DEWHIRST
EST.1880

IT User Policy

Policy Statement:
Dewhirst regards the integrity of its information technology and systems as central to the success of the business. Users must accept that their access to systems and ability to work outside of business premises may be restricted in order to ensure that the Corporate network is not exposed to risk or attack. This policy informs users of their responsibilities regarding data integrity, disclosure of information and compliance with appropriate legislation. The policy applies to all personnel with the facility to access Dewhirst IT systems.

Any user suspecting a security breach or misuse of company data should report this to local IT Management and Site Directors immediately. All incidents will be logged and investigated.

1 Client PC Physical & Environmental Security

Physical Access to Client Devices:

- Only PC's owned by or authorised for use by Dewhirst should be connected to the Dewhirst network.
  - Devices owned by users are not allowed to be connected to the Dewhirst Network.
    (Note: Users home devices can be used to remotely access Web based systems such as office 365 and Users Smartphones can be authorised to access the internet via Dewhirst networks with approval from site directors)
  - Visitors requiring access to the internet can be provided with guest wi-fi access, but their PC should in no way be attached to the Dewhirst network.
- Rooms containing Dewhirst computers should be locked at all times when the room is unattended.
- Visitors should not be left unaccompanied in areas where computer equipment is present.
- Users should not attempt to move or open or modify in any way the inside of computer equipment.
- Users should lock their computer screen if leaving them for more than 5 minutes (This happens automatically after 15 minutes)

PC/Laptop Computers / Company iPhone:

- Company PC's, Laptops and iPhone must be made available for IT staff to examine the contents if management deem this necessary.
- Users must never download or install software without the specific prior agreement of their IT manager.
- Laptops should be transported in appropriate carry cases to minimise risk of damage.
- Users should take all practical measures to reduce the risk of laptop / iPhone theft whilst the laptop is not on company property; this should include:
  - Placing the Laptop / iPhone out of site e.g. in the boot of a car.
  - Accompany the laptop when flying (never check in as hold luggage).
- When an employee leaves the company, they must return any laptop, mobile phone or other device which has been provided by the company.

2 Data Security

Privileges

- IT equipment is provided to users for business purposes. Limited personal use is allowed but this must not in any way hinder business work.

IT User Policy

PC Desktop & Laptop Data

- When using a Laptop or Desktop PC, all user data should be saved to the users OneDrive, SharePoint or local server shared drives.
- Data on Desktop PC and laptop Local Disks is not be backed up.
- Data saved to local drives (usually C: and D:) will not be backed up by Dewhirst and maybe lost if the computer fails, is stolen or is replaced. Therefore, it is the employee's responsibility to store all work related data on the personal OneDrive, SharePoint or Network shared Drives
- Dewhirst IT 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
- Laptops must not be left on top of the desk unattended overnight but must be locked in a desk draw out of sight.

Accessing Dewhirst Data via Office365 portal on non-Dewhirst Equipment.

- Dewhirst provide office 365 licences for all IT users; this enables them to access Dewhirst Emails / Data etc on any device connected to the internet. Whilst doing this user should ensure: -
  - They do not disclose any commercially sensitive or confidential information to any third parties.
  - After accessing Dewhirst data on non-Dewhirst devices, they log off and close any applications.

3 Access Control

System Access:

- PC's connected to the Dewhirst Network will lock the session after 15 minutes of inactivity and the user must enter their password to regain access to the PC.
- Lock your workstation (CTRL+ALT+DEL) when you are away from it.
- Users must close all applications and shut down their PC at least once a day to ensure all policy updates and security patches are applied.

Passwords:

- Staff must not share their password with anyone except IT staff, doing so may result in disciplinary action (IT may request it for setting up new equipment or troubleshooting issues)
- Staff must not use the User-id or password of any other staff member unless authorised by the Site Director in exceptional circumstances. (I.e someone has left or on holiday and we need access to emails from customers etc).
- User passwords to systems are granted for a limited 90 day period.
- If password changes in an application are not auto enforced, Staff must change them every 60 days.
- User passwords must meet the following rules
  - Must contain at least 7 characters
  - Must contain at least one Capital letter, one lower case letter, one number and one special character For example ! " # $ % & ' ( ) + , . : ; < = > ? @ [\ ] ^ _ ` { | } ~
  - Cannot be the same as any of your last 15 passwords
- For PC and Power 8 (as/400) access, you will have 3 attempts to enter a valid password, if you have not entered a valid password by then, your account will be locked out, it must be re-enabled by IT Staff.

Authorisation for System Users

- New Starters

When a staff member needs access to any systems or applications, a New Starters form should be completed by the local HR Dept and authorised by the site Director or General Manager and emailed to support@dewhirst.com

- Job Changes

When a staff member changes his/her job in a way which means they require different access to systems, the user's personnel department should notify the IT Manager by E-mail and a IT Access change form needs to be completed and emailed to support@dewhirst.com

- Leavers

When a staff member leaves the company, access to Dewhirst systems will be withdrawn with immediate effect. An Advanced Leavers form should be completed by the local HR Dept as soon as a leaving date is confirmed and authorised by the site Director or General Manager and emailed to support@dewhirst.com

4. Network Security

Email, Instant messaging & Anti-Virus

- Email and Instant messaging is not an informal communication tool. It carries the same authority as written communication
- Email and Instant messaging is primarily supplied for business purposes; personal use of Email and Instant messaging is allowed providing that it does not affect any Dewhirst employee's ability to perform their duties in the most effective and efficient manner.
- Users should try not to use the, 'reply all' function as this can be a way of unwittingly sharing information with hackers, make sure you only include people who need the information in the email.
- Dewhirst are not liable for any loss resulting from loss of personal confidential data, caused by the operation of any virus or anti malware security software resident on the PC being used.
- Statements made within Email and Instant messaging can give rise too personal or company liability. The user should be aware that Email and Instant messaging can be read by Third parties and can create binding contracts.
- All Internet e-mail both incoming and outgoing is checked for viruses.
- Users must never click on links in emails unless they are sure they are safe.
- Users must never open attachments in emails unless they are sure they are safe
- If a user has opened an attachment or clicked on a link that they then suspect is unsafe they should disconnect their device from the network and immediately inform IT.
- All Email and Instant messaging are copied to a journal. A condition of using Email and Instant messaging is that the user gives implied permission for Email and Instant messaging messages in the journal or in their mailbox to be inspected by IT staff. Dewhirst will ensure that this only occurs where system misuse or an Email and Instant messaging confidentiality breach is suspected and will only occur with the express permission of a Dewhirst Divisional Finance Director or Managing Director.
- Contents of Email and Instant messages not sent to, intended for or copied (inc cc and bcc) to a member of staff, must not be disclosed or forwarded by that person to any other staff within or outside the company.
- If a user suspects that his/her Laptop/PC has been infected by a virus or malware they should immediately disconnect from the network, shut down the PC and inform IT

- Users must never open email attachments from a sender who they do not know or trust. Hackers may try to mimic an email address of a known contact by creating a similar address. Users should ensure that any emails regarding monetary transactions are reviewed to ensure the sender if legitimate before replying.
- PC users should not use CD's, DVD's, memory cards or USB disks or Memory sticks. Any data to be copied to/from these devices should be by a member of IT who should scan for virus's while the device is off-WAN
- Laptop users are responsible for damage caused by loading local Media (CD's, DVD's and USB Memory Sticks etc.) into their PC. Viruses and malware may exist on such media. If this type of media must be loaded, users should ask the local IT department to check the media for the presence of viruses.

Connection of PC's to Dewhirst Network

Client PC's may connect to the Wide Area Network (WAN) in one of the following ways:

- By network cable to network connection point within a Dewhirst site
- By Wireless connection to a Wireless Access Point within a Dewhirst site.

Remote Access to the Dewhirst Network / Working from home or outside the office

- If a user requires access to purely office 365 applications and data, this is provided from any remote PC by using portal.office.com.
- Users should ensure any non-Dewhirst owned devices have up to date virus protection before logging into office 365
- Use of public devices should be avoided but if necessary, they must be from a trusted provider such as hotel business centre. During use of these devices you must never save any credentials and after use you must log off and close any browser sessions.
- Using VPN Remote Access system.
  Users needing remote access to JDE and users who infrequently work from a Dewhirst office will need to connect using the VPN. This is strictly controlled and reviewed quarterly, users no longer requiring VPN access will have this access removed.
- Only Dewhirst owned Laptops with VPN software should be used to gain full access to WAN services.

Access to the Internet

- Internet access is primarily supplied for business purposes; limited personal use of internet is allowed providing that it does not affect the user's ability to perform their duties in the most effective manner.
- Internet access will only be given to users who need it in order to perform their normal duties.
- Users must ensure that if downloading or copying the works of others, they do not infringe copyright. It is the user's responsibility to ensure that they do not access inappropriate Internet content, this is deemed to include any internet sites of the following types,
  - Adult, Explicit, War, Hate, Crime related, Terrorism,
  - Non-business related Audio downloads, Video downloads, or executable programs
- Social networking sites, messaging, file sharing other than for customer requirements.

- Web Filtering System Barred/Allowed access:
  Dewhirst use a Web Filtering system which will allow/restrict access as per the table below.
  Users who attempt to access any sites which have been categorised within these groups will have their access barred. If a user attempts to access a business-related site, and find they are unable to do so because of the existing categorisations, they should report this to their IT Manager.

- Details of Internet sites accessed or attempted to be accessed by each user are recorded. This information is available to management on request and may be used for disciplinary purposes.
- Dewhirst accept no responsibility for any losses resulting from personal or confidential information being entered or accessed, whilst accessing the Internet for personal use, via computers connected to the Dewhirst network.

	IT Staff	*Super Users*	*Std Users*	*Application Users*
Adult & Explicit sites	Barred	Barred	Barred	User Access given only to specific Job-Related sites.
War, Hate, Terrorism and Criminal	Barred	Barred	Barred	
IT Related sites	Allowed	Allowed	Barred	
Download of Audio, Video & Executable	Allowed	Barred	Barred	
All other unclassified business & general	Allowed	Allowed	Allowed	

5. Social Media

- Any website or social website created with the name relating to Dewhirst Group, any Dewhirst Division, Shanta Denims Limited, Shanta Industries Limited and Shanta Wash Works Limited has to be approved by Anthony Wood, CEO, DEWHIRST

- Without this permission Dewhirst has the right to remove any websites, or social media pages and will be duty bound to do this immediately with those that have been recently highlighted to the business.

- All employees are duty bound to refrain from involvement with unauthorised websites or social postings relating to the Dewhirst Group and are asked to be vigilant and report to the HR teams about the appearance of any such material on social media or the internet.

6. Sensitive Data changes

- Users must never change supplier or customer data without Finance director approval.
- Information such as Payment terms, bank account details etc must never be changed without Finance Director approval
- Users must take appropriate care to ensure sensitive company data is not shared with 3rd parties

7. Asset Classification, Control & Security – Hardware & Software Ownership

- All IT hardware and software used by Dewhirst employees must have adequate records to support its ownership.
- All software will either be the property of the software company with licensing given for Dewhirst to use this or developed internally by Dewhirst and all intellectual properties belong to Dewhirst.

Additions / Changes / Disposals

- IT equipment & software should only be purchased with the prior approval of the IT Manager.
- Only IT personnel are authorised to install software on computers
- Before any IT equipment is either disposed of, or permanently moved from one site to another, the local IT manager should be notified, in order to ensure the correct procedure for disposal and documentation is followed.

6. Disclosure

- IT staff and users, as part of their normal duties may have access to sensitive or confidential information; they should:
  - Be prepared to sign confidentiality clauses within their contracts.
  - Not share or sell information to any unauthorised personnel outside of the company. Or without the prior consent of the owner/creator of that information.
  - Comply in full with all appropriate laws e.g.UK Data Protection Act / GDPR etc.
  - Co-operate in providing information to external bodies (e.g. customs & excise) that are in the process of audits or investigations.

POLICY ACCEPTANCE

I HEREBY ACCEPT THE CONDITIONS OF THE DEWHIRST IT POLICY v10

Dewhirst Site		**Date**	
Employee Name		**Employee Signature**	