Team member before sending.
- Do not use the **Reply All** option to reply to a company-wide communication. Doing so sends your reply to the entire company unnecessarily and is considered bad e-mail etiquette. If you do need to send a reply e-mail, then you should only reply to the individual who has sent the original email. Do not copy in the entire company.
- Avoid sending or forwarding e-mails containing pointless or questionable contents.
- Delete e-mails from unknown senders requesting personal information or payment for any outstanding invoice. Especially if these emails contain a document which you are required to open. If you have any doubts and or the reliability of the sender cannot be guaranteed, then delete the e-mail. These could be SPAM or Phishing emails containing viruses or malware, such as Ransomware, which can infect your computer system and render your files unusable.

-/-

- Before sending an e-mail check that the e-mail does not contain any private individuals e-mail addresses, names of any colleagues who have left the company or any old e-mail distribution lists. Delete these e-mail addresses from your Outlook e-mail's cache memory (contact your local IT Helpdesk if you require any assistance with this).
- E-mail attachments should only be opened if the identity and reliability of the sender is known. Otherwise you can infect your computer with a virus.
- URLs (links to web pages) should not be clicked or accessed unless their reliability has been checked. The link in the e-mail may not necessarily take you to the destination it pretends to be leading you to (these are also known as Phishing mails).
- Receiving and sending of executable attachments (e.g. .exe files, even when they are included inside .zip archives) are blocked by the Grünenthal IT system.
- The maximum file size for e-mail attachments is 30 Megabytes (MB).
- Where possible always avoid e-mailing files as attachments internally. When sharing files and information, always save these under the folder appropriate for your department on the shared Network drives e.g.; (O drive, K drive or S drive etc.), or ask the person responsible for the local intranet to place these on the local Intranet.
- When sending e-mail to anyone outside the organisation, it is recommended to use the option BCC, (blind carbon copy), to include any Grünenthal colleagues, instead of CC (carbon copy). This option hides the colleagues' names and e-mail addresses from external recipients.
- E-mails containing business critical data may only be sent in encrypted form. Before sending business critical data, the user has to make sure that e-mail encryption is enabled for the external partner and a secrecy agreement is in place.
- Details regarding e-mail encryption and secure exchange of Grünenthal data with external partners can be found in the Global IT handout Secure Data Exchange.
- E-mails must be stored by the user in accordance with GL-IT-000-0007 Acceptable use of IT systems.
- The IT department is responsible for maintaining and updating company e-mail distribution lists.

	GB-IT-904-0007-02	page 7 of 10
---	-------------------	-----------------

5.2 Internet usage.

5.2.1 Basics rules for using the internet on company IT equipment.

The internet is considered a work tool. Any private usage is covered by the same regulations regarding security measures as business related use.

Any form of Internet use which harms the interests, the reputation of the company, cause offence to others or violates the law is forbidden and may result in disciplinary action.

In Particular:

- Content which violates privacy, personal rights, copy rights and laws is forbidden.
- Information, internet sites or web pages which are insulting, defaming, unconstitutional, racist or pornographic in content.


If for working purposes you require access to a web page which is blocked by the Web Filter security system, a request must be submitted to your local IT Help desk and thereafter the appropriateness to allow access to this site will be assessed. All requests will be reviewed separately.

5.2.2 Network and client security rules whilst using the internet.

Although an internet content filter and anti-virus software is in place, everyone must abide by the following rules concerning internet usage:

- Suspicious Internet pages (questionable web sites, doubtful contents, etc.) must be closed immediately.
- Business critical data may only be stored with qualified web application providers who have been approved by Grünenthal.
- You must pay attention to warnings issued by web browsers and report anything suspicious to your IT Department.
 - Special attention should be paid to certificate warnings as they could be caused by a man-in-the-middle attack.
- Downloading and executing of software from the internet is forbidden. Contact your local IT Help desk for further information.
- Documents or any technical documentation must be downloaded from official, trustworthy web sources (e.g. web site of manufacturer). Do not download documents provided by social networks or untrusted bulletin boards as there is a risk of malware infiltration.

-/-

	GB-IT-904-0007-02	page 8 of 10
---	-------------------	-----------------


- Only authorised Grünenthal employees are allowed to publish information on the internet, which has been through a formal approval process first.
- It is forbidden to establish a connection to the internet or a non-Grünenthal network which allows uncontrolled remote access to externals to IT systems on the Grünenthal network.
- Only solutions authorised by Grünenthal for remote connection, web conferencing and telephony must be used. Currently, Skype for Business is the Grünenthal preferred tool (See Attachment 1 Skype for Business).

5.3 Social Media and Social Networks.

Social media and social networks should only be used with respect to the guidance defined by the Grünenthal Code of Conduct. Employees are responsible for ensuring they are familiar with this guidance. Should they have any questions in relation to this they must speak to their Line Manager or Grünenthal IT. When using social networks, your actions and or behaviour must not harm or potentially harm the reputation of Grünenthal, its employees, customers, clients or bring the company into disrepute. Any content must be respectful, the content must not be offensive, sexual, racist, racial, homophobic, not connected with age, religion or related to a person's disability. It must not be abusive, harmful, offensive or discriminatory in any way or form. (See Page 6 GB-CM-908-0005 - Use of digital media in the conduct of business – UK & IE).

- Never post or share visuals, images, audio, logos or photographs taken at work related meetings, conferences with work colleagues or healthcare professionals.
- Posting or sharing images on social media or a social network could be deemed as inappropriate and could potentially lead to a claim of discrimination.
- Internal company information including but not limited to confidential information must not be shared on social media.
- See also Global Standard Operating Procedures GL-OR-067-0003 - Social Media Policy and GL-OR-067-0004 - Professional Use of Social Media which are available on McLaren.

-/-

	GB-IT-904-0007-02	page 9 of 10
---	-------------------	-----------------

If you come across any incident which is not outlined above or where you are unsure of which course of action to take. Please contact the Compliance department (UKCompliance@grunenthal.com)

Any matter or alleged matter in relation to misuse or misconduct of e-mail, internet and or social media will be managed in accordance to Grünenthal Disciplinary Policy.

6 Cross references

Not Applicable.

6.1 References to standard procedural documents

Grünenthal Code of Conduct (Available on the Group Intranet)

GL-IT-000-0007 - Acceptable use of IT systems (Available on McLaren)

GB-CM-908-0005 - Use of digital media in the conduct of business – UK & IE (Available on McLaren)

GL-OR-067-0003 - Social Media Policy (Available on McLaren)

GL-OR-067-0004 - Professional Use of Social Media (Available on McLaren)

6.2 Legal references


Not Applicable.

6.3 Other references (Available in GRT eRooms on the Group Intranet)

WINDOWS 10 GUIDE

SECURE DATA EXCHANGE

TERMS ON EXECUTION OF REMOTE SUPPORT

	GB-IT-904-0007-02	page 10 of 10
---	-------------------	------------------

7 Attachments

Attachment no.	Title	Number of pages
1	Skype for Business	4

8 Historical index

Version/ document no.	Description of changes	Valid from
GB-IT-904-0007-01	New Document (Local country version)	17-FEB-2017
GB-IT-904-0007-02	Updated change of Senior Management Group to Leadership Team, changes in shared drive J to O, Lync to Skype, SOP & Other references.	See page 1

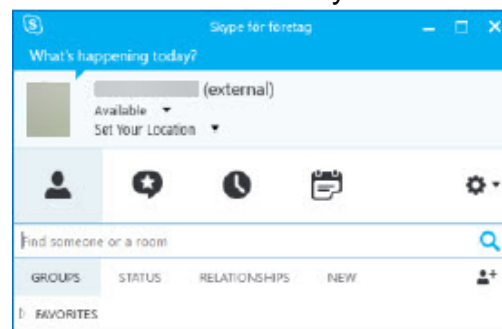
Start and Options

Skype is started from the Start menu and connects to the server automatically. Your presence information is displayed.









Latest information can be added daily under **(What's happening today?)**.

Your **presence status** is indicated by colour and text, settings can be changed in the **Tools, Options** found under the **Cogwheel** icon.

For further information you can also add your location information (**Set Your Location**).



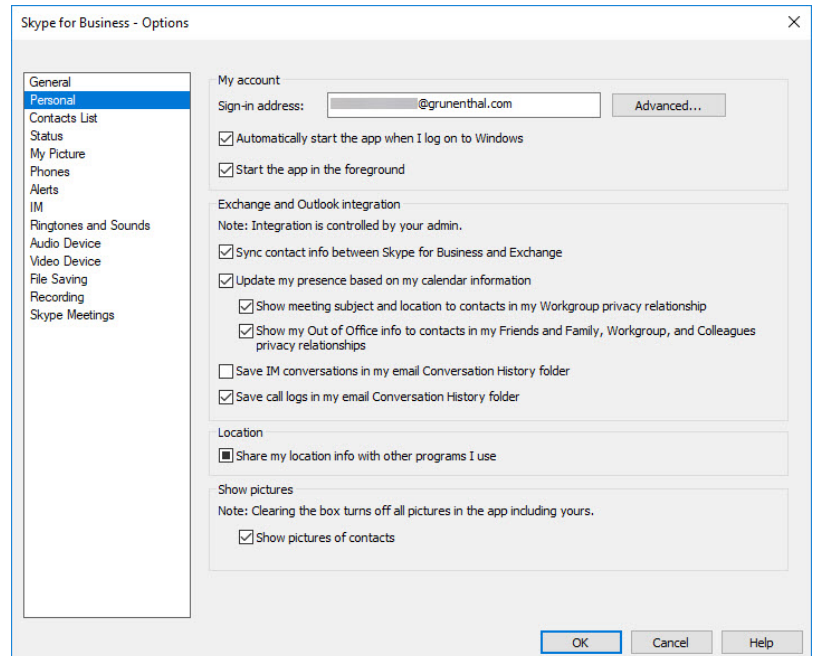
Options for Availability


	Available	You are online and people can contact you.
	Busy	You are in a Lync call or your Outlook calendar shows that a meeting is active and you don't want to be disturbed.
	Do not disturb	You don't want to be disturbed, Meeting notifications are only displayed, when they arrive from members of your workgroup.
	Be right back	You are not at your computer for a short time.
	Appear away	Your computer has been idle for some time (default 15 min.).
	Off Work	You are off work and cannot be contacted.
	Offline	You are not signed in. If your presence information is blocked for others, the status "Offline" is displayed to them.
	Unknown	No presence information is available.

Skype for Business - Options

The following settings can be set in the Options dialog (**Tools, Options**):

- Update of the presence information based on your Outlook calendar.
- Determination of the location where meeting and IM Conversations are saved.
- Activate/deactivate the sharing of your location to others.
- Activate/deactivate the display of photos of your contacts.
- Set the time periods for your Status **Be right back** and **Appear away**.
- Choice to hide or show the photo that is displayed (**My Picture**).
- Setting of the options which can be shown, when the status **Do not disturb** is set (**Alerts**).

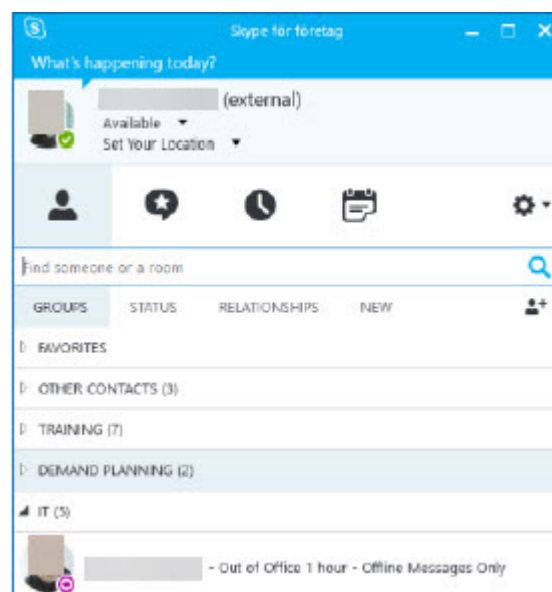
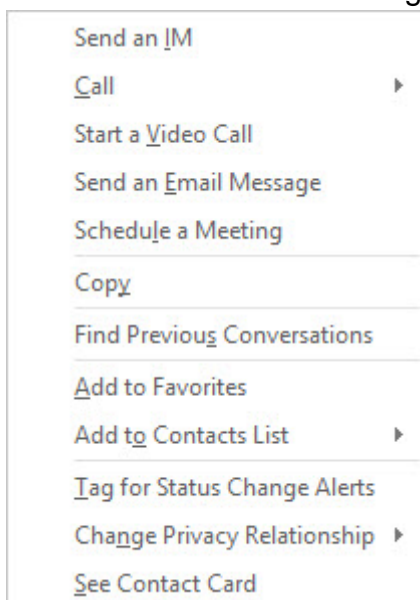


	<p>Attachment 1 of GB-IT-904-0007-02</p> <p>Skype for Business</p>	<p>page 3 of 4</p>
---	--	------------------------

Contact lists

You can gather people you contact regularly in a contact list.

- To search for contacts just enter the name or Email address in the search box (**Find someone or a room**).
- Right-click a person in the search results and select one of the following options:

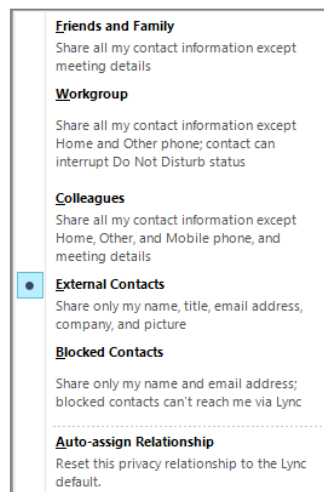


Existing Groups are additionally displayed in the menu.

Privacy Relationships

You can assign “Privacy Relationships” to each contact. The “Privacy Relationship” effects the information that is displayed to the members of the group.

- **Friends and Family** can see all information except meeting details.
- **Workgroup members** don't see private and other phone numbers, they can interrupt the status **Do not disturb**.
- **Colleagues** see all information except private and mobile phone numbers and meeting details.
- **External Contacts** only see name, company, title, email address and photo.
- **Blocked Contacts** see only name and email address and cannot communicate via Skype.

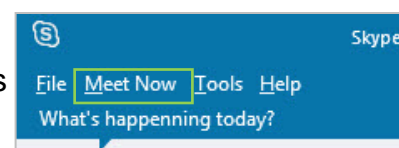


Instant Messaging (IM)

Instant Messages can be invoked by double-click on a contact, pointing at a contact or contact group (message is sent to all members of the group) or by Right Clicking the contact and selecting **Send an IM**.

Online Meeting

The option **Meet Now** in Skype allows you to immediately start an online meeting. You can choose to invite more participants into the meeting from the **Invite More People** option.



Participants receive a notification and can directly join the meeting.