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

Compass Group, UK and Ireland
Acceptable Usage Policy

May 2020

Category	Information Security
Version	8.5
Classification	Internal Use

Compass Group, UK and Ireland Limited

Acceptable Usage Policy

Document Control

Organisation	Compass Group, UK & Ireland Limited
Title	Acceptable Usage Policy
Author	Director of Legal Services – UK & Ireland
Filename	
Owner	Legal Department
Subject	Information Security
Protective Marking	
Review date	May 2020

Revision History

Revision Date	Version Number	Revised By	Description of Revision
2 August 2013	1	Jodi Lea/Roger Downing	Document creation
11 February 2015	2	Matthew Starling/ Roger Downing/Gary Morris/David Biggs	amendments to comply with IT restructuring including use of MS Cloud and use Your Own Device
7 April 2015	3	MS/GM/DB/MW/RD	Final amendments from steering group
16 April 2015	4	MS/GM	Pilot version of policy for approval by IT
2 June 2015	5	Roger Downing	Pilot version of policy including responses from user community
25 June 2015	6	Gary Morris	Use of Microsoft's encrypted email solution/ doc formatting
23 July 2015	7	Roger Downing	Final amendments from steering group
21 September 2015	8	Roger Downing	General release up-date
19 July 2017	8.1	Gary Morris	General review for applicability with technology.
04 Sept 2018	8.2	Gary Morris	General release update
10 June 2019	8.3	Gary Morris	GDPR best practice update
September 2019	8.4	Gary Morris	New technology update – Cloud use
May 2020	8.5	Gary Morris	Grammar amendments

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Legal Director	Jodi Lea	
ISSC		

Compass Group, UK and Ireland Limited

Acceptable Usage Policy

Document Distribution

This document will be distributed to:

Date	Method	Recipient Group
Sept 2019	Email	Howard James
Oct 2018 onwards	Published internally on Connect	All users

Contents

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

1.1 AIM

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

Where information consists of **personal data** under the Data Protection Act 2018 and associated legislation, Compass must comply with the requirements under that Act to keep this data secure and appropriately limit access to it.

One of the purposes of this Policy is to ensure we remain compliant with those requirements, in addition to other regulations, in our use of Information Technology Systems.

1.2 ADMINISTRATION

This Policy has been agreed by our UK GDPR Steering Committee.

Requests for permissions or assistance under any provisions of this Policy should be directed to the IT department, either by e-mail (support.services@compass-group.co.uk) or by phone on 0845 602 5555 (UK) or 1800 309 244 (Ireland).

1.3 SCOPE AND DEFINITIONS

This Policy applies to all employees using the Information Technology Systems, whether they access those systems from Compass-owned equipment or from their own devices away from Compass offices.

"Users" include employees, temporary staff, voluntary staff, employees of partner organisations, contractors and sub-contractors, agents and work experience placements or any other external users.

"Information Technology Systems" means all hardware and software provided or supported by Compass.

Use of the Information Technology Systems includes the use of data and programs stored on such systems, on USB, disc, CD or any other storage media owned or maintained by Compass.

This Policy must be read in conjunction with Compass's:

- **Social Media Policy**
- **Removable Media and Mobile Device Encryption Policy;** and
- **Information Classification Policy**

Compass's **Information Classification Policy** describes how we categorise our information. When read together with this Policy, it sets out how each category of electronic data must be treated by employees (for example; in relation to restrictions on how data may be shared or stored). Under that Policy, information is classed as:

- **Public**
- **Internal use only**
- **Confidential** or
- **Highly Confidential**.

The Information Classification Policy is referred to throughout this Policy where appropriate. Any references in this document to "**Confidential**" information or data apply to Confidential or Highly Confidential information as described in the Information Classification Policy.

For reference, the definition of "Confidential" under the Information Classification Policy is:

> This is information of a sensitive nature which should only be communicated to individuals or companies that strictly 'need to know' the information.
>
> If confidential information was disclosed to any individual or company other than those who specifically 'need to know' the information it would have an impact on Compass, e.g. financially, legally or to its reputation. It could also have a similar impact on Compass' customers and/or suppliers.

"**Non-confidential**" in this Policy means information that is classified as being **Public** or **Internal Only** under the Information Classification Policy.

1.4 Principles of information security

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

2 GENERAL PRINCIPLES

2.1 Things to know

- ⓘ This Policy outlines the standards you must observe when using our Information technology Systems, the circumstances in which we will monitor your use and the action we will take in respect of breaches of the standards of behaviour set out in this Policy.
- ⓘ This Policy does not form part of any employee's contract of employment and we may amend it at any time.
- ⓘ Information Security is **everybody's** responsibility.
- ⓘ Compass's Information Technology Systems are provided for business use. Use of our Information Technology Systems for personal reasons (including e-mail and the internet) is only permitted in accordance with the guidance in this Policy.
- ⓘ Compass reserves the right to monitor any aspect of its Information Technology Systems to protect its lawful business interests. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings.
- ⓘ Compass cannot give any guarantee of privacy for anything you put on the Information Technology Systems in contravention of this Policy.
- ⓘ 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 the Information Technology Systems
    - Disciplinary action
    - Dismissal for gross misconduct
    - Criminal proceedings
    - Civil proceedings to recover damages

2.2 Things to do

- ☑ Exercise care and common sense in your use of Information Technology Systems.
- ☑ Make sure you have read and understand our:
    - Information Classification Policy
    - Incident Reporting Procedure
    - Social Media Policy; and
    - Removable Media and Mobile Device Encryption Policy
- ☑ Report any security-related incident in accordance with the Incident Reporting Procedure.
- ☑ Contact your line manager or your HR representative if you are in any doubt about any aspect of Information Security or if an incident occurs of which you are aware.

2.3 Things not to do

- ☒ Anything illegal.
- ☒ Anything that contravenes this Policy 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', Information Technology Systems or business.

3 YOUR COMPUTER

3.1 Things to know

- ⓘ "Your" computer is the property of Compass and has been prepared by the IT department for use on the Compass network.
- ⓘ You are responsible for the security of the equipment allocated to or used by you and must not allow anyone else to use it other than in accordance with this Policy.
- ⓘ 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
- ⓘ If you have been provided with a Compass laptop or other corporate portable device, you must read Section 5 in this Policy.
- ⓘ Remote access to our network is only available through corporate VPN (Virtual Private Network) which is available from the 'START' menu on Compass-provided laptops look for "Fortinet SSL VPN".
- ⓘ Whenever possible remote users should always save or share data using their VPN to their network drive folders such as the departmental' K:' drive or if unavailable their 'My Documents' folders as these synchronise to One Drive and are, the most secure way of saving and sharing work-related files.

3.2 Things to do

- ☑ Lock your workstation (CTRL+ALT+DEL for Windows [or CTRL+ALT+L for Netbooks]) or log off when you are away from it.
- ☑ If you suspect that your computer may have a virus, leave your computer on, unplug the network cable and call IT Support.
- ☑ 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, contact IT Support Services.

- ☑ Report all incidents of virus/malicious code detected by anti-virus software to IT Support Services. Report immediately to your line manager and Compass IT Support Services any incident or suspected incidents of unauthorised data access, data loss, and/or disclosure of company resources, databases, networks, etc.
- ☑ Use passwords and encryption (where available) to protect access to Information Technology Systems and electronic documents.

3.3 Things not to do

- ☒ Do not allow anyone else to use your computer while you are logged in.
- ☒ Never leave your user account logged in at an unattended and unlocked computer.
- ☒ Do not attach any device to your computer without authorisation from IT. See Section 5 for more information.
- ☒ Desktop computers and cabling should not be tampered with or moved without first consulting the IT Department.
- ☒ Never attempt to install software on your computer other than the approved applications available from your desktop. Things that you should never attempt to install include but are not limited to:
  - Screen savers
  - Games
  - Music download software
  - MSN messenger, Yahoo messenger or other messaging software other than those authorised by Compass IT
  - Telephony software other than those authorised by Compass IT
  - Utilities that claim to remove spyware or viruses
  - News reader services
- ☒ Do not attempt to disable or uninstall any of the software that is installed on your computer
- ☒ Do not store non-business-related data such as personal photographs, music and video files on your Compass computer or Compass's storage facilities.

4 CLOUD APPLICATIONS

4.1 Things to know

- ⓘ Compass Cloud applications include but are not exclusive to – SAP, One Drive, MS o365 (email), MS Teams, SharePoint, Workplace, Yammer, Connect, Connections.
- ⓘ Microsoft OneDrive, Compass' colleague portal "Connect" and IBM "Connections" (available through Connect) allow users to access certain information from any device, over an ordinary internet connection.

- ⓘ Only approved mobile applications can be downloaded to corporate mobile devices. Requests for new/additional applications can be made through Compass Support Services
- ⓘ Remote users who are unable to connect to our network and who wish to use Cloud Applications must comply with the following requirements:
  - Users provided with an account name wishing to access Connect or Connections can do so remotely from any device and location, over the internet, it will use a secure https connection.
  - Where accessing these from their own device, users must comply with our **Removable Media and Mobile Device Encryption Policy**.
  - Not all features within Connect are available via the internet. Users requiring access to these applications must seek prior authorisation from Compass IT.
- ⓘ Connections Communities allow files to be securely shared with colleagues within a community, from your local computer or remotely over the internet.
- ⓘ Note at present Connections version 4.5 does not allow files to be shared with persons outside of Compass.
- ⓘ All user files in 'My Documents' are automatically uploaded/synchronised to Microsoft's Cloud Application -OneDrive, which you can then access using any device from any location, over an Internet connection (Note: some devices will require the MS One Drive Application installing from the app store).
- ⓘ You can also choose who to share a file or folder with from OneDrive by inviting persons to view or update the file, even if they do not work for Compass (remember to remove their access once finished with).
- ⓘ When accessing information from their own device, users must comply with our Removable Media and Mobile Device Encryption Policy.
- ⓘ Connections and OneDrive can be used to safely upload and share files, whether locally or when away from the workplace, including data classed as **Confidential**, provided users comply with this Policy.
- ⓘ Users are never permitted to access Confidential data stored on OneDrive or Connections from a non-corporate device, such as a user's own PC or mobile device**.**

4.2 Things to do

- ☑ Make sure you have read and understand our **Removable Media and Mobile Device Encryption Policy.**
- ☑ Use OneDrive to share information classified as **Confidential** (or higher) outside of Compass.
- ☑ Make sure that persons outside of Compass with whom you have shared **Confidential** data on OneDrive take care with how they access and handle that data. You should be satisfied, for example, that they will not download the data onto a personal device and that they will keep the data secure and delete their copy once no longer required.
- ☑ Be aware of whom you share documents and folders with, perform regular checks and remove superfluous access.

4.3 Things not to do

- ☒ Never access or download **Confidential** data from OneDrive or Connect/Connections using a device that has not been provided to you by Compass IT (a personal device).
- ☒ Do not keep work-related information on any non-Compass device for any longer than is necessary.
- ☒ Do not share information for longer than is necessary. Delete any shared folders from OneDrive once no longer required.

5 CORPORATE PORTABLE EQUIPMENT

5.1 Things to know

- ⓘ The term "portable equipment" covers any device that can access, read, change or store electronic information and is not permanently connected to a network either physically or wirelessly. Examples include laptops, tablets, phones, USB sticks, portable hard drives, CD's, DVD's, cameras, MP3 players and smart watches.
- ⓘ This section only covers use of Compass-provided portable equipment. If you are using your own device to access Compass systems, you must comply with Compass **Removable Media and Mobile Device Encryption Policy**.
- ⓘ You are responsible for the security, care and safe storage of any Compass portable equipment that has been issued to you.
- ⓘ You must ensure any Compass portable equipment issued to you is always kept secure, especially when travelling.
- ⓘ Passwords/PIN numbers must be used to secure access to data kept on such devices and you should also be mindful that when using devices away from the workplace, documents may be read by third parties, such as passengers on public transport. Consider using a privacy screen.
- ⓘ All devices must be protected where possible by a strong alpha numeric password in accordance with Section 5.
- ⓘ Compass IT Department reserves the right to refuse, by physical and non-physical means, the ability to connect portable devices to Compass systems. Compass IT Department will engage in such action if IT equipment is being used in a way that puts the Information technology systems, data, users, or clients at risk.
- ⓘ Compass IT Department will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with our overarching IT Security Policy. No device that has had its Operating System altered will be permitted access / connection.

ⓘ Compass IT department reserves the right for lost or stolen devices to be remotely wiped of all data. If a corporate device is recovered, it can be submitted to IT for re-provisioning. The remote wipe may destroy all data on the device, whether it is related to company business or personal. By agreeing to this usage Policy, the user understands that their personal data (music, photos, apps, calendar, contacts, etc.) may be erased in the event of a security breach, and therefore must be agreed with before connecting the device to corporate resources.

ⓘ The use of removable media such as USB sticks, portable hard drives, CD's and DVD's, is not permitted except where back-ups are required on Nexus machines or CCTV recording copies required from CCTV recorders which are not networked. In exceptional circumstances, and subject to approval by IT Security and Director, exemptions can be approved. Compass IT can provide a user with an encrypted USB device or with the means of encrypting a device.

5.2 Things to do

☑ Where you are using your own device to access our information, read and make sure you understand the requirements set out in our **Removable Media and Mobile Device Encryption Policy**

☑ Connect to the Compass Network to back up your work at regular intervals.

☑ Use passwords and encryption (where available) to protect access to the portable equipment (see the **Password** section below).

☑ Always consider the physical security of your portable equipment:

In an unlocked office	Kept in a locked drawer or physically secured by other means, such as a Kensington lock.
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	Always keep the equipment on your person and out of sight.
Screens	Lock your screen before moving away from your equipment.

☑ Ensure that your screen cannot be overlooked by anyone who ought not to view it, especially in public places.

- ☑ Ensure that any papers can be covered in the event of an interruption
- ☑ Consider the use of privacy screens on portable devices when used in public places such as public transport (IT.Orders@compass-group.co.uk).
- ☑ If your corporate device is lost or stolen, you must report this immediately to IT Support Services in accordance with the Portable Device Loss Reporting Process. If your corporate device has been stolen, you must also report this to the police and provide IT Support Services with the crime reference number.

5.3 Things not to do

- ☒ **Confidential** data should not to be stored on any portable device unless absolutely necessary. Where possible save such data to OneDrive or to the network drives, before deleting the data from your device.
- ☒ Do not store Compass information (any work-related data) on any non-authorised device, other than is permitted by our **Removable Media and Mobile Device Encryption Policy**.
- ☒ The use of USB storage devices is disabled by default. Data must not be saved to portable storage devices such as USB sticks, CDs and DVDs, unless:
  - you are using a NEXUS machine; or
  - prior approval is given by Compass IT (in exceptional circumstances); in such cases IT can enable USB storage functionality on your device.
- ☒ Do not view Confidential 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 portable device.
- ☒ Do not leave Corporate portable equipment in the car unless necessary and then ensure it is out of sight.

6 YOUR PASSWORD

6.1 Things to know

- ⓘ Each user is granted their own username and password and is accountable for all actions on Compass systems.
- ⓘ Temporary workers requiring access to Compass systems may be granted a username and password for a limited time period following approval by their line manager
- ⓘ Your password does not indicate that your use of Compass systems is private. All passwords are owned by and are the confidential information of Compass.
- ⓘ User accounts are deleted by IT Support Services 90 days after a user leaves Compass.
- ⓘ You can change your password at any time using Connect or Ctrl, Alt + Del, but you should always change it when prompted to by the system

ⓘ The access rights associated with your user account may be changed or revoked should your employment change or become terminated.

ⓘ All portable devices are subject to software and hardware control by Compass where this is technically possible. Applications and software will only be permitted if they are deemed valid business tools supporting the Compass strategy

6.2 Things to do

☑ Set a password or phrase. Your password must:

- be at least 8 characters long
- contain at least 6 alphabetic characters and 3 of the following
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %,@)
- not repeat more than 2 characters consecutively
- contain a combination of upper- and lower-case characters
- not use sequences e.g. 1234, QWERTY

☑ Always change your password if you suspect that someone else may know it.

6.3 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 teams
- A rude word
- An item or brand name that you can see from your desk

☒ Do not disclose your password to anyone. IT Support Services do not need to know it.

☒ Do not use anyone else's account.

☒ Do not write your password down and leave it near the equipment.

7 E-MAIL

7.1 Things to know

- ⓘ Compass's 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 in accordance with the Monitoring section in this? [our] Acceptable Usage Policy.
- ⓘ E-mail is not a secure method of communication unless it is encrypted. Once a message is sent you have no further control over who reads it.
- ⓘ ALL Internal e-mail is encrypted. External e-mail IS NOT.
- ⓘ All external email received has **(EXT)** preceding the subject take extra care with external emails.
- ⓘ Compass IT have provided a secure mail/file transfer solution called 'Egress Switch' for all employees, use can be requested from the Software Centre on the START screen.
- ⓘ 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 cannot 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.
- ⓘ **Confidential data must be encrypted if sent outside of Compass.** Users should consider sharing such data by secure means, such as OneDrive as well as encrypted e-mail or 'Egress Switch'.
- ⓘ Access to an individual's email, for example to cover a colleague absent from work, is blocked by default. Access can only be granted by request in accordance with Compass's Accessing Employee Data Procedure (managed by IT Security and HR).

7.2 Things to do

- ☑ Use OneDrive or encrypted email when sharing any **Confidential** information with anyone outside of Compass. See Section 4.
- ☑ Take care when sharing or sending information using distribution lists (such as emails sent to groups of people) – check who is in the group and make sure you intend sending the e-mail to all persons in the group.
- ☑ When typing the recipient's name, check that auto-complete does not suggest the wrong recipient. Always check the name before sending.

- ☑ Be wary of external email. Check the subject line for **(Ext)** then check the email address carefully for unusual or duplicate characters, especially if requesting information or authorisation.
- ☑ Personal e-mails should be labelled "personal" or "private" in the subject header
- ☑ 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, MS Teams and/or Skype 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.
- ☑ Before sending e-mail:
    - Check whether it contains any **Confidential** information. If it does, you must ensure it is encrypted before sending to an external email address outside of Compass. Consider using OneDrive, 'Egress Switch' or a Connections Community instead;
    - Check that you are not accidentally sending on information to someone which you do not intend e-mailing to that recipient, such as content in the bottom of long chains of e-mails.

7.3 Things not to do

- ☒ Never send e-mail containing **Confidential information** outside of Compass **UNENCRYPTED**.
- ☒ Never forward business e-mail to a private address. Automatic forwarding rules to personal, external email accounts are **prohibited**. Users should consider using OneDrive for remote access to corporate information.
- ☒ Never open an attachment that you were not expecting, even if you know the sender. E-mails are scanned by Compass's IT systems but always be wary of opening unexpected attachments.
- ☒ Never open spam mail. Send it instead to spam.monitor@compass-group.co.uk where IT can investigate it. Note attach the spam mail to another email and send to Spam Monitor, this retains the meta data needed to interrogate the email.
- ☒ Always be wary of unexpected e-mails and the links within them. E-mail is the primary attack vector for criminals; if in doubt contact the sender or contact Support.Services@compass-group.co.uk
- ☒ 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.
- ☒ Never respond to requests for information unless you are 100% certain the request is genuine. If in doubt contact the requester via their publicly available contact details. Do not use links, phone numbers or e-mail addresses in any e-mail sent to you as these may be fake. If still in doubt contact Support.Services@compass-group.co.uk for assistance.

- ☒ Do not send or forward anything that includes but is not limited to:
  - 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 and will be disclosable in litigation or other investigations.
- ☒ Never use the e-mail system to store documents as items which are lost, damaged or deleted, may not be recoverable.
- ☒ Do not delete Compass's standard disclaimer wording on the end of e-mails; it is there for a purpose.

8 INTERNET ACCESS

8.1 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 internet 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.**
- ⓘ Some browsers will offer to 'save' your passwords to enhance the user experience when revisiting a secure site. Be aware these are stored within your browser in the clear and could accessed by someone else if you share your login session.
- ⓘ You can download, but you cannot install unless you have Administrator access.

8.2 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.
- ☑ Inform IT Support Services if you click on anything suspicious or you suspect you've entered your credentials on a suspicious website – Compass IT can check the authenticity of sites.

8.3 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
  - Fonts (Please Note: Downloadable fonts are a regular point of access for malware generally. Fonts seem innocuous but such malware can be embedded within them. Use only the fonts available through Word and O365)
- ☒ Do not use the web for listening to radio or watching video unless as part of a Compass work or training requirement.
- ☒ 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 personal web-based e-mail (such as Hotmail or Gmail) for corporate information.
- ☒ Do not attempt to install any web browsers on Compass equipment which have not been provided with your device.
- ☒ 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
  - Games
- ☒ 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 online document conversion tools – you do not know who can access your document after it has been converted by them.

9 PRINTING

9.1 Things to know

This Policy applies to all printing including photocopying and scanning.

- ⓘ 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.

9.2 Things to do

- ☑ Dispose of all business-related printed material you no longer need, using paper shredder waste bins provided for Confidential and Non-confidential material.
- ☑ Be selective about what you print. Print only when necessary and, if possible, only the necessary pages of a document.
- ☑ Print double sided to save paper where possible.
- ☑ Use a photocopier when producing many copies.
- ☑ Keep the area around printers tidy.
- ☑ Use the secure printing function where possible.
- ☑ Ensure you map the correct 'follow me' printer to your current location.
- ☑ Check which printer you send print to BEFORE printing.

9.3 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
- ☒ Do not leave printing or scanning on or around the printing or photocopying area where this is likely to be viewed or intercepted by others.

10 PERSONAL USE

Reasonable personal use of Compass Information Systems, such as e-mail and the web is permitted. Reasonable use is defined below.

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 applicable Compass policies. Employees that choose to make personal use of company systems do so in acceptance of the monitoring measures outlined in Compass's applicable Policies.

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.

10.1 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.

10.2 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.

11 LEGAL RESPONSIBILITIES

11.1 Things to know

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

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

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

11.2 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 2018 and Compass's various policies that support our compliance with all data protection legislation.

11.3 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's reputation through inappropriate content in any method of communication.

12 MONITORING

12.1 Information Technology 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.

12.2 Users should be aware that access to websites or personal e-mail 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.

12.3 If, while 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.

12.4 Incidents involving possible misuse of Compass's Information Technology 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.