THINK. PROTECT. RESPECT.

Compass Group UK and Ireland Limited
IT and Information Security
Acceptable Usage Guidelines

WE'RE INFORMATION SECURITY

COMPASS GROUP

PRINCIPLES

- Responsible use of information systems and information security APPLIES TO US ALL
- Use CARE and COMMON SENSE in your use of all information systems
- NEVER do anything which is illegal, could cause harm to Compass' business interests or reputation or could cause damage or disruption to Compass systems
- Be aware of the INCIDENT REPORTING PROCEDURE and report any security related incident IMMEDIATELY

ALL EQUIPMENT

- All IT equipment and information systems are FOR BUSINESS USE ONLY
- Lock your workstation/laptop when you are away from it
- Use passwords and encryption where available to protect unauthorised access
- Ensure that all files received have been subject to virus checking before they are opened
- NEVER install unauthorised software (all installation should be carried out by the IT department) or connect your own devices to equipment
- If you suspect that your computer has a virus leave the equipment on, unplug the network cable and call the IT Helpdesk IMMEDIATELY
- Never let anyone else use your portable equipment/systems or your desktop system whilst you are logged in
- Use CARE and COMMON SENSE in your use of all information systems

PORTABLE EQUIPMENT

- YOU are responsible for the care, safe storage and physical security of portable equipment (see policy table for prescribed procedure)
- Do not view sensitive information in public areas where there is a possibility of being overlooked

PASSWORDS

- Don't disclose your password to anyone or use anyone else's password
- Don't use predicable passwords and change your password regularly
- Don't write your password down and leave it near to equipment

E-MAIL

- Remember that e-mail is not a secure method of communication and should be marked in accordance with the Information Classification Policy
- Use the same care in drafting e-mail as for any company headed letter
- Do not circulate non-work related material
- The content of any e-mail is governed by Compass' Business Ethics policy and Code of Business Conduct

WEB ACCESS

- This is provided primarily for BUSINESS use only
- Reasonable personal web access is permitted during authorised breaks or out of working hours subject to company policy (including rights to monitor or withdraw such facility)

PRINTING

- Be cost conscious when printing documents ensuring that printing is essential (printing relevant sections, double sided, black and white where possible)
- Never leave printing in the printing/photocopying area where it can be viewed or intercepted by others

Any breaches of the above guidelines and rules may lead to disciplinary action being taken in line with the Company's Disciplinary Procedure.

Document Owner: Legal Department
Version: v1 August 2013

THINK. PROTECT. RESPECT.

Compass Group UK and Ireland Limited
IT and Information Security
Acceptable Usage Policy

Compass Group UK and Ireland
Acceptable Usage Policy

July 2013

Category	Information Security
Version	1.0
Classification	[Internal Use]

Compass Group UK and Ireland Limited
IT and Information Security

Acceptable Usage Policy

Document Control

Organisation	Compass Group UK & Ireland Limited
Title	Acceptable Usage Policy
Author	Jodi Lea, Legal Counsel
Filename	
Owner	Legal Department
Subject	Information Security
Protective Marking	
Review date	

Revision History

Revision Date	Version Number	Revised By	Description of Revision
2 August	1	Jodi Lea/Roger Downing	Document creation

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Roger Downing		
ISSC		

Document Distribution

This document will be distributed to:

Date	Method	Recipient Group

Compass Group UK and Ireland Limited
IT and Information Security

Acceptable Usage Policy

Table of Contents

Compass Group UK and Ireland Limited
IT and Information Security

Acceptable Usage Policy

1 INFORMATION SECURITY WITHIN COMPASS GROUP, UK & IRELAND LIMITED ("COMPASS")

AIM

The aim of this Policy is to govern the use of Information Technology Systems in order to protect Compass, its people, its clients and suppliers.

SCOPE

This Policy applies to all users granted access to Compass IT Systems including, for example, employees, temporary staff, voluntary staff, employees of partner organisations, contractors and sub-contractors, agents and work experience placements or any other external users. IT systems include all hardware and software provided or supported by the local Information Technology Departments and/or those connected to Compass' network. Use of the IT systems includes the use of data and programs stored on such computing systems, on USB, disc, CD or any other storage media owned or maintained by Compass.

Principles of information security:-

- Information is an asset. Like any other business asset it has a value and must be protected.
- The systems that enable Compass to store, process and communicate this information must also be protected.
- 'Information Systems' is the collective term for the information and the systems used by Compass to store, process and communicate it.
- The practice of protecting Compass' information systems is known as 'Information Security'.

2 GENERAL PRINCIPLES

Things to know

- ⓘ Information Security is everybody's responsibility.
- ⓘ Compass' Information Systems are provided for business use.
- ⓘ Use of any Compass Information Systems for personal reasons (including e-mail and the web) is only permitted in accordance with the guidance in this Policy.
- ⓘ Compass reserves the right to monitor any aspect of its Information Systems in order to protect its lawful business interests. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings.
- ⓘ You should have no expectation of privacy when using Compass Information Systems.
- ⓘ Breach of this Policy will result in one or more of the following, depending on the severity of the breach:-
    - Short term or permanent suspension of access to Compass IT systems
    - Disciplinary action
    - Dismissal for gross misconduct
    - Criminal proceedings
    - Civil proceedings to recover damages

Things to do

- ☑ Exercise care and common sense in your use of Information Systems.
- ☑ Report any security-related incident in accordance with the Incident Reporting Policy [insert link].
- ☑ If in doubt, contact your line manager or your HR representatives.

Things not to do

- ☒ Anything illegal.
- ☒ Anything that contravenes this or any other Compass policy.
- ☒ Anything that will harm the commercial interests, reputation or business objectives of Compass.
- ☒ Anything that could cause damage or disruption to Compass' systems or business.

3 YOUR COMPUTER

Things to know

- ⓘ "Your" computer is the property of Compass and has been prepared by the IT department for use on the Compass network.
- ⓘ Data saved locally on the C drive will be centrally backed up. In the event of your laptop/computer breaking, being lost/stolen or replaced, your data can be recovered from the last successful back up.
- ⓘ Desktop data stored locally on the C drive is not backed up centrally. If you do not either move this data to a network drive or take regular backups yourself, this data will be lost if your desktop breaks or is replaced.
- ⓘ Compass may at any time and without prior notice:-
  - Audit your computer to ensure compliance with policy
  - Require the return of your computer and any associated equipment
- ⓘ Remote access to Compass' network and resources is available through VPN (Virtual Private Network) software.

Things to do

- ☑ Lock your workstation (CTRL+ALT+DEL for Windows or CTRL+ALT+L for Netbooks) when you are away from it.
- ☑ Save data to network drives where it will be automatically backed-up for you.
- ☑ Ensure that files received from anywhere outside Compass are virus checked before you open them. This includes files on CD, floppy, or USB drive. If in doubt, ask IT Support Services to scan it for you.
- ☑ If you suspect that your computer may have a virus, leave your computer on, unplug the network cable and call IT Support Services.
- ☑ Turn your PC and monitor off at night to save energy unless there is a specific reason to leave it on.
- ☑ Ensure that your computer is supported via an approved anti-virus system. You can receive the latest updates by connecting to the network which you should do at least every 30 days. If you are unsure whether your computer has received relevant updates then contact IT Support Services.

- ☑ Report all incidents of virus/malicious code detected by anti-virus software to IT Support Services.
- ☑ Use passwords and encryption (where available) to protect access to Information Systems and electronic documents.

Things not to do

- ☒ Do not allow anyone else to use your computer while you are logged in.
- ☒ Never install software on your computer. This should only be done by IT Support Services. Things that you should never attempt to install include but are not limited to:-
  - Screen savers
  - Games
  - iTunes or other music download software
  - MSN messenger, Yahoo messenger or other messaging software
  - Skype or other telephony software
  - Utilities that claim to remove spyware or viruses
  - News reader services
- ☒ Do not disable or uninstall any of the software that is installed on your computer
- ☒ Never connect your own devices to your company computer unless the mobile device has first been scanned using anti-virus software installed on your computer.
- ☒ Do not play music CDs. These can sometimes install unwanted software on your computer.
- ☒ Do not store non business related data such as personal photographs, music and video files on Compass' storage facilities.

4 PORTABLE EQUIPMENT

Things to know

ⓘ You should read and understand this section even if you do not normally use portable equipment. You may need to do so at some point in the future.

ⓘ You are responsible for the care and safe storage of any portable equipment that has been issued to you.

ⓘ The term 'portable equipment' covers any company-owned device including:-

- Laptop or tablet PCs
- PDAs (also known as Pocket PCs, Palms or iPaqs)
- Blackberry e-mail devices
- Mobile telephones
- Removable media (e.g. USB or memory sticks, external storage drives, CDs)

Things to do

☑ Back up your work to the network at regular intervals

☑ Use passwords and encryption (where available) to protect access to the portable equipment

☑ Always consider the physical security of your portable equipment:-

In an unlocked office	Kept in a locked drawer.
In the car	You should not leave portable equipment unattended in the car unless there is no safer alternative. In such cases the equipment must be concealed from view, ideally in a locked boot or glove compartment.
At home	Ideally locked away in a cabinet/safe or drawer or otherwise protected by the security measures of your home.
In a hotel	Concealed from view. Ideally locked in a safe or cabinet.
Travelling	Keep the equipment on your person and out of sight at all times.
Screens	Lock your screens or ensure a screensaver has deployed before moving away from your equipment.

- Ensure that your computer screen cannot be overlooked
- Ensure that any papers can be covered in the event of an interruption

Things not to do

- ☒ Do not view sensitive information on the train, plane or in any public area. This provides an opportunity for onlookers. Consider using a privacy screen when it is necessary to view information in public areas.
- ☒ Do not allow family, friends or anybody else to use the equipment.
- ☒ Do not leave portable equipment in the car unless absolutely necessary.

5 YOUR PASSWORD

Things to know

- ⓘ You can change your password at any time utilising the Compass Identity Management system but you should always change it when prompted to by the system.
- ⓘ If you need to grant shared access to files, a diary or e-mail account, this can be arranged by IT Support Services. You do not need to share passwords.
- ⓘ The access rights associated with your user account may be changed or revoked should your employment change or become terminated.

Things to do

- ☑ Set a password or phrase. Password specifications will be notified to you.
- ☑ Change your password if you suspect that someone else may know it.

Things not to do

- ☒ Do not use one of the 'top 5 predictable passwords':-
  - The name of a family member
  - The name of a pet
  - Your football team
  - A rude word
  - An item or brand name that you can see from your desk
- ☒ Do not disclose your password to anyone. Even IT does not need to know it.
- ☒ Do not use anyone else's password.
- ☒ Write your password down and leave it near the equipment.

6 E-MAIL

Things to know

- ⓘ Compass' e-mail systems are provided for business use. Reasonable personal use is permitted, and is defined later in this policy.
- ⓘ Compass monitors all e-mail to ensure compliance with policy.
- ⓘ E-mail is not a secure method of communication. Once a message is sent you have no further control over who reads it.
- ⓘ Contracts can be made by e-mail.
- ⓘ E-mail is admissible in court and carries the same weight as a letter on company headed paper.
- ⓘ Compass can not be held responsible for the content of any e-mail users receive but there are systems in place to minimise e-mails that may be offensive or inappropriate.
- ⓘ Every user will be provided with a fixed amount of storage space on the e-mail server. Failure to monitor and manage space requirements may result in a user's e-mail being temporarily disabled.
- ⓘ Using the Compass e-mail system for personal purposes may result in your address being targeted by spam which increases the risk of viral attack. If your e-mail account receives large volumes of spam contact IT Support Services immediately.

Things to do

- ☑ Use the same care when drafting an e-mail message as you would when writing a letter or memo on company headed paper.
- ☑ Make sure that your message is concise, relevant and sent only to the people that need to read it.
- ☑ Use the telephone or face to face conversation instead of e-mail where this is possible and appropriate.
- ☑ Clear out old and unwanted messages from your mailbox.
- ☑ Delete and/or report to your Line Manager any offensive or inappropriate e-mails received.

Things not to do

- ☒ Never open an attachment that you were not expecting without first having them scanned for viruses, even if you know the sender. Emails are scanned by Compass' IT system but always be wary of opening unexpected attachments.

- ☒ Never supply banking or payment details in response to an e-mail message. This is a well-known method of fraud. Your bank will never request security details by e-mail.
- ☒ Do not use e-mail to send sensitive or confidential information unless it is password protected or encrypted.
- ☒ Do not send or forward anything that:-
    - Contains statements, opinions, comments or transmit documents – text or picture – which are likely to be illegal, pornographic, racist, sexist, discriminatory, offensive or otherwise contrary to the aspirations of Compass.
    - May be defamatory (about an individual or organisation).
    - Is covered by a copyright.
- ☒ Do not circulate non work-related material. This includes but is not limited to:-
    - Jokes
    - Chain letters
    - Virus warnings
    - Software
    - Music, pictures or video
- ☒ Do not disclose any information about a person that you would object to being disclosed about yourself.
- ☒ Never use e-mail to rebuke, criticise or complain about somebody. You may say something that you regret, and the record will be permanent.
- ☒ Never use the e-mail system to store documents, as individual's items which are lost, damaged or deleted, may not be recoverable.
- ☒ Never forward business e-mail to a private address. Automatic forwarded rules to person, external email accounts are prohibited.

7 WEB ACCESS

Things to know

- ⓘ Web access is provided for business use. Reasonable personal use is permitted, and is defined later in this Policy.
- ⓘ Compass monitors and records all web access to ensure compliance with policy.
- ⓘ Access to certain web sites may be blocked in order to protect you and the business. This does not imply the suitability of sites that are not blocked. You must always use your discretion along with the guidance below when visiting web sites.
- ⓘ Where access is permitted, use of social media must be in accordance with the Social Media Policy [LINK].

Things to do

- ☑ Inform IT Support Services if access to a legitimate and business-related web site is blocked.
- ☑ Inform IT Support Services if you believe you have a virus or spyware infection on your computer. Do not attempt to remedy the infection yourself.

Things not to do

- ☒ Do not view or download anything that others may find offensive.
- ☒ Do not download anything that is likely to be covered by copyright. This includes, but is not limited to:-
  - Music
  - Pictures
  - Software
- ☒ Do not use the web for listening to radio or watching video.
- ☒ Do not post comments about individuals on internet bulletin boards, chat rooms or websites as these may give rise to an action for libel.
- ☒ Do not use web-based e-mail (such as Hotmail or Gmail).
- ☒ Do not visit the “high-risk” site categories shown below. Although their content appears to be free, it is often funded by installing spyware on your computer’.
  - Free screensavers and smileys
  - Free music downloads or ringtones

- Free software
- Adult material

☒ Do not post or transmit over the internet any confidential or sensitive information (for example, sensitive company financial or employee information) without encryption technology.

☒ Do not use instant messaging tools as they are not considered to be secure.

8 PRINTING

Things to know

ⓘ Colour printers cost much more per page than black and white ones. Even if there is no colour on the page.

ⓘ Printers are provided for business use only.

ⓘ This Policy applies to all printing including photocopying and scanning.

Things to do

☑ Be selective about what you print. Print only when necessary and only the necessary pages of a document.

☑ Print double sided to save paper where possible.

☑ Use a photocopier when producing a large number of copies.

☑ Keep the area around printers tidy.

☑ Use the secure printing function where possible.

Things not to do

☒ Do not print to a colour printer unless colour conveys important information in your document that would be lost in black and white.

☒ Do not resend your print job if nothing happens. Instead, check the following:-

- Is the print job still listed in the queue?
- Did you send it to the right printer?
- Is the printer switched on?
- Is the printer in an error state because:-
  - There is paper jam

- It is out of paper
- It is out of toner or ink

☒ Leave printing on or around the printing or photocopying area where this is likely to be viewed or intercepted by others.

9 PERSONAL USE

Limited and reasonable personal use of e-mail and the web is permitted. Reasonable use is defined below. Personal use of all other systems is prohibited.

E-mail and web access for personal use have been provided at considerable risk and cost to the company. Compass asks that employees make sensible and conscientious use of these facilities in return.

All e-mail and web access is monitored to ensure compliance with policy. Employees that choose to make personal use of company systems do so in acceptance of the monitoring measures outlined in this Policy.

Personal use of these systems is a privilege. Compass reserves the right to withdraw it either individually or globally at any time without notice or explanation.

Reasonable Use

Reasonable personal use of company systems is that which:-

- ☑ Is lawful and ethical.
- ☑ Is in accordance with this policy.
- ☑ Takes place during authorised breaks or outside of your working hours.
- ☑ Does not adversely affect your productivity.
- ☑ Does not make unreasonable use of limited company resources.

Unreasonable Use

Unreasonable personal use of company systems includes but is not limited to:-

- ☒ Contravention of any Compass policy in any way, including the sending, viewing or downloading of:-
  - Material that others may find offensive
  - Unauthorised software
  - Material covered by copyright, such as music, videos or games

- ☒ Personal use that can reasonably be described as excessive within the context of a professional working environment.
- ☒ Activities for personal financial gain.
- ☒ Use for business other than that of Compass and its associated businesses.
- ☒ 'Blogging' or use of any other social media which contravenes Compass' Social Media Policy and Code of Business Conduct [LINKS].

10 LEGAL RESPONSIBILITIES

Things to know

ⓘ You are personally responsible for ensuring that your use of Information Systems is lawful. Failure to do so may result in any or all of the following:-

- You being personally liable to criminal prosecution.
- You being personally sued for damages in a civil court.
- Compass directors being personally liable to criminal prosecution.
- Compass being sued for damages in a civil court.

ⓘ Emails are disclosable documents which may be required to be produced in legal proceedings or regulatory investigations.

Things to do

☑ Comply with software licences, copyrights and all other laws governing intellectual property.

☑ If you process personal data (data that identifies a living individual) in the course of your work, you must do this in accordance with the Data Protection Act 1998 and Compass' Data Protection Policy [LINK].

Things not to do

☒ Do not borrow or copy company software for use at home or elsewhere.

☒ Do not write or say anything defamatory or potentially libellous about another individual or company.

☒ Do not compromise Compass' reputation through inappropriate content in any method of communication.

11 MONITORING

Information systems and infrastructure are the property of Compass. Compass therefore reserves the right to monitor and record use of these facilities, within government guidelines, to ensure this Policy is being adhered to. Users should be aware that access to websites or personal email correspondence or messages sent via the Intranet or Internet, will be subject to the same monitoring procedures applied to business related access and e-mail correspondence.

If, during the course of carrying out routine monitoring checks, concerns arise about the level of personal use of a user, or if material is discovered that contravenes this Policy, then the user's Line Manager will be informed as well as the appropriate HR representative. Such incidents involving possible misuse of Compass' Information Systems will be investigated and, depending on the outcome of the investigation, may amount to anything from minor to gross misconduct. Users involved in incidents of misuse amounting to gross misconduct may be liable to dismissal.