

Digital & Technology (D&T)

Acceptable Usage Policy

Management Standard

Changes made

|  |  |  |  |
| --- | --- | --- | --- |
| **WHAT** | **WHO** | **WHEN** | **CHESS #** |
| **First Issue** | K Marappan | 01-Jul-2017 | CHESS 100033 |
| Updated Social Networking | K Marappan | 07-Feb-2018 | CHESS 103669 |
| Reviewed the document and replaced references to Human Resources / HR with People, IS&T / IT with D&TS. | K Marappan | 23-Mar-2020 | CHESS 137229 |
| Add Section on Hardware and Software Standards. | Darren Shearsby | 03-Sep-2020 | CHESS 158380 |
| Replaced references to Digital & Technology Solutions (D&TS) with Digital & Technology (D&T). | C Tuite | 20-Oct-2020 | CHESS 162818 |
| Roles and Responsibilities | K Kehoe  S Gandabhai | 30-Aug-2021 | CHESS 204907 |
| Briefly describe the changes made to the document. | Enter the first initial and surname of the person who is making a change to the document. | DD-MM-YYYY | CHESS |
|  |  |  |  |
|  |  |  |  |

Contents

[PURPOSE 4](#_Toc81211643)

[SCOPE 4](#_Toc81211644)

[ROLES AND RESPONSIBILITIES 4](#_Toc81211645)

[GUIDING PRINCIPLES 4](#_Toc81211646)

[1. Acceptable use of company electronic communication systems 5](#_Toc81211647)

[2. Acceptable use of company Internet systems 7](#_Toc81211648)

[3. Maintain security 9](#_Toc81211649)

[4. Hardware and software standards 12](#_Toc81211650)

[5. Monitoring 14](#_Toc81211651)

# Purpose

This document sets out the Compass Group PLC (and other head office companies based in Australia, such as Compass Group (Australia) Pty) ("the company”) policy governing use of Digital & Technology (D&T) systems with the purpose of protecting the company, its people and its customers. As company users frequently need to access company systems and the Internet to conduct business, this policy provides acceptable use requirements when working on a company system.

# Scope

This Policy applies to all company employees (including temporary, contractor and consultant personnel) and external users who have been authorised to access company D&T systems. D&T systems include all hardware and software and internet-based D&T services provided or supported by the local Digital & Technology (D&T) departments and / or those connected to the company network. Use of the D&T systems includes the use of data and programs stored on such computing systems, on removable media (e.g. USB storage device, DVD / CD, disk, portable hard drive, tape), or any other storage media owned or maintained by the company.

# Roles and responsibilties

All employees are required to use D&T facilities in a professional and responsible manner at all times and in accordance with this Digital & Technology (D&T) Acceptable Usage Policy.

It should be noted that all work performed on company D&T systems (e.g. servers, desktop PCs, laptops, tablets, mobile devices, telecommunications, Internet, e-mail) belongs to the company and may be monitored. Although the equipment is provided solely for business use, the company has no objection to occasional personal use on the proviso it does not become significant or cause disruption to company systems – this is in line with generally accepted good practice.

Tracking of desktop PCs, laptops, tablets and mobile devices may be activated; you are therefore on notice and by continuing to use such device you give your informed consent to Compass Group tracking your desktop PC, laptop, tablet and mobile device for the purpose of locating lost or stolen devices.

The security measures described within this document set out the minimum requirements for safeguarding company systems and information. Failure to comply with this Policy is a security violation and will be reported to management. Depending on the severity of the violation, a user may lose short-term or permanent access to the D&T systems, and employees of the company may be subject to disciplinary action up to and including dismissal.

# Guiding principles

In order to protect users and the company, use of company D&T systems should adhere to the following principles:

* It does not break the law\*
* It does not risk bringing the company into disrepute or place it in a position of liability
* It does not violate any provision set out in this or any other company policy
* It does not cause damage or disruption to company systems or business
* It does not place company confidential information at risk of unauthorised access

\*In certain instances, misuse of either the Internet or e-mail can constitute a criminal offence. Where the company believes a criminal offence to have taken place, it has a duty to inform the police and / or local authorities. In such cases, individual staff may be open to prosecution and the company, and the individual, could be liable to pay damages. Using company D&T systems in any way that breaks the law is also a serious disciplinary offence.

It is the user’s responsibility to ensure they understand the legal restrictions of the country in which they are working and to adhere to them. Special attention should be paid to sending international messages, which will be subject to the law of other jurisdictions. For further guidance on legal restrictions, users should contact their local People or Legal departments.

## Acceptable use of company electronic communication systems

Only users authorised by local management may utilise electronic communication tools. Approval for access to e-mail, instant messaging and collaboration services must be specifically granted by the user’s departmental head or line manager. It is the responsibility of each department head or line manager to determine what forms of electronic communication and types of services his / her staff require to perform their job responsibilities.

Users utilising electronic communication equipment and systems are required to safeguard company information and assets by understanding and complying with this Policy.

**Ensure use of the company’s e-mail does not risk the company’s reputation**

Users must not make 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 the company.

All usage of company e-mail and instant messaging (e.g. Skype) is monitored. Local D&T departments may, subject to consideration of national privacy laws, scan and record e-mail traffic and instant messaging for information that may be defamatory, illegal, offensive, contrary to the commercial interests of the company or where usage is deemed to be excessive.

E-mail messages are formal communications sent in the name of the company and as such, are the property of the company. Proper business standards should be applied to e-mails. E-mails must be drafted with the same care and accuracy as any other written corporate communication. It is important to note that contracts can be legally enforceable even when made by e-mail or instant messaging using informal language.

Company D&T departments cannot be held responsible for the content of any e-mail users receive, but endeavour to prevent e-mails that may be offensive or inappropriate. If users receive such e-mails, they should delete them immediately and report to them to their line manager or the local D&T Security Manager.

|  |
| --- |
| Users ***must not:***   * Open unknown or unusual looking e-mail messages or attachments to unknown e­mails, without first having them scanned for viruses by D&T * Forward security and virus warnings, special offers or chain-letter messages. Such messages tend to be hoaxes and are designed to cause unnecessary concern. Continued re-forwarding of these hoaxes wastes time and e-mail bandwidth * Forward company e-mail to a private address * Use the e-mail system to store documents, as individual items which are lost, damaged or deleted, may not be recoverable or * Send confidential or sensitive information via e-mail without encryption technology.   Confidential or sensitive information includes, without limitation, communications of a litigious nature, sensitive company information (including financial) and personnel employee information. |

**E-mail, instant messages\* and recorded voice may be admissible as evidence in a court of law**

Users should ensure they do not compromise the company's reputation through inappropriate content in e-mail, text-based messaging, instant messaging or teleconferencing. E-mails are disclosable documents which may be required to be produced in legal proceedings or regulatory investigations.

**Ensure electronic communication is not potentially libellous**

Users must not make personal comments about an individual, or discuss their characteristics or abilities using e-mail or instant messaging\*. Additionally, users must not request responses about an individual's characteristics or abilities via e-mail or instant messaging as comments may inadvertently be libellous.

**Personal messages**

E-mail and instant messaging should be used primarily for legitimate business purposes, however, brief and occasional e-mail or instant messages of a personal nature may be sent and received.

**Conflicts of interest**

Users may not use e-mail or other electronic communications tools provided by the company to conduct any other business or commercial activities to the extent that such business or commercial activities interfere with the user’s employment, is competitive with the company’s business, or may be construed as a conflict of interest. As such, users shall not subscribe to mailing lists or mail services for personal use.

**Storage capacity**

Every e-mail 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.

**Use of customer electronic systems**

The use of a customer's or client's electronic system is governed by this Policy. Users must adhere to the confidentiality provisions of this Policy and refrain from transmitting any of the company’s confidential and / or proprietary information, sensitive information, or personally identifiable information via customer or client systems. Specific questions regarding use of such systems should be directed to local D&T departments.

## Acceptable use of company Internet systems

**General use**

Users who are authorised to access the Internet should use the Internet for legitimate company business only. The company recognises; however, users may need to access the Internet for personal business. Brief and occasional personal use is acceptable, provided such use is not excessive.

Excessive use of the Internet for personal business during work hours is considered outside a user's scope of employment or services and, depending on the severity of the infraction, a user may lose short-term or permanent access to the Internet, and employees of the company may be subject to disciplinary action up to and including dismissal. "Excessive use” is determined by the user's immediate manager or department head, and the local People department. Additionally, users should limit their use of streaming media of audio or video (including internet radio, web TV, music, web cams) from the internet due to the impact on the company network.

|  |
| --- |
| Local D&T departments control access to the Internet and software has been deployed to filter and monitor access and Internet usage. When accessing the Internet using company D&T equipment, users ***must not:***   * Access, download, forward or distribute material via the company's systems which is illegal or likely to cause offence * Unless required for business purposes, intentionally download, launch, install or save any unauthorised wallpaper, sound, screen saver, video clip, game or executable file (for example, files with extensions such as .exe, .com, .avi, .mpeg, .bat, .js, .mp3). In addition to these types of files, users must not distribute (by e-mail or otherwise) image files (for example, files with extensions such as .jpg) that are not for business purposes * Access web pages or news feeds or participate in a chat room whose content is unknown to the user or whose content is likely to involve pornography or support for an illegal, racist or offensive activity * Post comments about individuals on Internet bulletin boards, chat rooms or websites. These may give rise to an action for libel against the company and/or the author * Post, or transmit over the internet, confidential or sensitive information without encryption technology. Confidential or sensitive information includes, without limitation, communication of a litigious nature, sensitive company information (including financial information) or personnel employee information * Publish personal information on the Internet. This may expose users to the risk of identity theft. Users should always review the privacy and security settings of sites being used * Store non-business-related data such as personal photographs, music, and video files on the company's storage facilities * Join any chat groups or special interest groups for business purposes or on behalf of the company unless authorised to do so by management. A copy of the written authorisation should be retained * Use the Internet for any personal monetary interests or gain. Personal Internet use shall not cause the company to incur a direct cost in addition to the general overhead of an Internet connection * Use the Internet devices to disable, impair, or overload performance of any computer system or network, or to circumvent any system intended to protect the privacy or security of another user. |

**Instant messaging**

Instant Messaging (IM) tools should not be considered secure and as such, use of public IM tools is prohibited. Use of IM tools approved by local D&T management are permitted, however, users should never click on a URL link sent via instant messenger if it appears unfamiliar or out of character for the sender. Users should confirm the validity of the link with the sender before attempting to access the site. In addition, files received via instant messenger must be scanned with a virus scanner prior to being opened or executed.

**Web logs (‘blogs’)**

‘Blogging’ is the practice of posting entries in a Web log. A Web log, usually shortened to ‘blog’, is a web-based publication consisting primarily of periodic entries, or articles, regarding a particular subject, normally in reverse chronological order.

Users are expected to exercise good judgment and act in a professional manner whenever accessing the Internet or any other external system. Users should not disclose or discuss company confidential or proprietary information in a blog. Users should not include libellous, slanderous, threatening, abusive or other inappropriate messages about the company or its customers in any web posting or blog. Users should also refrain from using, posting or copying third-party materials protected by copyright laws. If protection is in question and the user believes ‘fair use’ rights may allow for such use, posting, or copying, he/she must ensure, without reservation, the materials are not protected. Users must refrain from using third-party trademarks, logos, and slogans, as well as disclosing any trade secrets without the third party's permission.

**Social networking**

Compass Group Australia is active on social media, with accounts on Facebook, LinkedIn and Instagram. Our employees are encouraged to like, follow and contribute to Compass’ social media pages, however the use of Compass’ social media channels are no different to any other form of company communication. Employees must not post any material that is confidential or proprietary in nature, that may be offensive, discriminatory or damaging to Compass, a fellow employee, a customer or client. Please ensure you are familiar with the full Digital & Technology (D&T) Acceptable Usage Policy, as breaching these guidelines may result in disciplinary action.

## Maintain security

**D&T systems and infrastructure**

Maintaining the security of company D&T systems and infrastructure is imperative. It is the user’s responsibility to ensure that any system which has been entrusted to them is secure and complies with relevant company security standards and policies.

**Payment card industry data security standards (PCI DSS)**

PCI DSS is an international set of comprehensive requirements for enhancing payment account data security and was developed by the Payment Card Industry Security Standards Council (PCI SSC). The PCI DSS are technical and operational requirements created to help organisations which process card payments, to proactively protect customer account data. The standards apply to organisations which store, process or transmit cardholder data.

**Processing of customer credit card transactions**

Users must not use company computer systems to process or transmit customer credit card information (including e-mailing card numbers or using web-based payment systems). The appropriate handling process for transactions where the customer is not present (such as phone orders) is described in more detail in local Finance and D&T policies. Non-compliance with the PCI DSS could lead to fines and / or penalties for the company in addition to reputational damage.

**Report a missing PC, laptop, mobile device or removable storage device immediately**

Security of company data is the priority when D&T equipment is identified as missing.

Users must report **immediately** missing D&T equipment or storage media which contains sensitive data to their local D&T department and to their Line Manager. This includes all types of storage media including USB memory sticks and storage devices, DVDs/CDs, disks, portable hard drives and tapes.

**Removable media**

In general, use of removable media (e.g. USB storage device, DVD/CD, disk, portable hard drive, tape) is prohibited. Users with specific authorisation and access rights to use such devices must ensure data is retained in the password protected area of the device and encrypted to ensure data is kept secure if mislaid or stolen. Where usage is authorised, all data-files and programs must be scanned with anti-virus software before opening the content from removable media.

|  |
| --- |
| **Keep data safe**   * Users must lock their screen before moving away [Ctrl + Alt + Del, lock workstation] * Users must keep their laptops and mobile devices (including storage media) physically secure and out of sight (where possible) e.g., in a lockable drawer or cupboard when not in use at any time during the day and in particular at night, week-ends and when travelling * Users should carry laptops and mobile devices (including storage media) in hand­ held baggage when using public transportation. Users should **not** "check-in" such items for transportation by another party * Users must not connect any PC not owned by the company to the company's network unless specifically authorised by local D&T management. This includes visitor, consultant and contractor owned PCs * Users must ensure they protect their screen from being viewed by others whilst working on public transport or in public places such as airports, railway stations or cafes and * Users must return removable media and storage devices to their line manager or local D&T department when no longer needed or on termination of employment. |
| **Protect data against unauthorised access**   * Users must use passwords and encryption to protect access to company D&T systems and electronic documents * Users must not disclose passwords to anyone or share their user account with any other person. An exception to this is that a user may provide his/her password, at his/her discretion, to authorised personnel within their local D&T department, only if the user has initiated a support request. On completion of the support request, the user must change his/her password * Users must not write their passwords down * Users must not allow an unauthorised person (including family members or friends) to use their PC. Unauthorised use of a login and use rid will be attributed to the user and may result in disciplinary action * Users must not install or use software on company-issued computers and devices (i.e., desktops, PCs, laptops, phones, tablet computers and other mobile devices) that is not pre-approved and installed by local D&T departments and * Users must ensure that access permissions are set appropriately so that electronic documents and other data files are only accessible by authorised personnel. |

**Remote access**

Remote access to the company network and internal D&T resources is only granted to users with a specific business requirement and must be approved by local D&T management. Users must connect to the network using VPN (virtual private network) software that is approved by local D&T management. The same guidelines defined in the section ‘acceptable use of company Internet systems’ must be adhered to.

**Mobile devices**

Users must ensure the same security precautions be adhered to with the use of any mobile devices (i.e. tablet computers, phones and other mobile computer devices).

Mobile devices must not be used if they contravene this Acceptable Usage Policy. Users should treat mobile devices in the same way as any company laptop under the rules for safeguarding systems and the information on them set out in this document. This includes protecting access to the device by setting a password and encrypting sensitive data.

The use of mobile devices in motor vehicles must never compromise safety. Countries have enacted laws regulating use in vehicles and users are expected to become familiar with and to comply with these laws.

Users must not store company confidential or sensitive information on their privately owned personal electronic devices.

**Maintain anti-virus protection**

* Users must ensure their company issued devices receive regular anti-virus and security system updates if they are working away from the office
* Users must not bypass anti-virus checks when sending or receiving data files. Any received file, whether by email attachment, or downloaded from the internet, or provided on a removable storage device, can introduce a virus to a PC or mobile device
* Users must immediately report all incidences of virus / malicious code detected by anti-virus software to their local D&T department

## Hardware and software standards

**Compass assets – hardware**

Hardware always remains the property of Compass Group, on cessation of employment all Compass Group hardware must be returned in a clean, tidy, working and prompt fashion to D&T.

Where possible hardware shall be purchased from Compass Group D&T catalogue, where this is not possible hardware shall be purchased from preferred suppliers in the country where the business unit is located to ensure that any warranty is easily claimable.

**Compass assets – software**

The unauthorised duplication of copyrighted computer software violates the law and is contrary to Compass Group standards of conduct and business practice. D&T disapproves of such copying and recognises the following principles as the basis for preventing its occurrence within Compass.

* Neither permits nor tolerates the making or use of unauthorised software copies within the organisation under any circumstances.
* will provide in a timely fashion enough legitimately acquired software to meet all software needs for all computer hardware.
* will comply with all licensing terms and conditions regulating the use of any software it acquires.
* Will enforce strong controls to prevent the making or use of unauthorised software copies. These will include effective measures to verify compliance with these standards and appropriate disciplinary action for any violation of these standards.
* will take steps to inform current and future employees of their legal responsibilities in relation to software theft.

|  |
| --- |
| **Technology and cyber risk**   * User must not purchase cloud software without approval from D&T. Software that is not reviewed is a risk to our systems and data from cyber-attacks. * Users must not purchase unapproved hardware. Un-verified hardware increases the risk of devices that run unsecure software and a lack of hardware maintenance. * Users must not purchase desktop software that is not on the MyService catalogue. Unapproved software creates exposure to licencing breaches and software vulnerabilities. * Users must not purchase hardware and software using P-cards. * Users must lodge an authorisation to purchase request through my service. A ticket number will be assigned, and the request validated as standard or non-standard. * Users must not purchase software or hardware from unapproved vendors. All purchases must be reviewed and approved boy Foodbuy & D&T. * Users must not make unauthorised purchase that put personal identifiable information, credit cards data or health data at risk. Data of this nature is regulated and can result in compass being fined affecting reputation and revenue. |

All software purchases (such as more specialised software and cloud) must go through D&T. This is to ensure:

* That software is correctly added to the asset register upon purchase and receipt.
* That software is allocated against the asset in the database.
* That audits of software on computers can occur against a reliable account of owned software.
* Appropriate risk assessment and data classifications are completed of Cloud based software and installed software.
* That site licence price savings can be achieved through a coordinated approach to purchasing software.
* That upgrades of software can occur, generally business wide, to ensure minimum confusion between versions.
* That all instances of licence documentation, software media and copies of delegation/invoice details for the software are held and accounted for in the company.
* Software compliance by the company as outlined in this policy.

Software always remains the property of Compass Group, on cessation of employment all Compass Group software must be returned in a prompt fashion to Compass Group. Users are not permitted to install their own software on any company computers, without prior approval from their supervisor or manager.

Failure to comply may result in users being held personally responsible for any data loss or penalties imposed for breach of copyright. Installation or use of peer to peer file sharing programs such as LimeWire, BitTorrent, etc, is not permitted on computers connected to the Compass Group network. Users shall not download or authorise downloading of information or software from the internet or emails to provide to a third party violate copyright, license agreements or contract of usage.

## Monitoring

Compass Group uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems.

In keeping with these objectives, management maintains the authority to:

* Restrict or revoke any user's privileges
* Inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives and
* Take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users.

Compass may take disciplinary action, including termination of employment, depending upon the severity of the policy breach

D&T systems and infrastructure are the property of the company. The company, therefore, reserves the right to monitor and record use of these facilities, where local privacy laws permit, to ensure the policy on acceptable use is being adhered to. 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.

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 personnel within their local People department. Such incidents involving possible misuse of company D&T systems will be investigated and, depending on the outcome of the investigation, may result in disciplinary action including, in appropriate cases, dismissal.

Compass Group (Australia) Pty D&T