



ISG – ACCEPTABLE USE POLICY

Applies across all legal entities within the ISG group

CONFIDENTIALITY

All information contained in this document is confidential to ISG and all Group companies. No copying or distribution is permitted without the consent of a Company Board Director.

DEFINITIONS

For the avoidance of doubt where necessary, clarification of the meaning of terminology used within this document is given below;

The Company – refers to the parent company and to all member companies of The Company. Equally, in context it refers to the specific company by which a user is employed.

User – any person within the scope of this document having been provided with Company equipment or having been granted access to Company Information Systems i.e. Company employees, all temporary staff, sub-contractors, contractors, freelancers and third parties.

IT Systems – any and all IT related equipment provided for users in the course of their work either during employment or during their association with the company, and;

Any and all IT related systems and services to which the same users are granted access to for the purpose of performing their duties



Contents

1	INTRODUCTION	5
1.1	OBJECTIVES	5
1.2	SCOPE.....	5
1.3	CONTACT DETAILS	5
1.4	RESPONSIBILITIES OF EVERYONE IN THE COMPANY	5
1.5	USE OF COMPANY COMPUTING AND COMMUNICATION FACILITIES.....	6
1.6	USE OF PERSONAL COMPUTING AND COMMUNICATION FACILITIES.....	6
1.7	HARDWARE PURCHASING	6
1.8	SOFTWARE PURCHASING AND USAGE	7
1.9	COMPLIANCE WITH RELEVANT LEGISLATION AND REGULATORY CONTROLS	7
1.10	USER ACCOUNT(S)	7
1.11	DEALING WITH CONFIDENTIAL OR COMMERCIALY SENSITIVE INFORMATION.....	8
1.12	PROTECTION OF PERSONAL DATA.....	9
1.12.1	Collecting Personal Data.....	9
1.12.2	Use of Personal Data	9
1.12.3	Loss of Personal Data.....	9
1.12.4	Retention and destruction of Personal Data	9
1.13	WORKING WITH GOVERNMENT OR CONFIDENTIAL CLIENTS	10
1.13.1	Government Clients.....	10
1.13.2	Confidential Clients.....	11
1.14	WORKING WITH COMPANY OWNED IT SYSTEMS	11
1.15	REMOTE / HOME WORKING	12
1.16	REPORTING SECURITY INCIDENTS	13
1.17	FILE SYNCHRONISATION SOFTWARE	13
2	INTERNET USE AND SECURITY	13
2.1	RESPONSIBILITIES FOR INTERNET USERS.....	13
2.2	UNACCEPTABLE ACTIVITIES	14



- 2.3 INADVERTENT ACCESS TO INAPPROPRIATE CONTENT 15
- 2.4 ACCESS TO WEBSITES 15
- 3 EMAIL USE AND SECURITY 15
 - 3.1 RESPONSIBILITIES OF EMAIL USERS..... 16
 - 3.2 USE AND COMPOSITION OF EMAIL 16
 - 3.2.1 Use of Personal Email Accounts for Company Business 17
 - 3.2.2 Personal Email..... 17
 - 3.3 EMAIL SECURITY 17
 - 3.3.1 Email retention..... 18
 - 3.3.2 Access to your email by other members of staff 18
 - 3.3.3 Out-of-Office Messages 18
 - 3.3.4 Auto-forwarding Email 19
 - 3.3.5 Company Issued Email Capable Devices 19
 - 3.3.6 Personal Email Capable Devices..... 19
- 4 COMPANY DEVICES, INCLUDING LAPTOPS, TELEPHONES & MOBILE DEVICES 19
 - 4.1 PERSONAL USE OF TELEPHONES 19
 - 4.2 USING YOUR COMPANY PHONE IN THE CAR..... 19
 - 4.3 DATA USAGE AND CONSUMPTION..... 20
 - 4.4 PERSONAL MOBILE TELEPHONES & TABLETS 20
 - ISG Asia, Commtech and Middle East use of personal mobile phones for business purposes 21
 - USE OF PERSONAL COMPUTING AND COMMUNICATION FACILITIES..... 21

1 INTRODUCTION

This Policy establishes the Acceptable Use & Data Security Policy within the Company for access to and use of all Company IT Systems.

This is a vital part of ensuring that we conduct our business lawfully (meeting regulatory, legal, and contractual requirements), deliver a quality service to our customers and protect the reputation of the Company.

1.1 OBJECTIVES

This Policy has a number of objectives, covering all aspects of information security. These include:

- Ensuring that all information held by the Company is protected appropriately, commensurate with its value and the associated risks
- Avoiding breaches of any criminal, civil and statutory law, including national data protection laws, regulatory or contractual obligations, including the Construction industry and Financial regulations
- Ensuring the business needs are met while adhering to standard policy stipulations and governance best practices
- Providing a framework for the implementation and administration of more specific and detailed Data Security standards and implementation guides
- Providing guidelines for your responsibilities when using the Internet and email facilities provided by the company

1.2 SCOPE

For the purposes of this Policy, Data Security includes information in any format, including that which is processed, stored or transmitted by IT systems (including, but not limited to, PCs, laptops, mobile devices and tablets), networks, telecommunications systems, paper or any other processing, storage or transmission mechanism or method.

This policy applies in addition to all existing obligations of confidentiality placed upon employees, all temporary staff, sub-contractors, contractors and third parties.

This policy is endorsed by the Company Board and complies with industry standards. The policy will be reviewed regularly and may be amended at any time to address further risks to the business and to reflect changes in technology or business practices and standards.

1.3 CONTACT DETAILS

For enquiries about this policy contact your IT Business Partner. Details of the IT Business Partners can be found within the Group IT section on Workspace.

1.4 RESPONSIBILITIES OF EVERYONE IN THE COMPANY

Acceptable Use and Data Security depends upon all 'Users' playing their part and fulfilling their responsibilities. This policy defines acceptable use of these facilities.

Compliance with these responsibilities and requirements is mandatory, and further action will be taken where there is a breach of this policy. In the case of employees, this may result in disciplinary action, including dismissal.

All Directors and Department Heads are responsible and accountable for this policy and guidelines and to ensure that this is regularly communicated to their teams.



1.5 USE OF COMPANY COMPUTING AND COMMUNICATION FACILITIES

These are provided primarily for business purposes. Personal use is permitted provided that it is appropriate and reasonable, complies with this policy and does not interfere with an individual's day to day duties.

ISG will protect personal data collected as a result of your employment. You should not have an expectation of privacy when using Company computing and communication facilities. The Company will, at its discretion and in line with current legislation, monitor and record usage to ensure compliance with legislation and internal policies. To guarantee the confidentiality, integrity and availability of ISG's networks, systems and data, we may monitor the length of time you use the facilities, the contact details of the individuals or services you contact and the content of any communication.

Company computing and communication facilities must not be used in any way that is derogatory, defamatory, offensive, illegal or could bring the Company into disrepute.

You are responsible for company equipment and communication facilities provided to you and must take all reasonable care to protect them. Laptops are not to be left in the office overnight unless they are secured to your desk by an approved method, i.e. Kensington Lock or they are locked in your pedestal or a secure locker when not in use.

The company reserves the right to seek financial recompense for any unreasonable loss or damage. Any lost or stolen company device must be reported to the IT Service Desk or your IT representative as soon as possible. Where a device contains personal data (data from which a living individual can be identified), this must be stated when reporting the loss. In some instances legislation requires ISG to report theft or losses to the authorities within 72 hours.

Items include but are not limited to:

- Mobile Phones
- Laptops
- Tablets
- Portable USB devices
- CDs / DVD

Printed documents containing personal data of ISG employees or individuals external to the company which are lost or stolen, must also be reported immediately to the IT Service Desk.

It is the Line Manager's responsibility to ensure that all IT equipment is returned to Group IT. All leavers must return all ISG issued equipment to their Line Manager or Group IT or in the event that neither of these are available, to their local Human Resources representative. All equipment must ultimately be returned to the Group IT department. Equipment must not be passed onto another ISG employee to use without prior approval by Group IT. The Company reserves the right to seek financial recompense for any equipment that is not returned.

1.6 USE OF PERSONAL COMPUTING AND COMMUNICATION FACILITIES

It is forbidden to connect any personal computing or communication device to the company network. Failure to comply with this may result in disciplinary action, which may include dismissal.

1.7 HARDWARE PURCHASING

All requirements for new IT hardware must be submitted via the IT Service Desk to the Asset and Vendor Management Team within Group IT. This includes all hardware for ISG offices and ISG project sites. This includes all hardware for ISG offices, ISG project sites and homeworkers

New hardware includes but is not limited to:

- Monitors
- Laptops
- Multifunctional devices (MFD's)
- Printers
- iPads
- Routers
- Wireless Access Points
- File Servers

1.8 SOFTWARE PURCHASING AND USAGE

All requirements for new software purchases and license renewals must be requested via the IT Service Desk to the Asset and Vendor Management Team within Group IT. It is not permitted to use or access software via any ISG owned device which has not been purchased and therefore approved by Group IT. This includes all platforms or applications which are accessed via the internet including Software as a Service.

1.9 COMPLIANCE WITH RELEVANT LEGISLATION AND REGULATORY CONTROLS

You must comply with all legislative and regulatory requirements that apply in your jurisdiction, and specifically in the UK where Company data rests. In particular:

- You must comply with **all privacy laws**. In the UK and Europe GDPR is applicable to all personal data (i.e. data from which a living individual can be identified) stored or processed by The Company. Outside of Europe, please consult your national data protection authority or seek advice from ISG's Data Protection Officer. See section 1.10 **Protection of Personal Data** for more information.
- You must comply with **Computer Misuse** laws and must never try to access systems or data unless you are entitled and need to do so.

In the UK, the Computer Misuse Act makes it an offence for a person knowingly to attempt to access data or systems without proper authorisation.

- You must comply with **Copyright and Intellectual Property Rights** (IPR) legislation.
- Only Group IT authorised and licensed software may be installed on your Company PC.

In the UK, the **Copyright, Designs and Patents Act** makes it an offence to copy licensed software without prior permission from the owner.

Government contracts will likely be subject to tighter regulations


1.10 USER ACCOUNT(S)

Users are assigned a unique User ID and password. This User ID and password is for sole use by the individual to which it is assigned.

Passwords should be a minimum length of 9 characters and include a combination of letters and numbers. They are to be changed on a 60 days basis. Previously used passwords must not be reused.

You will be held personally accountable for all activities performed with your user ID. To protect the integrity of your user accounts, ensure that you:



- Do not share your account or password details with anyone. This includes “logging someone on” to your account for them to use.
- Do not attempt to use the account of another user.
- Choose a password that is difficult for anyone else to guess.
- Change your password immediately if you think someone else knows it, when the system prompts for change, or at least every 60 days as a matter of course.
- Find an easy way to remember your password. Avoid writing it down.
- Lock your computer screen (*Ctrl-Alt-Del + Lock Computer* or  +L) or log off when you leave your desk. Always shut down your system completely at the end of the day.
- Only access systems for which you have an account and approved access.

1.11 DEALING WITH CONFIDENTIAL OR COMMERCIALY SENSITIVE INFORMATION

Confidential information is information that could damage the Company materially or cause reputational damage if disclosed.

Commercially sensitive information is information that if disclosed could prejudice our commercial or regulatory interests.

For the purpose of this policy Confidential and Commercially Sensitive information will be known as sensitive information.

Do not give out sensitive information unless you are sure you know who you are communicating with and that the recipient is entitled to the information.

You must protect hard copy documents containing sensitive information by:

- Only printing a copy of sensitive information if it is necessary. Collect it from the printer immediately.
- Disposing of sensitive documents using a confidential waste disposal process.
- Adopt a “clear desk” policy and do not leave documents lying around if you are away from your desk. Put important and confidential documents in secure cupboards or other secure storage when not in use, and especially overnight.

At all times, you must protect electronic copies of sensitive information:

- Do not download information to removable media (USB devices, CD/DVD-ROM, external hard drive, etc.) for transmission out of premises without permission from your line manager. Any removable media (USB devices, CD/DVD-ROM, external hard drive, etc.) must be encrypted.
- Only upload sensitive information to online storage services managed by Group IT, i.e. ShareFile, OneDrive and SharePoint. Examples of online storage services not managed by Group IT are WeTransfer and DropBox. If you are unsure, please contact the IT Service Desk for advice.
- Do not leave sensitive messages on answering machines or voicemail.
- Ensure that the appropriate level of permissions have been applied to any sensitive information being published on Intranets (e.g. Workspace) or stored on a file server.
- All information media (including CD-ROMs, USB devices, old IT equipment) must be disposed of by the IT department using the proper disposal facilities.

In all cases, you must not remove sensitive information or equipment from the office without permission from your Line Manager

1.12 PROTECTION OF PERSONAL DATA

As of the 25th May 2018, the law effecting how ISG uses personal data changed in Europe. A full list of what is meant by personal data or Personally Identifiable Information (PII) can be found within the Data Protection page on workspace on the GDPR FAQ document. For other jurisdictions, please consult with the Data Protection Officer. Personal data is data that can identify a living individual (such as national identity numbers, home address, mobile phone number) and for the purpose of this policy this includes personal data for current and former employees, individuals external to the company and members of the public. When collecting or using personal data, it is important that you ensure you are doing so lawfully and securely. The person whose data you are collecting and using is referred to below as the "Data Subject". You are expected to use reasonable judgement when collecting and using personal data and ensure that you are not using the data in a way that the data subject may not expect.

1.12.1 Collecting Personal Data

At collection you must ensure that the data subject is fully informed about how the personal data will be used and shared. This information must be provided to the data subject within a privacy notice. The privacy notice will also include how long ISG will keep their personal data. The Data Protection Officer (DPO) / Data Protection Team will assist with the privacy notice if one is not currently in place.

1.12.2 Use of Personal Data

When using personal data, you must make sure that you are only using it for the purposes that the data was collected for. Make sure you do not use it for any purposes not stated at collection and that you do not share the data with parties outside of ISG unless this was made clear to the data subject at the time of collection.

Personal data can only be copied to removable media with the explicit permission of both HR and the DPO / Data Protection Team. In the event that approval is given by these two parties, the removable media must be encrypted. No exceptions are permitted under this policy in respect of the transfer and encryption of personal information.

In all cases, you must not remove personal data from the office without permission from HR and DPO/Team.

Do not give out personal data unless you are sure you know who you are communicating with and that the recipient is entitled to the information.

You must protect hard copy documents containing personal data by:

- Only printing a copy of personal information if it is necessary. Collect it from the printer immediately.
- Disposing of documents containing personal information using a confidential waste disposal process.
- Adopt a "clear desk" policy and do not leave documents lying around if you are away from your desk. Put documents containing personal data in secure cupboards or other secure storage when not in use, and especially overnight.

1.12.3 Loss of Personal Data

Any loss of personal data must be reported to the IT Service Desk immediately.

1.12.4 Retention and destruction of Personal Data

You must make sure that personal data is not kept for longer than the data subject was made aware of at the time of collection. Once the retention period has lapsed and the data is no longer required, please ensure it is securely destroyed or disposed of. ISG's Data Retention Schedule can be found here https://isgplc.sharepoint.com/human-resources/Pages/your-employment/12_policies.aspx

For advice on destroying or disposing data please contact the IT Service Desk or your IT Business Partner.

1.13 Data Storage and external file sharing

1.13.1 ISG File Shares and Microsoft SharePoint online

ISG's own file shares (shared folders) must only be used to store sensitive data along with online storage services managed by Group IT, i.e. OneDrive and SharePoint

1.13.2 Microsoft Teams

Microsoft Teams must not be used to store sensitive personal data due to the external sharing risks associated with Teams

1.14 User Access reviews

Application, platform and external 3rd party system owners must review user access on a regular basis and remove or adjust access in a timely manner

Shared File owners, SharePoint site owners and Teams group owners must review user access on a regular basis and remove or adjust access in a timely manner

User Access review frequency is dependent on the nature of data being stored:

- Sensitive and Personal data user access must be reviewed every 6 months at a minimum
- Other user access must be reviewed every 12 months

1.15 WORKING WITH GOVERNMENT OR CONFIDENTIAL CLIENTS

1.15.1 Government Clients

When working on Government contracts a framework computer security policy will be issued by the client and this is to be adhered to at all times (*in addition to any other ISG or non ISG policies*). If you believe these policies contradict as a general rule, the highest security standard takes precedence and is to be enforced. If in doubt, contact the IT Security Officer for further advice.

Generally, the following standards will be required for all government contracts:

- Government approved 2 factor authentication disk encryption will be used on all laptops
- Removable devices such as USB memory devices, CD & DVDs will need to be encrypted when being used to transmit government data.
- Any lost laptop or portable device must be reported to the Government Framework Coordinator and IT, items include but are not limited to:
 - Mobile Phones
 - Laptops
 - Tablets
 - Portable USB devices
 - CDs / DVDs

It is the Line Manager's responsibility to ensure that all IT equipment is returned to Group IT. All leavers must return all ISG issued equipment to their Line Manager or Group IT or in the event that neither of these are available, to their local Human Resources representative. All equipment must ultimately be returned to the Group IT department. Equipment must not be passed onto another ISG employee to use without prior approval by Group IT. The Company reserves the right to seek financial recompense for any equipment that is not returned.

- The IT department are not to reissue any device that has been used to process government data unless it has been data cleansed using an approved data scrubber.

- Government data is not to be stored in the cloud without the express permission of the client.

If a device containing personal data of ISG employees is lost or stolen, this must be reported immediately to the IT Service Desk.

1.15.2 Confidential Clients

When working on contracts of a confidential nature a framework computer security policy will be issued by the client and this is to be adhered to at all times (*in addition to any other ISG or non ISG policies*).

Generally, the following standards will be required for all commercially confidential contracts:

- Single factor authentication disk encryption will be used on all laptops
- Removable devices such as USB memory devices, CD & DVDs will need to be encrypted when being used to transit commercially confidential data.
- USB ports are to be disabled on Laptop and desktop computers.
- Any lost laptop or portable device must be reported to IT, items include but are not limited to:
 - Mobile Phones
 - Laptops
 - Tablets
 - Portable USB devices
 - CDs / DVDs
- It is the Line Manager's responsibility to ensure that all IT equipment is returned to Group IT. All leavers must return all ISG issued equipment to their Line Manager or Group IT or in the event that neither of these are available, to their local Human Resources representative. All equipment must ultimately be returned to the Group IT department. Equipment must not be passed onto another ISG employee to use without prior approval by Group IT. The Company reserves the right to seek financial recompense for any equipment that is not returned.
- The IT department or Line Manager are not to reissue any device that has been used to process commercially confidential data unless it has been data cleansed to an appropriate standard by Group IT.
- Where a client has specified that their data is under a NDA clause, refer to the key ISG account manager before storing their data in the cloud, as you may need to seek permission from the client.

1.16 WORKING WITH COMPANY OWNED IT SYSTEMS

Company IT Equipment has been configured to provide consistent operation and support functions. Do not seek to modify configuration or settings.

In particular:

- Do not install software or alter the system or configuration files on your computer. Never try to modify system or configuration files on your computer (or anyone else's) without explicit instructions to do so from IT.
- Do not leave portable computer equipment (for example laptops, iPads) and/or mobile telephones unattended in a public or publicly accessible place. Always lock your laptop in a secure cupboard overnight if you do not take it away with you. Do not leave your laptop in a visible or unsecured place.
- Do not keep business information on your local hard disk (e.g. the C: drive or My Documents) as it will not be backed up. Important information needs to be stored on an IT approved system that is regularly backed-up. If you are unsure if it is an IT approved system, please contact the IT Service Desk.

- Do not access sensitive information when casual observers who are not authorised to have access to the information can see your computer screen. Take particular care in this regard if using a laptop in a public place. This same principle applies to reading hard copy documents containing sensitive information in a public place. You can seek approval for a screen protector from your Line Manager if necessary and request one using the self-service portal on the Intranet.
- IT systems are perhaps most at risk from the very users to whom they are assigned. It is expressly forbidden for users to impair performance, prevent from operating correctly or otherwise compromise IT systems security;

Users shall not;

- attempt to disassemble, modify, deliberately damage or misuse IT equipment nor use it for anything other than the intended use;
- reconfigure IT equipment in any way, for any purpose;
- connect peripheral equipment not supplied by the company, unless there is a genuine need and the IT department are able to inspect the device / peripheral first;
- attempt to penetrate computer network security, including unauthorised access or attempted access to another person's computer, including access to e-mail;
- introduce packet-sniffing software (i.e. software which is used to intercept data on the network) or password detecting software;
- download or install software or applications from the Internet (other than previously installed product updates. (If in doubt consult the IT Department));
- install software or applications from any source. All software acquisition and installation must be sanctioned by the IT Department;
- seek to gain access to restricted areas of the company's network;
- knowingly seek to access, download, copy, print or remove any work in which the company has intellectual property rights or is subject to GDPR and financial regulations. Such intellectual property rights shall include but are not limited to all trademarks, design rights, copyright, database rights, patents and any other registered or unregistered intellectual property rights owned by the company;
- knowingly introduce any form of computer virus, spyware or malicious code;
- engage in any form of hacking activities;
- use illegal file sharing applications;

1.17 REMOTE / HOME WORKING

This applies to individuals who work remotely (which applies to an individual's home or any other location that is not a Company Office or Site). If remote working is a routine part of your role, you must work on a Company supplied and supported computer and use an ISG approved Secure VPN access client. *(If you do not have this installed, please contact IT)*

Do not share or send ISG information to your home personal device

Ensure that sensitive and personal data is disposed of properly. Do not use your household waste disposal – dispose of all documents or equipment using the company waste disposal facilities provided.

All users must return information and equipment on request, or upon termination of employment.

1.18 REPORTING SECURITY INCIDENTS

All Information Security incidents must be reported to the IT Service Desk and your Line Manager.

If you identify or suspect a data security weakness or incident, do not attempt to investigate it. Report it immediately to IT.

Report the loss or theft of information or equipment (for example laptops, iPads, mobile phones) to the IT Service desk, or confidential documents to your Line Manager. In the event that equipment has been stolen, report the theft to the police and provide the crime reference number to IT.

If you think your Company supported computer is infected with a virus or malicious code, do not try to deal with it yourself, remove it from the network and contact the IT Service desk immediately.

If you suspect a software malfunction, report it to the IT Service desk by email immediately, taking note of the symptoms or error messages.

1.19 FILE SYNCHRONISATION SOFTWARE

Many users are linking file synchronisation tools to their PC's and mobile devices to allow "documents on demand" and synchronisation of personal files and folders.

This software, although very useful and efficient, stores the company data in networks that are not controlled by the Company. The Company cannot control the security of these files.

Some examples of 3rd. party File Synchronisation apps are;

- Dropbox
- Box
- Mediafire
- iCloud
- personal OneDrive (not to be confused with ISG's corporate OneDrive solution)

If you have a genuine business requirement for a third-party application that will be stored in the "Non ISG Cloud", then you must make a business case to IT via your IT Business Partner. It will be reviewed and will depend on the sensitivity of the data being stored.

You as the user have a duty of care to ensure due diligence when storing and working on sensitive information pertaining to the company.

2 INTERNET USE AND SECURITY

The Internet is an unregulated network and does not have the same degree of authentication, protection and control as The Company systems and networks. Access to and use of the Internet carries associated risks. Everyone in The Company who uses the Internet must act appropriately to comply with this policy and with legal requirements. This section outlines the requirements that are placed upon you as a user of the Internet at work and defines acceptable use of these facilities

2.1 RESPONSIBILITIES FOR INTERNET USERS

Company Internet facilities are provided for business purposes. Personal use is permitted provided that it is appropriate and reasonable, complies with this policy, and does not interfere with an individual's day to day duties. ISG logs all internet use for IT operational purposes and to detect, mitigate and investigate cyber threats and inappropriate activity. Your Line Manager can provide guidance about the level of personal use that is acceptable. The following should also be considered:

- You are responsible for considering your use, including personal use, of the Internet and for complying with this policy. If there is any uncertainty regarding personal use, guidance should be sought from your Line Manager.
- You are responsible for ensuring that your use of the Internet facilities does not bring the Company or our clients into disrepute.
- Internet facilities must not be used for any unlawful purpose whether in the UK or any of the countries in which the Company operates.
- You will be held personally accountable for your actions, or the actions undertaken using your account, when using these facilities, regardless of your physical location.
- By using the Company Internet facilities, you agree to the terms of this policy. For employees of the Company, these terms are deemed to form part of your terms and conditions of employment.
- You must report any unexpected security alerts to the IT Service desk (e.g. unusual screen messages referring to security).
- You should not have an expectation of privacy when using Company Internet facilities. The Company will, at its discretion and in line with current legislation, monitor and record usage to ensure compliance with legislation and internal policies, including this policy. This includes monitoring the length of time you access the Internet; the number of times you access the Internet and the content of the sites you access.

2.2 UNACCEPTABLE ACTIVITIES

The following are examples of unacceptable use and may result in further action being taken against you and in the case of Employees, disciplinary action, which may include dismissal.

You must not:

- Download, duplicate, transmit or publish any data or image that violates copyright, data protection laws or licensing agreements;
- Download software or executable files to Company resources. If you require a software package for specific business purposes, you must request this from the IT Service Desk.
- Transmit sensitive or personal information via the Internet. If you have a requirement to transmit sensitive or personal data consult the IT Service Desk or your IT Business Partner
- Browse, download, duplicate or transmit to Company resources, or to other resources and/or organisations connected to the Internet, any data which falls within any of the following categories:
 - For the purposes of crime or fraud
 - Sexually explicit
 - Harassing, offensive or abusive
 - Racist, disability or sexist
 - Terrorist or criminal associated data
- Attempt to defeat, circumvent or in any way reduce the effectiveness of ISG IT Security systems.
- Download software or data to computers for the purpose of unauthorised access to data or files.
- Attempt to gain unauthorised access to computers, networks or information.
- Use Company resources for gambling or other forms of gaming.
- Publish or approve the publication of sensitive or personal data (yours and others) on the Internet, unless you are approved to do so.
- Use the Internet in any way that reduces the availability of the service to other employees.



- Use the Internet for personal commercial purposes, such as selling goods online or running a personal business.

The above list of prohibitions is illustrative and not exhaustive. If you have a query as to whether a particular activity is / is not permissible, you should go to your IT Business Partner.

2.3 INADVERTENT ACCESS TO INAPPROPRIATE CONTENT

If you inadvertently access or receive inappropriate content or material, you should close all your browser windows and notify your Line Manager, IT and HR. Inadvertent access of inappropriate content may still be recorded by automated monitoring tools and may result in further investigation.

2.4 ACCESS TO WEBSITES

Access to certain websites is restricted by the use of content filtering. This is done to protect Company resources, and reputation.

You are responsible for ensuring that your use of the Internet does not breach the Acceptable Use Policy. The ability to access a website should not be interpreted as endorsement of that site by The Company, or that it is acceptable use as defined by this policy. If you believe that you have a legitimate business reason to access a site that is restricted by the content management software, you should contact the IT Service Desk.

Accessing certain sites is not regarded as acceptable use. Below are some of the main classifications, although this list is not exhaustive:

- Adult Material
- Advocacy Groups
- Drugs
- Gambling
- URL Translation Sites
- Hacking
- Illegal Activities
- Internet Auctions
- Message Boards & Clubs
- Violence
- Militancy & Extremism
- Personals and Dating
- Proxy Avoidance
- Racism and Hate
- Weapons

The Company reserves the right to monitor employees' internet usage- The Company considers the following to be valid reasons for checking an employee's internet usage:

- If the Company suspects that the employee has been viewing offensive or illegal material, such as material containing racist terminology or nudity.
- If the Company suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.

3 EMAIL USE AND SECURITY

Email is a pervasive business tool. It is not, however, a secure communication channel. Internet email suffers from the following security weaknesses:

Confidentiality

Emails can be easily intercepted. Do not send sensitive or personal data over the internet without seeking advice and without applying additional protection. For further advice please contact the IT Service Desk.

Integrity

There is no proof that the sender or the contents of the message are genuine

Availability

There are no guaranteed delivery times. Email sent over the Internet may never arrive, and neither the sender nor the recipient would be notified

3.1 RESPONSIBILITIES OF EMAIL USERS

When using Company email services:

- You are responsible for ensuring that you do not bring the Company or our clients into disrepute
- Do not use them unlawfully
- You will be held personally accountable for your actions, regardless of your physical location
- You accept the terms of this policy.
- The Company will, at its discretion and in line with current legislation, monitor and record the content of email use to endeavour to prevent security breaches, to monitor compliances with legislation and internal policies.
- Do not send emails from other user's accounts, except where permission has been provided by Group IT after consultation with HR.
- Do not impersonate other people.

The Company reserves the right to monitor emails to ensure compliance with legislation and internal policies. The Company considers the following to be valid reasons for checking an employee's email:

- If the employee is absent or has left the employment for any reason and communications must be checked for the smooth running of the business to continue. Where no proper handover or automatic message (or similar solution) had been able to be put in place before the employee's absence. In such case, the Company will limit the monitoring only for the time necessary to ensure such handover is implemented.
- If the Company suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the Company understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the Company suspects that an employee has been using the email system to send and receive an excessive number of personal communications.
- If the Company suspects that the employee is sending or receiving emails that are detrimental to the Company.
- If the Company suspects that the employee has committed a disciplinary incident which the Company is required to investigate.

When monitoring emails, the Company will, save in exceptional circumstances, confine itself to looking at the address and subject heading of the emails. Employees should mark any personal emails as such and encourage those who send them to do the same. Where possible, the Company will avoid opening emails clearly marked as private or personal.

The Company will make sure that the necessity to access the contents of your emails has been evaluated on case by case basis, any such access is proportionate and limited for specific purposes and your information is securely disclosed to a restricted number of staff

3.2 USE AND COMPOSITION OF EMAIL

Email should always be written in a careful manner and with consideration for the intended recipient(s).

- Care and consideration needs to be given to the content to ensure that you are not committing the Company to a legally enforceable agreement without having the authority to do so.
- Email messages may need to be authorised in the same way as other written communications.

The company will not tolerate bullying by any means on any company accessed systems, including but not limited to email, Skype and Yammer. Please refer to the Company's 'Dignity at Work' policy on Workspace. The use of obscene language or swear words is prohibited.

- Do not send sensitive or personal information to external recipients without encrypting the content first.
- Do not rely on the authenticity of an email message.
- Do not send or forward an email message which falls into any of the categories below:
 - Fraudulent
 - Phishing (that is, seeking to have the recipient disclose their authentication credentials or financial details to you)
 - Harassing, offensive or abusive
 - Racist or sexist or any other form of discrimination
 - Terrorist or criminal associated data
 - Sexually explicit
 - For the purposes of gambling or other forms of gaming for personal reward. This does not include internally organised charity draws and sweeps
 - Contains a political or religious opinion or position
- Emails can be used as legal evidence. A copy of all emails, including deleted items, is retained. However, accessing and retrieving such items can be complex and costly and should not be relied upon except where there is a valid business requirement, such as for a legal inquiry.

3.2.1 Use of Personal Email Accounts for Company Business

It is prohibited to use personal email accounts for the transaction and storage of company business, both externally with clients or with colleagues. All email related to company activity must be transacted from a company email account.

It is prohibited to forward work data from your ISG email account to a personal email account. If your corporate email account is not working, contact the IT Service Desk immediately.

3.2.2 Personal Email

Company email facilities are provided for business purposes. You are responsible for considering your use, including personal use, of email and for complying with this policy. If there is any uncertainty regarding personal use, guidance should be sought from your line Manager.

- Personal email sent from your company email account, is subject to the same scanning, monitoring and recording by the Company as work-related email.
- Personal email should be just that – personal. Your company email must not be used for commercial purposes, such as buying or selling goods, or for running a personal business.

3.3 EMAIL SECURITY

The Company undertakes automated scans of email, both internal and external, to monitor and reduce spam, viruses and inappropriate content. This may result in some messages being quarantined by the scanning software.

If you believe that a message you have sent, or that has been sent to you, has been blocked without good cause, firstly, check Mimecast for on-hold messages or contact the IT Service Desk for assistance

Unsolicited email attempting to sell commodities or services (Spam), malicious software and viruses are a continuing and ongoing problem.

You must:

- Be wary of unsolicited emails, especially those with “enticing” content. If in any doubt, delete emails of this kind without opening them. Do not open attachments or follow Internet links in unsolicited email. Be especially wary if the email message has originated from the Internet.
- Report all emails purporting to be from banks or other institutions, requesting personal details, bank details or money, to the IT Service Desk as these are treated as fraudulent requests.
- Please be cautious before providing any personal details, bank details or money in response to internal email requests. Although most requests made on internal email will be legitimate, some hoaxers will try to impersonate an internal member of staff.
- Report any security alerts, unexpected events or warnings about malicious software or viruses to the IT Service Desk.

However,

- Do not forward “chain email”, virus messages or other warnings. If you receive a security message or warning that you believe may need to be distributed throughout The Company, please contact the IT ServiceDesk.
- Do not subscribe to Internet and email lists unless they are for business purposes.
- Spam is usually a service issue rather than a security issue. However, you should report the receipt of persistent Spam message to the IT service desk to enable the sending email address to be blacklisted.

3.3.1 Email retention

Certain Email messages may constitute a business record, representing a material discussion leading to a business decision, or indeed an agreement or offer between the Company and its customers or suppliers. Such emails must be retained.

The use of Microsoft Outlook Mailbox folders as a long-term storage area is not allowed. Emails will automatically be archived.

3.3.2 Access to your email by other members of staff

There are times when it is necessary for another member of staff to access your email account (such as when you on leave for an extended period of time). Wherever possible, you should set up this access before you go on leave by setting the appropriate permissions in Microsoft Outlook.

In situations where this is not possible, such as sickness, another member of staff may be granted access to your email at the request of your Line Manager, who should send the request by email to the IT Service Desk.

3.3.3 Out-of-Office Messages

If you are unable to check your email due to leave or working away from the office, you should set up an out-of-office message on your Microsoft Outlook Mailbox.

Care should be taken when composing the message to ensure that it does not contain any sensitive information, as out-of-office reply messages can be forwarded over the Internet.

3.3.4 Auto-forwarding Email

Auto-forward rules should only be set after consultation with your Line Manager and with due consideration to both the sender(s) and the recipient.

Auto-forward rules must not be used to forward email over the Internet or to personal email accounts.

3.3.5 Company Issued Email Capable Devices

The care and security of both fixed and portable equipment, such as laptops, tablets, desktops, printers, cameras, mobile telephones, portable storage devices etc., (this list is not exhaustive), is the responsibility of the person to whom it is allocated. Treat any company equipment as you would your own. In particular:

- When travelling and wherever possible, carry portable devices as hand luggage.
- Do not leave devices where they are visible to others, whether in a car, in a site office, or in hotel rooms.
- No equipment must be left in a car overnight.
- Do not leave corporate devices in unsecured locations.

Security devices are available from your IT department to lock laptops. All laptops must be locked away or secured at the end of each day.

Ultimately, the company reserves the right to recover the cost of repair or replacement for any device lost, stolen or damaged as a result of negligence on behalf of the person to whom it is assigned.

3.3.6 Downloading company emails and data to a personal device

ISG does not permit the downloading of company emails and data to a personal device, widely known as 'bring your own device or BYOD'

4 COMPANY DEVICES, INCLUDING LAPTOPS, TELEPHONES & MOBILE DEVICES

4.1 PERSONAL USE OF TELEPHONES

Private use of company telephones and mobiles is allowed provided it does not disrupt your work or the work of others. In order to avoid such disruption, the number and duration of private calls should be kept to an absolute minimum.

Calls to premium rate lines are not permitted. Be aware of calls to '08xx' as they will incur larger call costs. Similarly, text messages to premium rate numbers are also not permitted.

The cost and duration of calls may be monitored and if the level of any private usage is deemed unacceptable, the user may be expected to meet the cost of those calls.

Overseas usage should be kept to a minimum, and only occur during business travel because of the extremely high cost of international calls and text messages.

Before travelling, you should find out data, call and text charges of the country of travel, so potential high charges are known.

4.2 USING YOUR COMPANY PHONE IN THE CAR

Never use a **hand-held** telephone or any similar device whilst driving. The rules are the same if you are stopped at traffic lights or are queuing in traffic.

4.3 DATA USAGE AND CONSUMPTION

When downloading data, wherever possible use Wi-Fi. Be conscious of data charges, for example if viewing videos, especially when not connected to Wi-Fi. You are expected to use reasonable judgement when using data services. Note also, that Company equipment, should not be used whilst abroad for personal use. Employees may be held financially responsible for anything deemed as excessive use.

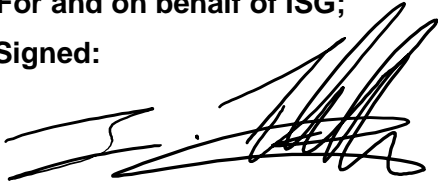
Hotspots can be very useful; however, they have variable levels of security. Whilst the leading mobile providers will have a good level of security, smaller organisations, institutions and shops may not. If your conversation is of a confidential nature or if sending data, you should exercise caution.

4.4 PERSONAL MOBILE TELEPHONES & TABLETS

The use of personal mobile telephones and tablets during working hours should be kept to a minimum.

For and on behalf of ISG;

Signed:



**Ian Tyler-Clarke
Group IT Operations Director**

30th November 2020



APPENDIX A

Appendix A replaces sections 1.5 and 1.6 of the Acceptable Use Policy for any staff in ISG Asia, Commtech and Middle East who use their own personal mobile devices to access company email.

For staff in ISG Asia, Commtech and Middle East who use a corporate device to access company email, sections 1.5 and 1.6 of this document still apply.

ISG Asia, Commtech and Middle East use of personal mobile phones for business purposes

Only personal devices which are supported by Microsoft will be permitted to be used to access company information and at the discretion of ISG these devices may be enrolled onto our company portal, so that we can ensure ISG data is deleted when no longer needed. Details of the devices and the supported operating systems can be found on the Microsoft website.

ISG will protect personal data collected as a result of your employment. You should not have an expectation of privacy when accessing Company data via your personal mobile device. To guarantee the confidentiality, integrity and availability of ISG's data, we may monitor the emails and the content of any communication sent from your ISG email account on your personal device.

When using your personal device for ISG activities, such as sending emails, it must not be used in any way that is derogatory, defamatory, offensive, illegal or could bring the Company into disrepute.

Any personal device containing ISG data which is lost or stolen, must be reported immediately to the IT Service Desk, so that access to ISG email accounts can immediately be disabled.

On leaving ISG's employment, ISG's data will be wiped from the personal device. In the event that you wish to use a new or different device to access company data, you must ensure that ISG data is completely removed from your previous device. Call the IT Service Desk for assistance or advice if required.

It is the Line Manager's responsibility to ensure that all ISG IT equipment is returned to Group IT. All leavers must return all ISG issued equipment to their Line Manager or Group IT or in the event that neither of these are available, to their local Human Resources representative. All equipment must ultimately be returned to the Group IT department. Equipment must not be passed onto another ISG employee to use without prior approval by Group IT. The Company reserves the right to seek financial recompense for any equipment that is not returned.

USE OF PERSONAL COMPUTING AND COMMUNICATION FACILITIES

Only personal devices on the approved Microsoft list (as per link referenced above) with the latest support operating system can be connected to the ISG Office 365 portal or company network for the sole purpose of accessing ISG data.