colart

GLOBAL TECHNOLOGY POLICY

Table of Contents

Overview

INTRODUCTION

This document has been completed by the Technology department, in conjunction with HR and the GLT. It is a Global Policy.

The Human Resources department will issue this policy statement to all new employees as part of the induction process. It will also be issued to all existing staff. The declaration on the last page must be signed by all staff and returned to the Human Resources department. The signed declaration will be retained in the employee's personal file. A copy of the document is also held on the IT section of the Intranet toolbox.

This document is live and there will be updates. Any significant updates will be notified and circulated to all global staff as appropriate.

RESPONSIBILITIES

All data is the property of the company "Colart" as a corporate unit. It is the responsibility of **all** employees to protect all data used within the company.

It is the responsibility of the Global IT Team to ensure that no unauthorised access to any IT Systems is allowed by proper control of access to user accounts, devices, communications and server equipment.

Access control measures, and protection, of the sales, financial, IT, marketing, I&D, accounting and personnel records systems is the responsibility of the appropriate department managers who will authorise relevant access rights as are required for members of their staff to undertake their duties.

No data shall be disclosed unless authorised. In some cases this is implicit as part of the job being carried out such as disclosure to a customer of the details held on file as part of a customer enquiry.

When working with partners when the sharing of company data is required such as a project utilizing third party resources, an appropriate Non-Disclosure Agreement (NDA) should be in place, a template of which is available on the Colart intranet.

Hardware and Software

Software

Authorised Software

Only approved software may be loaded onto the Company's computers and networks. The Company will provide for all staff the software that is required.

If an employee requires additional software to carry out their job, then they should bring the matter to the attention of their line manager. If the line manager approves the request it should then be passed to the IT department. The IT department will evaluate the request, and respond to the line manager following the evaluation, informing of price implications and if alternatives exists.

Approval from Group IT will be required before any purchase. Specialist software would be charged to the department of use. Under usual circumstances, the IT department would carry out installation of all software and hardware. It may be appropriate under some circumstances for software or an "App" to be installed directly by the user themselves. But please verify this with IT before proceeding with any installation.

Colart's corporate browser for general internet and intranet use is **Google Chrome**. This should remain at all times your default browser. Other browser clients such as Firefox, Microsoft Edge or Safari maybe installed, but should not be set as default, as this can interrupt operation of other corporate systems.

The IT Department will maintain an inventory of all software installed on the company's computers and keep the master disks, downloaded installation files and manuals in a secure place.

The IT department will be responsible for administration of licences, maintenance contracts and warranties.

Unauthorised Software

The IT department may check any PC's for unauthorised software. Unauthorised software will be deleted, the employee's line manager and the IT management informed and appropriate action taken when relevant.

If an employee detects unauthorised software or activity on their PC then the IT department should be immediately informed and steps will be taken to remove it and/or safeguard the relevant equipment.

Having unauthorised software on a Company PC or laptop is a disciplinary offence.

The use of software that has not been purchased or licenced is 'piracy' and is illegal. The copying and installing software licenced to the Company on a private PC for personal use is a disciplinary and potentially a criminal offence. If in any doubt about your actions, please liaise with your IT department for advice.

By using only approved software, installed by the IT department, we reduce the risks associated with non-approved software.

Hardware

The IT department will purchase all computers, mobile devices, network equipment, and peripherals for the business, and will allocate appropriate equipment to allow staff to complete their duties. This will ensure that:

- we have a consistent set of equipment within the business;
- investments are cost effective;
- we obtain the best possible prices;
- funded in the most appropriate way;
- equipment is compatible, where necessary;
- it is properly licenced;
- appropriate maintenance and warranty is in place, and
- it is properly installed and configured.

The IT Department will maintain an inventory of all computer and mobile devices which indicates to whom the equipment is assigned. All additions and modifications to computer hardware and or mobile device must be authorised by the IT Department.

No (non mobile) hardware may be removed from the facility without prior permission. No equipment should be moved unless the IT Department is notified. This excludes mobile equipment such as laptops, tablets and mobile devices.

Use of your own equipment is allowed subject to approval by your line manager and the IT department. You won't be able to access internal network resources. However, you will be able to use Office 365 applications together with OneDrive and access the Internet and Intranet. Corporate data should not be downloaded or kept on a personal device. It can now be viewed, accessed and updated in cloud services to which we subscribe.

Third Party IT equipment

Non-Colart staff, such as those employed by 3rd parties, freelancers and contractors, using their own PC's, are responsible for their own hardware and software inclusive of licence and maintenance agreements. These PC's may not be connected to the Colart network unless explicit authorisation has been obtained from the IT Department.

Gaining access to the Internet via Colart provided guest Wi-Fi is permissible without prior arrangements with IT.

Consumables

All consumables for IT equipment (memory sticks and cards, ink and toner cartridges) are purchased centrally and are available from stationery stores or our recommended suppliers. Staff should not purchase supplies from unauthorised sources, or keep stock of such supplies. If there is an urgent requirement, please liaise with IT before proceeding with a purchase to ensure sensible, correct and compatible purchases.

Travel, Off-Site Use and Equipment moves

Appropriate approval from the IT department should be sought before taking any PC or related equipment off-site. Generally, users are not permitted to move IT equipment from site or within offices, as if not done correctly could cause damage, or equipment may not operate correctly if moved. Before attempting any such move, please contact the IT team for advice and support where necessary.

This section applies to non-mobile IT equipment only. Laptops, tablets, mobiles, mobile projectors and other mobile equipment is purchased to be mobile. There is no need to obtain permission to move such equipment around. Please just be careful with the equipment and use in accordance with manufacturers guidelines.

Security

Virus protection

Viruses are malicious programs that can cause serious costly damage to Company computers. They are frequently hidden within other programs that may be presented as 'freeware', 'shareware', games etc. Some also reside within MS Office documents. Files received via the Internet should be regarded as high risk.

Virus Checking

All files accessed on Company PC's are automatically scanned for viruses and suspicious software using Cisco AMP. All virus scanning is controlled centrally by Colart IT. Any attempt to remove such software is a dismissible act.

Firewall

The Internet firewall prevents intrusions to the Colart Wide-Area Network.

Web filtering and Monitoring:

We use Cisco Umbrella to monitor web browsing activity and prevent access to sites containing inappropriate or dangerous content.

Accessing Personal Email

Personal email access is allowed via the web – but please do not download any files from that email as that is a way of introducing un-monitored files into the organisation. This access could be revoked if at any stage we believe this threat is too great a risk to the business, so please support us in using this privilege wisely.

Downloading Software

Employees with Internet access should never download software to install from un-known or unauthorised sources. Software should only ever be installed with guidance from the IT team.

Detected Viruses

If an employee detects a virus or unusual activity on their PC then this ***must*** be reported to the IT Department immediately. The IT department has the right to remove the infected device from the company network for investigation until such time that the device is found to be safe. The IT department cannot guarantee the recovery of infected files. The employee may be required to assist the IT Department in tracking the source of the virus. Where an employee has sent files out of the business they may be required to advise contacts that a virus has been discovered and the external contact should check any of their own equipment that may be affected.

Downloading / Bit Torrents / Peer Sharing

These tools are used to enable the downloading of digital assets (such as software, audio or visual files). Often the material is illegally sourced copyrighted material. The use of Bit Torrent, Peer to Peer sharing tools and 'sharing' websites using company computer equipment in order to download illegal or pirated content is not acceptable or permissible under any circumstances. These activities may be illegal and present a serious security and virus risk to our corporate network.

If you are in any doubt about your actions in this area, please contact the IT team for guidance.

Tor Network

The TOR network is part of the internet where users can access unindexed web content anonymously through special web browsers like TOR. Although the TOR network itself is legal, many of the activities on the TOR network are illegal.

The act of installing a TOR browser and accessing the TOR network is not permitted under any circumstances. This activity may result in viruses or malware being passed onto your computer, also putting confidential company data at risk.

Access Control

User ID's

Under usual circumstances, only one network user ID will be allocated per person. The password associated with your unique ID should be kept secret, and should not be passed on to anyone else for their use. This is ***your*** electronic finger print on any actions that take place on the company's network and resources.

Where possible, the same format will be used for individual application sign on IDs. Wherever possible 'single sign on' will be used to gain access to company systems and resources (this means to use your authenticated network ID to gain access to other resources – e.g. Office 365, The Intranet, Emperform, M3).

It will sometimes be necessary to issue specific system usernames and passwords in addition to your network credentials. These should be treated with the same regard as your network ID.

No employee may use another employee's password or User ID. Use of another employee's user ID, ***even with their consent***, is in contradiction to the guidelines of the Global IT Policy, and may lead to disciplinary procedures for the person who failed to keep their password secret, or who used another user's credentials.

Passwords

User's network passwords will expire after a period of ninety (90) days when the system will prompt users to enter a new password. The password should not be easily guessed or identifiable. It is good practice and enforced, that any password contains at least eight characters, with at least one capital letter and one number and a symbol (for example: MarsBar86$). Passwords should not be re-used within a period of one year. The system will keep a password history preventing any attempt to re-use an earlier password.

Automatic lockout will be enforced after 5 invalid login attempts. Password reset will then only be enabled by the IT team.

This policy will be reviewed periodically, and if updated will be communicated to all relevant users.

Be aware that your password when changed maybe required to be updated in multiple locations. Including your PC, your phone (email), your browser sessions for access to cloud resources.

Setting up New Users

The IT team are responsible for setting up, changing and the disabling of all network users ID's within the Company. 10 days' notice is required for a new user, or a leaver, to be attended to in a timely fashion. The active users list will be double checked with HR periodically, to ensure

that all active users are current employees, but this is a backup check only, not how IT should be notified!

Please take care to be accurate, when notifying IT of new user details as changes to names and spellings can be problematic.

Authorised Signatories

All Department Managers are authorised to grant access to the Colart Network, and standard systems. This includes, but not limited to; Internet Access, public folders, an email account.

Access to specific systems is under the control of the relevant System Owner. The IT department cannot authorise access to any system without permission granted by the nominated system owner(s). In the absence of the nominated System Owner, authority would lie with a Site Director, or any GLT member. It is possible for system owners to appoint other alternative contacts who have the rights to grant permission to specific systems. The IT department will retain a list of systems and the persons authorised to grant access to them.

New Starters

IT services for new starters, or changes for existing employees needing new facilities should be requested by the relevant manager who has appropriate authority.

All new user, mobile, software and hardware requests must be done by the requester using the servicedesk portal which can be access at https://techsupport.colart.com/ . This ensures that all requests are correctly logged and visible by the IT team.

All users will be set up with access to Microsoft Office (Word, Excel, PowerPoint, and Outlook) software. In order to access other software, completion of the software requisition form will be required, outlining the requirement and justification, and returned to IT department via the servicedesk as above.

OneDrive cloud storage which will be integrated to your PC, and available on multiple devices, including your mobile and tablets and should be used to store work related files and documents.. See the mobile section for full details.

IT department staff will discuss use of the computer system with all new starters during their induction to the business.

Changes to Existing User Accounts

When a member of staff changes job role, especially when they change department, their line manager must review the system access required for the new position. These should be requested as for new starters. However, in addition, the line manager must remember to ask for facilities no longer needed to be disabled.

Service Level

The set-up of a standard new user account and changes to an existing account will normally be completed within **10 working days** from receipt of correctly completed requests by the IT department. If the 10 days is not enough, then the line manager will be informed by the IT department.

Access to specific IT systems in addition to the standard office suite may take additional time depending upon the system to be accessed.

Leavers

Leavers need to be advised on a monthly basis to the IT Department by the Human Resources department. If immediate action is required (e.g. there are security issues), then the person's line manager should ask the IT Department to immediately disable the user's access rights on the network.

Leavers' user ID's will be deactivated and files will be archived as soon as the IT Department receives notification from Human Resources.

Privileged Accounts for the use of changing System Data

On occasion it may be necessary for a member of the IT team to update data on behalf of the users in one of the back office or ERP systems (M3). It maybe that a status flag is preventing an order being processed or an account needs unlocking. If Data needs to be updated then the following procedure should be followed:

1. A request from a user should generate a servicedesk ticket with a reference for the request
2. The task should be assigned to an appropriate member of the IT team.
3. If line manager approval is required from the requesting team, or from the manager responsible for that area of the system is required, this should be sort as an email and logged with the ticket.
4. If specific privileged accounts exist for this purpose they should be used. If a member of the IT team is to use their own account this should be logged in the ticket.
5. The update can be made, verified with the users and then the ticket closed.

If privileged accounts are in place that are able to update the systems on behalf of the users in the ways indicated, we should be able to produce a report on request of the actions that the accounts have been used for.

Tickets that raised should be classified under their system name with a sub category of "Data Maintenance"

Server Room and Comms Cabinet Access Policy

The purpose of this policy is to define standards, procedures, and restrictions for accessing Colart International Holdings Limited internal server room and comms cabinets(s).

The overriding goal of this policy is to reduce operating risk. The Colart International Holdings Limited Server Room Access Policy will:

- Regulate human traffic into the facility which tends to open up security vulnerabilities or cause server outages.
- Protect corporate data, networks, and databases from unauthorised use and/or malicious attack.

Therefore, all access to server rooms and comms cabinets owned and/or operated by Colart International Holdings Limited must be controlled, monitored and conducted in a manner that adheres to company-defined processes for doing so.

This policy is complementary to any previously-implemented policies dealing specifically with security and network access to the enterprise network.

A ticket should be created within the service desk ticketing system for entry to server/comms room to ensure correct record and visibility of entry in case of any issues/security concerns.

This policy applies to all Colart International Holdings Limited company-owned, company-operated, or company-controlled servers. The designation or creation of new server rooms within corporate facilities will be managed at the sole discretion of the IT department. Non-sanctioned access, or use of server rooms, is strictly forbidden.

Responsibilities

The Chief Financial Officer of Colart International Holdings Limited has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

The Chief Financial Controller of Colart International Holdings Limited has delegated the execution and maintenance of IT and Information Systems (IS) to the Chief Technology and Digital Officer (CTDO).

Other IT and IS staff under the direction of the CTDO are responsible for specific procedures and policies within IT.

Policy Details

It is the responsibility of any employee of Colart International Holdings Limited who is accessing the server room or comms cabinet to protect Colart International Holdings Limited's technology-based resources (such as corporate data, computer systems, networks or databases) from unauthorised use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Based on this, the following rules must be observed:

Levels of Access

1. Authorised access

The server rooms and comms cabinets are physically secured by either a pin coded lock, padlock or a standard door lock.

Server rooms where possible are monitored 24 hours a day, 7 days a week by building Security. Server Room access is available to the server room on a 24x7 basis for authorised employees. A listing of currently authorised staff can be found in section **Server Room and Comms Cabinet Access List**.

1. All staff included in **Server Room and Comms Cabinet Access List** have been authorised for access based on job related needs. The need for authorisation will be reviewed no less than annually.
2. Entry into the server room by 'tailgating' other staff is strictly forbidden.
3. Staff must report all security or health and safety incidents to the Health and Safety Officer immediately.
4. Staff will accompany visitors in the server room at all times.
5. Staff are expected to challenge any unescorted visitors within the server room.

2. Vendor access

A listing of currently approved vendors can be found in **Approved Vendor Access List**.

1. All vendors included in **Approved Vendor Access List** have been authorised for access based on job related need. The need for continued authorisation will be review by Group Infrastructure Manager no less than quarterly.
2. Vendors with approved access to the server room are required to identify themselves to a member of the Server Room Access List and sign in/out of the server room using the Site Access Log.
3. Entry into the server room by 'tailgating' others is strictly forbidden.
4. Vendors are expected to report any security or health and safety incidents to the Health and Safety Officer immediately.

3. Visitor/Guest access

In general, casual visits or tours of the server room are not allowed. However, approval of a tour or casual visit may be granted. Requests for a visit or tour of the server room should be directed to the Group Infrastructure Director or the site IT Manager.

1. Visitors are required to identify themselves to the Group Infrastructure Director or the site IT Manager and sign in/out of the server room using the Site Access Log.
2. While onsite visitors must be escorted at all times.
3. All visitors will be made aware of this policy. It is the responsibility of the staff member accompanying the visitor to ensure their conduct conforms to this policy.

Conduct in the Server Room

In order to maintain a safe and secure environment, it is mandatory for all persons working within and visiting the server room to adhere to the following rules:

1. No food or drink is allowed within the server room.
2. No Hazardous materials are allowed within the server room.
3. No cleaning supplies are allowed within the server room without prior approval.
4. No cutting, grinding, or whittling of any material (pipes, floor tiles, etc.) can be performed inside the server room unless special arrangements have been made.
5. Only authorised staff shall access the sub-floor or remove floor tile.
6. All packing material (cardboard, paper, plastic, wood, styrene, etc.) must be removed from equipment in the staging area before being moved into the server room.
7. Staff and visitors must wear identification badge at all times.
8. All persons are expected to report any security or health and safety incidents to the Health and Safety Officer immediately.
9. No person shall connect any equipment, network/wireless devices, or monitoring tools without permission or specific Change Control authorisation.
10. Server or comms rooms are NOT storage facilities and should not be used as such.
11. Regular checks of the state and condition of the server rooms should be carried out by local IT staff, and maybe checked at any time by the Head of Infrastructure or Group IT Director to ensure that standards are maintained (cabling, power, temperature, cleanliness).

Monitoring and Audit

The server room access is controlled and monitored by various sub-systems (reader door lock system, video surveillance cameras, etc.) which produce access records. All server room access records are subject to the following rules:

1. Access records will be monitored by Group Infrastructure Director, unauthorised access and access which is inconsistent with staff schedules will be investigated and appropriate action taken.
2. Access records produced by the reader door lock system will be maintained for 1 year.

Server Room and Comms Cabinet Access List

The staffs listed below are currently authorised for access based on job related need. The need for authorisation will be reviewed no less than annually.

Table 1. Server Room Access List

Employee Name	Title/Position	Location	Access Level
Stuart Cooney	Director of Infrastructure	Head Office	24x7
Sanjay Marwaha	Director of Systems	Head Office	24x7
Dam Russak	Head of Service Desk		
Jevgenij Fiodorov	Principal Infrastructure Specialist	Head Office	24x7
Andrew Field	Principal Infrastructure Specialist	Head Office	24x7
Elliott Maguire	Service Desk Specialist	Head Office	24x7
Jean Francois Emery	Senior ERP Specialist	Le Mans	24x7
Hicham Sellami	ERP Specialist	Le Mans	24x7
David Quantin	Service Desk Specialist	Le Mans	24x7
Jean Marc Petitprez	Maintenance Manager	Le Mans	24x7
Eric Villanueva	Senior Service Desk Specialist	Piscataway	24x7
Ammar Ibrahim	Service Desk Specialist	Piscataway	24x7
Charles Liu	IT Manager China	Tianjin	24x7

Approved Vendor Access List

The vendors listed below are currently authorised for access based on job related need. The need for authorisation will be reviewed no less than quarterly.

Table 2. Approved Vendor Access List

Vendor Name	Company	Access Level
SPI	SPI	24x7

Non-Compliance

The CD3O will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

Restoration of Data Files

Files maliciously or accidentally deleted can be restored from back-up providing they were stored on the network and the IT Department is asked to retrieve them before the medium is re-used. The back-ups are on a rolling 14-day cycle, with a monthly save kept for a year. These monthly backups are point in time backups.

The request to restore a file should be made in writing or e-mail by the owner of the file or their line manager.

Under some circumstances files or folders may not be able to be restored such as data corruption, damage caused by virus.

Temporary or Contract Staff

In the case of Temporary or Contract staff at the time they are appointed their leaving date will also be required. At this date their user access will be disabled. Extensions to the leaving date should be requested in advance by the line manager. If the leaving date is unknown at the time of appointment, it will be assumed to be a monthly contract and will be disabled after one month.

A departmental generic account can be created (e.g. HR_TEMP, COMMERCIAL_TEMP) to allow for short term holiday cover or short term engagements that require systems access for ease of set up. However for longer term contract employees and contracts a named account is best practice. Even short term contracts for users with access to business systems (M3) should be named, so that their actions are identifiable and auditable.

Depending on the role that the temp or contractor is employed for it may be appropriate to lock down access to particular websites such as social media, job sites, holiday website or other internet based distractions.

File / Software Access

If an employee needs access to another member of staff's files or to software to perform tasks for an absent employee then the request to provide access should be made in writing by the 'donor' employee's line manager, a director or a relevant controller. This memo should be addressed to the Group Infrastructure Manager.

Preferably, files to which other members of the team need access should be saved in a public area of the network, either on a department work area or in a global drive for the whole business to access. Contact the IT department for advice on how to do this.

Reconciliation

The IT department will reconcile active user accounts with Human Resources records on a quarterly basis. The purpose is to ensure that all live accounts have an active person working within the organisation.

Network Security

Staff must ensure they lock PCs and log out of any software that it is required to do so. The best practice at the end of the day is to shut your PC down completely, to conserve power, and to ensure it goes through the appropriate start up sequence on a new day, when updates or settings may need to be applied.

Users should also lock or log off the network when PC's are left unattended.

Please note that files on users' PC's and laptops are not being backed-up it is your responsibility to ensure its security, and availability. Make use of network shares, SharePoint, and OneDrive to ensure your vital data is kept securely.

Mobile PC users are responsible for making their own backups using the network when they connect.

When a PC is temporarily not in use it should be set to 'Locked' by pressing CTRL + ALT + DEL and selecting the button to 'Lock this Computer'.

Mobile Device Security

Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the organisation and their use is supported to achieve business goals. This Policy is about using these devices to the advantage of you, and Colart, but ensuring we don't take any risks that might be damaging to us. This is an important part of Colart being a sustainable company.

Mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

Colart has a requirement to protect its information assets in order to safeguard the organisation's intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

Key Points of this Policy:

- We use a platform to central manage and audit company mobile devices.
- Look after your Colart devices, don't smash it up! They are expensive to buy, repair and replace.
- If you lose it tell us straight away, so we can prevent information being lost.
- Don't get an android device they are not secure enough for us!
- Don't jailbreak, install dodgy software, download illegal content to any of your work devices.
- Buy your own personal games, apps, pokaballs, coins, gems, potions, don't charge it to Colart.

Scope

- All mobile devices, whether owned by Colart or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers.

- Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorised by IT and a line manager.

Policy

Technical Requirements

- Devices must use the following Operating Systems: Android 6 onwards or IOS 7.x onwards
- Devices must be installed with the Snow mobile device management profile. This will be done by IT when given a new or replacement device. Users can also install the management profile for devices themselves, guidance is found on the Colart Intranet here: Snow Mobile Device Manager User Guide
- Devices must be configured with a secure password that complies with Colart's passcode policy (6 characters for mobile devices). This password must not be the same as any other credentials used within the organisation. As part of the Snow security profile this policy will be mandatorily pushed out to mobile devices when the profile is installed.
- Colart IT have the right to view (via the administration portal) any apps that are installed on the device.
- With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network and Colart email. Any devices that are not installed with the Snow security profile are subject to being blocked.

User Requirements

- Users must only load data essential to their role onto their mobile device(s).
- Users must report all lost or stolen devices to Colart IT immediately.
- If a user suspects that unauthorized access to company data has taken place via a mobile device the user must report the incident to Colart IT and their line manager immediately.
- Devices must not be "jailbroken"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- Users must not load pirated software or illegal content onto their devices.
- Applications must only be installed from official platform-owner approved sources (The official App Stores). Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact Colart IT.
- Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy. So don't connect it to a home computer with no anti virus protection.
- Users are to use their own app store credentials for the purchase and installation of software on the mobile device. If you need an application for work purposes, IT can get it for you or with prior agreement, buy it, and claim any legitimate costs back through expenses.
- Users may must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Colart IT immediately.

- It is possible to set up your phone so that company mail goes into the outlook or apple mail app, with personal email segregated into another app such as the gmail app, yahoo etc... which would keep the two worlds apart.
- Once a mobile device is returned to the organization, the users own app store account should be correctly removed.
- Any damage to the device by the user is the users own responsibility and such any expense occurred should be held by the user or their department.
- In the event of damage or fault, if an iOS device an appointment should be arranged with the Apple Store by the user to provide a fix if local IT are unable to resolve the issue.

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

Software Application Use

Email Policy

Colart aims to use e-mail to its full potential. It should be used, where possible, for all types of formal communication, both internally and externally.

It is recommended that the application is left active and set to notify you of the arrival of new mail.

Rules for the Use of E-Mail

It is extremely important that care is taken to ensure that e-mail does not bring Colart into disrepute.

The following are not permitted:

Making personal comment outside Colart unless it is clear from the e-mail that it does not represent the views of the Company.

Sending unauthorised formal messages outside the Company. It is the employee's responsibility to ensure that he or she is authorised to send the message to an external Company before it is sent.

Sending confidential or commercially sensitive information externally unless this has been explicitly authorised.

Making any slanderous or derogatory comments which may result in legal action against or embarrassment to, Colart or its employees.

Sending messages that infringe copyright or other property rights.

Producing, introducing or forwarding "chain letters" even if they appear to be innocuous such as charitable appeals or virus warnings.

Sending multiple mail messages to a destination or to a group of destinations with the objective of causing disruption or a system failure.

Registering a Company e-mail account on an external mailing list for receipt of e-mail (other than for business purposes).

Using distribution lists set up for Company use for personal mail.

Sending material that could offend others because of its nature or content.

The E-mail system is regularly monitored. Abuse of the system will be reported to the Human Resources department and your line manager.

Screening of Messages

The IT department will use systems to screen incoming messages. Messages that contain profane language or Computer viruses will be returned to the sender. By signing the declaration at the end of this document you agree to allow the Company to review the content of E-mail that you have sent and received using the Company's E-mail system.

Internet Usage

Colart Group Internet Access Policy

Colart aims to use appropriate business technology to its full potential. Hence Internet access is provided to staff determined by business need.

Rules governing use of the Internet

A number of categories of sites are blocked at the web and email filtering, as they are considered unsuitable for business use. Access to these categories will be denied and the attempt to access will be recorded.

Staff making use of Internet access must avoid using the Internet to engage in activities that are illegal, that might harm the Company's reputation or that might otherwise violate other Company policies. Employees may not use the Internet to engage in activities such as:-

- Adult Material / lEntertainment
- Pornography
- Illegal Drugs
- Gambling
- Militancy or Extremism
- Racism and Hate
- Tasteless
- Hacking
- Weapons
- Violence

Sites that are described and tagged as above will be blocked, but not all sites will be tagged. So this policy explicitly lists these activities, meaning the employee is accountable, as the web filtering won't be 100% at filtering all such sites.

Websites and internet resources are categorised by external agencies, for use in industry standard web filtering software. It is NOT based on the opinion of the IT department. Specific sites that are required for genuine business need, that may have been filtered due to such categorisations, can be made allowable on request to the IT team.

Transferring files

Do not register to use these services for company business. We have no formal way of using these in a corporate fashion, and data that might be stored in the Cloud on a Google app or similar service may be lost to the company in the event of staff leaving etc... this includes:

- Google drive
- Dropbox
- The box
- And other numerous and emerging others!

Our corporate standards for the transmission of larger files that won't go through on email is FTP, and corporate cloud services like SharePoint and OneDrive.

For the best corporate use, please stick to the standard tools provided.

IT resource usage

Personal use of company equipment

It is recognised that employees may occasionally make use of Company computer facilities for personal use. It IS acceptable that employees install applications such as iTunes to manage a mobile device. Employees may have a 'sensible' amount of music or video content for synchronising with their iPhone, or for their use while travelling, stored on their PC or laptop, NOT on the company Network. Storage of personal photo's or back ups of photos from mobile devices, that might include some personal photography is permissible on the individuals PC or Laptop. However the Laptop or PC remains the property of Colart, and has been provided for work purposes. This is its primary purpose, and any personal files are of secondary importance to the work use of this equipment.

Colart do not expect to have 'excessive' amounts of personal data stored on the Laptop or PC equipment. And no provision for additional storage will be made in order to accommodate excessive personal data.

The use of network shares and devices for the storage of personal music, video or photographs is not permitted. Any infringement of this policy, and your personal data is at risk of being deleted.

Use of privately owner systems for company business

Where an employee uses their own computer in order to fulfil their duties this is at their own risk. If they need tools we [Colart] should provide them. If you choose to use your own then you agree this is at your own risk. All liabilities and costs will remain with the employee. The company may make a contribution, at the discretion of the employee's line manager & or budget holders, to costs of stationery and consumables where this is exceptional. The department and line management in question is responsible for ensuring that company data is not at risk. This includes documents and data produced by this employee on a personal computer, the Department or line manager must ensure that copies of any required information is also stored in a company location, as we will have no access to personal computers to recover this.

Employees are advised that the Company's software may not be installed on Privately Owned IT even if it is intended that it will only be used for Company Business. If software is required the contractor should purchase it themselves, so it is licensed to their business, and invoice us if agreed that Colart will reimburse the 3rd party. This requires agreement ahead of the purchase.

IT support

If you need assistance in operating your PC, if it develops a fault or fails in any other way please open a ticket using the service desk portal https://techsupport.colart.com/

Calls are prioritised based on business criteria. Hence, if your issue is more significant than it may appear please make it clear so that it can be scheduled accordingly. Equally, if a problem can wait please inform the service desk as well. IT will aim to respond appropriately to all requests made. Some calls will of course be dealt with as higher priorities, and those that can be dealt with at a later date will be agreed with the individual caller.

Standard hours for IT support are 9am to 5pm for the teams location.

Security

All corporate data and files are the property of the Company and as such should be stored on network drives or (in the case of laptop users) regular copies made either on to a network or appropriate corporate cloud locations.

When using your PC it is recommended that you create your own folders to keep your work organised. These folders and their contents can have detailed names.

In addition, most of the applications allow you to save document information or a 'preview' picture.

Care of equipment

Your PC and attached equipment should be switched off overnight and at weekends.

Contract cleaners clean all electronic office equipment on a regular basis. You may periodically clean your screen with a soft cloth and a suitable cleaning agent. Screen filters should be wiped with a soft cloth occasionally.

Keep drinks and food away from your computer. Beware of knocking cups when moving your mouse! If you spill anything into any part of your PC do not touch it. Call for help from your local IT Support at once. Please tell support staff what has happened, not that it has just "stopped working."

Do not attempt to repair your PC or any other IT equipment yourself, or via a local support company, or your friend "who is good with computers" without the prior approval of the IT department. If it needs service then a member of the IT Support team will attend to it, or get the appropriate support services for you.

Usage environment

PC's and other computer equipment should be kept in a ventilated location to dissipate heat generated by the machine. The screen should not be used in an area where direct sunlight falls upon it.

Closed laptops may resemble tea trays, but they are not. Do not place a hot cups on its closed lid. It can often cause damage.

Health and safety

Cables should be positioned to avoid trip hazards. Take regular breaks, sit in a suitable chair, and use suitable foot and other rests if required.

Printing

Colart operate a policy of not printing documents unless business critical and we only provide a limited printing capability as a result.

By default new starters PCs will not having printing enabled. In order to gain access to printers please open a ticket in the service desk and subject to your line managers approval printing capabilities will be added.

With multi-tray printers, one tray may be designated for use with A4 paper and a second for A3 paper.

Printers should be operated in a ventilated area. Small quantities of carbon dioxide and ozone are produced during operation. This does not pose a hazard to health.

Additional guidelines for laptop users

Do not leave your laptop unattended in an unlocked car.

Do not leave your laptop open to view in your car. If you put it in the boot before leaving the car do this in a secure place where you are not observed.

Do not leave your laptop in your car during periods of very hot or very cold weather.

Make sure the carry case is zipped shut before moving it.

If you are travelling in a high-risk area do not use an obvious PC carry case.

Take regular backups of your data. If you want advice or help with this, please contact the IT team.

Sustainability

Introduction

The policy of Colart is to be carbon neutral by 2030 and we recognise the formidable challenge this presents to the business and its use of technology platforms. We are committed to achieving this goal and as such are setting down policies that will allow us to achieve this.

Our approach is as follows:

- Maximize the amount of renewable energy we use and minimize overall energy usage.
- Minimize the purchase of new equipment and maximize the life span of existing equipment through repair and reuse.
- Maximize our use of technology to identify and implement sustainability change throughout the business.
- Minimize the usage of all consumable items.

Energy usage

- We will strive to build full accounting of energy usage from IT equipment and will progressively seek to improve the granularity of our accounting to ensure complete visibility.
- Where possible exists we will only renewable energy sources for powering our cloud, server, infrastructure and desktop equipment.
- From 2023, we will carbon offset any energy usage from non-renewable sources.
- We will minimize the overall energy usage of technology platforms by identifying opportunities reduce by:
    - Decommissioning equipment where power used exceeds the impact of replacement.
    - Turning off equipment when it is not needed
    - Optimizing the use of air-conditioning of equipment so its impact is minimized.

Reuse and repair

- As far as it practical all IT equipment will be repaired and reused to minimize the environmental impact.

Equipment end-of-life

- When equipment has reach end of life where appropriate it will be donated to schools/charities.
- For equipment that cannot be donated we will ensure it is properly disposed of and recycled where possible.

Consumable usage

- We will work to minimize the usage of consumables.
- Access to printers will be minimized and on a strict need basis.