NEW LOOK

INFORMATION TECHNOLOGY SUPPLIER AND CONTRACTOR SECURITY POLICY

POLICY NUMBER	NL/POL/003
ISSUE DATE	15TH July 2024
VERSION NUMBER	4
TERRITORIES COVERED	All
APPLICABLE TO	Third Party Suppliers, Contractors, Freelancers and Consultants
POLICY OWNER	Chief Information Officer

1. Purpose

1.1. This Policy provides a framework for Supplier and Contractor, Freelancer, or Consultant (hereafter referred to as Contractor) responsibility within an Information Security context across New Look.

2. Scope

2.1. This policy applies to:

2.1.1. Any Supplier or Contractor required to access New Look's applications, systems or data for business purposes using IT equipment not provided by New Look.

2.1.2. All IT systems and devices that are not provided by New Look and need to access, or be attached to, New Look's computer or phone networks.

2.1.3. All information processed by New Look or the supplier relating to operational activities, whether it's processed electronically or in hard copy form.

2.1.4. Any communications sent to or from New Look and any information about the company held on third party or cloud systems external to New Look's network.

3. Responsibilities

3.1. All Suppliers, their employees and Contractors must make sure they follow this policy and complete any mandatory security training.

3.2. Suppliers are responsible for making sure their employees understand this policy and the consequences of not following it.

3.3. The Head of Information Security is responsible for making sure this policy is available to Suppliers and Contractors, and that it is reviewed regularly.

4. Core Policy

4.1. General Requirements

4.1.1. Access Control

4.1.1.1. Supplier and Contractor remote access to the New Look network is only permitted via private leased line or New Look approved encrypted VPN. Any new remote access approach must be approved by New Look.

4.1.1.2. No Supplier or Contractor owned device is permitted to connect to the internal Company Network without authorisation from:

i. Technical Services Group Manager; and

ii. Head of Information Security

or an appropriate officer designated by them.

4.1.1.3. Supplier or Contractor owned devices which need to be connected to the Company Network or to process New Look information must comply with the following requirements:

i. Anti-Virus or Endpoint Detection and Response (EDR), Firewall, and Internet Security software installed and running

ii. Updated signature files installed

iii. Latest security patches for the Operating System and applications installed

iv. The device's Hard disk is encrypted at disk level

v. Access to the device is secured via an authentication method which complies with New Look's Access Management Policy

vi. User Access is facilitated from a User ID provided by New Look IT Services

vii. User Access control is configured to limit access to only those areas which are required to perform the function

4.1.2. Compliance

4.1.2.1. Suppliers and Contractors must comply with the requirements of Article 32 of the General Data Protection Regulation 2016 (EU2016/679) relating to security of processing and with the appropriate requirements set out in the following extracts from the New Look Information Security Policy documents:

i. Information Security Policy (Appendix A)

ii. Access Management Policy (Appendix B)

iii. Backup and Recovery Policy (Appendix C)

iv. Personal Data Retention Policy (Appendix D)

v. IT Use Policy (Appendix E)

vi. Information Classification and Handling Policy (Appendix F)

4.1.2.2. Personal, non-enterprise email systems must not be used to process or transfer New Look personally identifiable information or corporate sensitive information. Approved solutions will be provided for this purpose.

4.1.2.3. Contractors who are provided access to the New Look email system will be provided with an email address in the format: firstname.surname@contractor.newlook.com.

4.1.3. Incident Management

4.1.3.1. Suppliers and Contractors shall ensure a security incident response procedure is in place and maintained.

4.1.3.2. All actual and suspected Information Security Incidents must be reported as soon as they are identified.

i. During store hours the New Look IT Help Desk should be contacted on +44 (0)1305 765544.

ii. Out of store hours, suppliers should contact the confidential hotline on +44 (0)800 0289075.

4.1.3.3. Suppliers and Contractors must provide New Look with any assistance required to implement remedial actions and restore New Look information and systems in the event of a security incident.

4.1.3.4. Suppliers must aid in any subsequent investigation, providing security logs, forensic details and any other evidence as required.

4.2. Supplier Requirements

4.2.1. Information Risk Management

4.2.1.1. Suppliers shall designate named individuals or teams who have responsibility and accountability for Information Security. These nominated persons will act as the point of contact for New Look Information Security matters.

4.2.1.2. Suppliers shall, at all times, maintain their own management-approved corporate Information Security Policy, or set of Information Security Policies, defining responsibilities and setting out the Suppliers approach to information security.

4.2.1.3. New Look retains the right to audit any Supplier against the security requirements contained within this policy and any other referenced New Look Information Security Policy.

4.2.1.4. Where a Supplier will process data on New Look's behalf, or will access New Look's systems and/or Network, they shall be required to complete a Supplier Security Questionnaire during the onboarding process.

4.2.2. Human Resources Security

4.2.2.1. Suppliers shall ensure that information security roles and responsibilities of all employees are clearly defined and documented.

4.2.2.2. Suppliers shall ensure that all employees have read, understood, and remain in compliance with this and all relevant New Look security policies and procedures.

4.2.2.3 Suppliers and Contractors must ensure they, or their employees, complete appropriate information security training at least annually. Where this is not provided, New Look will facilitate access to its learning platform so this can be completed.

4.2.2.3. Formal disciplinary procedures must be in place for employees and subcontractors who breach any applicable security policy related to the protection of New Look information and systems.

4.2.3. Information Handling

4.2.3.1. Suppliers shall ensure that an appropriate set of procedures for classifying and handling New Look information, aligned to the requirements of the New Look Information Classification and Handling Policy, are developed, and implemented.

4.2.4. Asset Management

4.2.4.1. All Supplier IT assets used to process New Look information must be recorded in a maintained inventory.

4.2.4.2. The Supplier shall ensure all New Look information is appropriately sanitised or destroyed in line with relevant data protection requirements, and any device or media used to store or process New Look information is securely disposed of, when no longer required.

4.2.4.3. Where a third-party is used to dispose of or recycle assets holding New Look information:

i. The third-party should be an ADISA certified company.

ii. A certificate of data destruction must be retained by the Supplier for each asset and available to New Look on request.

4.2.5. Physical Security

4.2.5.1. Suppliers shall ensure appropriate physical controls are in place to prevent unauthorised access to New Look information and systems including, but not limited to:

i. Physical access mechanisms

ii. Manned receptions

iii. Alarm systems (including appropriate environmental alarms)

iv. CCTV

4.2.5.2. Suppliers shall review the strength and effectiveness of the management of physical security controls at all sites on which New Look data is processed at least annually.

4.2.6. Technical Security Requirements

4.2.6.1. The supplier shall install and maintain a supported enterprise grade malware protection tool on all systems and devices which process New Look information and/or interact with New Look systems.

4.2.6.2. Encryption solutions shall be used where appropriate to secure all New Look information at rest and in transit. Suppliers must only use approved public encryption algorithms such as AES or RSA public key cryptography and SHA-256 or better for hashing.

4.2.6.3. Suppliers must ensure an appropriate patch management policy and procedure are in place to ensure security patches and fixes are applied to all systems processing New Look information in a timely manner.

4.2.6.4. Suppliers shall ensure that regular penetration testing is carried out by an approved third party against all network environments holding or processing New Look information. Suppliers are required to provide confirmation that this has taken place at least annually, notify New Look of the results of such testing, disclose any exceptions and take action on the recommendations in timescales commensurate with the associated risks.

4.2.7. Backup & Retention

4.2.7.1. Suppliers shall ensure that backups of all systems hosting New Look information are performed and scheduled at risk-based intervals.

4.2.7.2. Processes must be in place to ensure recovery from the loss or damage of New Look information, or systems used to process New Look information. These restoration processes must be tested at least annually and after any major changes.

4.2.7.3. Suppliers shall ensure that where backups are stored off-site they are encrypted and securely transported, and a written register maintained.

4.2.8. Access Control

4.2.8.1. All employees of a Supplier accessing the New Look network or systems containing New Look information must have an individual account with a unique user ID.

4.2.8.2. Suppliers shall have a technically enforced password policy that meets or exceeds the requirements of the New Look Password policy and New Look Privileged Password policy.

4.2.8.3. Supplier devices may only use the Network Connection for business purposes.

4.2.9. Software Escrow

4.2.9.1. New Look will ensure a copy of the source code of a software system is deposited with a third-party escrow agent whenever one or more of the following conditions are met:

i. The software is maintained by a supplier on behalf of New Look;

ii. The software is bespoke or has been customised to meet New Look requirements;

iii. The software forms part of a Business Critical service; or

iv. It is possible that the Supplier will cease development or support of the software before New Look decommissions the system.

4.2.9.2. Third party escrow agents must be approved by New Look and must sign a Non-disclosure Agreement (NDA) to ensure the confidentiality of any stored source code.

4.2.9.3. If a decision is made to not deposit application source code with a third party escrow agent, the justification for this action must be fully documented and approved by a relevant senior manager at Head-of level or above.

4.2.10. Compliance

4.2.10.1. Suppliers may be required to provide current evidence of compliance to the requirements of this policy via the Supplier Security Questionnaire at any time.

4.2.10.2. Where financial transactional functionality involving payment card information forms a part of the Supplier services, the Supplier will maintain all applicable PCI DSS requirements to the extent the Supplier handles, has access to, or otherwise stores, processes, or transmits customers cardholder data or sensitive authentication data, or manages customers cardholder data environment on behalf of a customer.

4.2.10.3. Suppliers will provide New Look with evidence of PCI-DSS compliance through external certification or self-assessment declaration before commencement of services and at least annually thereafter.

5. Enforcing the policy

5.1 This policy is enforced by IT Services where possible, using technical or automated controls.

5.2 If an application or device is provided that doesn't allow the user to follow this policy, an exception and risk will be agreed by senior management.

5.3 A deliberate breach or serious or persistent inadvertent breaches of this policy will be taken very seriously. Employees will be investigated under the company's disciplinary policy and procedure which could result in loss of privileges, suspension and disciplinary action including dismissal without notice.

5.4 3rd party suppliers, agencies and supplier representatives will be reviewed, and any breaches could result in the immediate termination of their assignment or relationship with New Look.

6. Reference Documents

Document Title	Location
PCI DSS Version 3.2	Buzz & Runway
Disciplinary Policy	
Disciplinary Procedure	
Security Incident Management Policy	
Access Management Policy	
GDPR Data Protection Policy	
GDPR Personal Data Breach Policy	
Information Security Policy	
Data Retention Policy	

7. Contacts

If you require more information about this Policy, the related reference documents or have any suggestions on how it can be improved, please email Information.Security@NewLook.com.

NEW LOOK

Appendix A: Information Security Policy Extract

A.1 It is the Information Security mission of New Look to protect the New Look Brand, business, customers, and its colleagues from reputational, financial, and other damage as a result of information theft, modification, disclosure, use or destruction or other breaches however caused by:

A.1.1 Implementing an Information Security Risk Management Strategy to mitigate and manage information security and cyber risks which impact upon New Look's information assets.

A.1.2 Facilitating an information security governance structure, including the formation of an information security steering committee.

A.1.3 Identifying, assessing, and addressing all vulnerabilities, issues and incidents which present a threat to the Confidentiality, Integrity, and Availability of New Look's information assets as defined below:

- Confidentiality: Ensuring New Look's information assets are accessed by only the right people.
- Integrity: Ensuring information assets can only be changed by authorised people or processes.
- Availability: Ensuring information is available to use whenever it is needed.

A.1.4 Providing adequate and appropriate protection to minimise the impact of information security threats, including:

- Identifying existing and new Information Security threats;
- Investigating potential impacts on the New Look information systems;
- Prioritising the threats based on potential impact and likelihood; and
- Implementing controls to effectively mitigate the risks in such a way to realise the best value for investment whilst minimising the impact on business operation.

A.1.5 Implementing Information and IT Security controls which conform to industry best practice, including, but not limited to:

- The NIST Cybersecurity Framework; and
- The Payment Card Industry Data Security Standard (PCI-DSS).

A.1.6 Complying with relevant Laws, Regulations, Statutory Instruments, and contractual requirements.

A.1.7 Providing appropriate Information Security awareness programmes and materials to all New Look colleagues.

A.1.8 Providing, communicating, and enforcing Information Security and IT Security Policies, Standards, Guidelines, Processes, and Procedures.

A.1.9 Establishing and maintaining relationships with law enforcement agencies, regulatory bodies and industry and specialist groups.

NEW LOOK

NEW LOOK

Appendix B: Access Management Policy Extract

B.1 All computer systems and applications must be protected by an effective authentication challenge that complies with the requirements below at a minimum.

B.2 Wherever possible, systems access should use one of the following:

B.2.1 Multiple factor authentication via a secure password and one of the following:

- Something you have, such as a token device or smart card.
- Something you are, such as a biometric element.

B.2.2 An approved passwordless authentication solution.

B.3 General Password Policy

B.3.1 Passwords must contain at least 8 characters. It is recommended that passwords are 12 characters or more.

B.3.2 Passwords must contain at least three of the following four features:

- Upper case letter
- Lower case letter
- Number
- Special character (i.e. symbol or punctuation character)

B.3.3 If passwords are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation), then passwords must be changed at least once every 90 days.

B.3.4 When creating a new password, you cannot re-use any of your previous four passwords.

B.3.5 Passwords must be kept secret.

B.3.6 Passwords must be reset immediately if users suspect that their password has been compromised or discovered by another person.

B.3.7 Accounts will lock after six unsuccessful password attempts.

B.3.8 Your New Look password must be unique to your New Look user ID such that:

B.3.8.1 You must not use your New Look password for accounts on any other external website or service, such as Internet shopping or social media sites.

B.3.8.1 You must not use any existing passwords you have for external sites or services as your New Look password.

B.3.9 When creating your password, the use of dictionary words, common sequences (such as qwerty or 123123), and the names of children, celebrities, pets, football teams, places etc. should be avoided.

B.3.10 You must not access or try to access any password-protected or restricted parts of the company's systems if you're not an authorised user.

B.3.11 Passwords must not be written down in an identifiable format.

B.3.12 New passwords assigned on joining the company, or passwords reset by the IT Help Desk, End User Computing (EUC) or Technical Services Group (TSG), must be changed after their first use.

B. 4 Privileged Password Policy

B.4.1 Privileged Passwords must have a length of at least 12 characters. It is recommended that privileged passwords are 16 characters or more.

B.4.2 Privileged Passwords must contain at least three of the following four features:

- Upper case letter
- Lower case letter
- Number
- Special character (i.e., symbol or punctuation character).

B.4.3 If passwords are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation), then passwords must be changed at least once every 90 days.

B.4.4 The previous 12 Privileged Passwords cannot be re-used.

B.4.5 No two systems should use the same Privileged Password.

B.4.6 Privileged Passwords that are required by more than one person must be kept secret in the Password Vault maintained and administered by IT Services.

B.4.7 Privileged Passwords must only be disclosed to authorised colleagues, and not disclosed to any other user.

B.4.8 Privileged Passwords must be changed immediately whenever a colleague who knows it changes role or leaves the company.

B.5 Third-Party Access

B.5.1 Third-party access guest must be uniquely identifiable and provide non-repudiation.

B.5.2 Before granting access to the New Look network, all third-party partners must have been fully onboarded and completed an associated supplier security questionnaire.

B.5.3 All third-party access must be compliant with the requirements of the Supplier Security Policy.

Appendix C: Backup and Recovery Policy Extract

C.1 All information assets processed by the Supplier on behalf of New Look shall be backed up regularly according to identified and documented business requirements.

C.2 The Supplier shall develop, maintain and test back up recovery procedures on a routine basis according to business needs.

C.3 Business owners are to be informed of and authorize all data recovery requests.

C.4 Critical back up data shall be subjected to regular tests and verification before being sent off-site for secure storage.

C.5 Backup data shall be stored on media that is appropriately labelled in accordance with the Information Classification and Handling Policy.

C.6 Backed up data and media used shall be provided with appropriate electronic, physical and environmental protection.

C.7 Media used for back up purposes shall be disposed of in a secure manner if no longer required in-line with the Information Retention Policy.

C.8 Backup data is to be transferred to off-site secure storage as soon as it has been successfully verified as complete.

C.9 Backups shall not be performed to USB, CD or similar removable media without explicit approval from New Look IT Services, adequate encryption and appropriate physical security.

NEW LOOK

Appendix D: Personal Data Retention Policy Extract

D.1 Personal Data should not be retained beyond its retention period in order that it can be used for a new purpose that is incompatible with the purpose for which it was originally collected. In the event that there is a requirement for Personal Data to be retained for a new purpose advice should be sought from the DPO.

D.2 Retention periods apply to all formats of Personal Data e.g. paper, electronic, images, oral recordings etc. unless specifically stated otherwise.

D.3 New Look shall ensure secure and appropriate disposal of Personal Data at the end of the retention period.

D.4 Retention periods are stated in the Personal Data Retention schedule available via Runway.

NEW LOOK

Appendix E: IT Use Policy Extract

E.1 Company IT Equipment and services are provided for business use and remain the property of the New Look Group. This includes, but is not limited to:

- Laptop or Desktop computers;
- Company Mobile Phones;
- Printers;
- Local and Network storage devices;
- Email and messaging systems; and
- Internet access.

E.2 All Company IT Equipment must be returned to New Look when the employee to whom it is assigned:

- leaves the company; or
- transfers to another role within New Look where the equipment is not required.

E.4 Portable Company IT Equipment such as Laptops, Tablets, HHTs and mobile phones, must not be left unattended where it may be accessed by an unauthorised person.

E.5 All Portable Devices used for processing Company information must be protected by a Password or PIN which complies with the New Look Password Policy.

E.6 The theft or loss of any Company IT Equipment or Personal Device used for Company business and protected by standard Company security controls must be reported to the IT Help Desk as soon as the loss is discovered.

E.7 Protected, Confidential or Internal information held on paper must be disposed of in a Confidential waste bin or tote bag.

E.8 Disposal of Company IT Equipment

E.8.1 Company IT Equipment must be returned to IT Services at the end of its life

E.8.2 IT Services will ensure that:

- All Confidential and Sensitive information stored on the equipment is appropriately sanitised or destroyed.
- The equipment is disposed of in accordance with the Waste Electrical and Electronic Equipment Directive (WEEE directive).

E.9 Prohibited Activities:

E.9.1 Accessing, or attempting to access, the company network, corporate applications or cloud services using a User ID and Password combination belonging to another user.

E.9.2 Allowing any other user to access the company network or any other corporate device application or cloud service through sharing a User ID and Password combination.

E.9.3 Using any open Network or Application session utilising a User ID and password combination which belongs to someone else.

E.9.4 Accessing any internet site which is blocked by, or attempting to bypass, the corporate Internet filtering software.

E.9.5 Signing up to or accessing any corporate application or cloud service using a personal account and/or email service.

E.9.6 Connecting any Personal Device to the internal Support Centre, Retail Store or Distribution Centre networks or corporate VPN without prior approval from IT Services.

E.9.7 Installing or attaching, or attempting to install or attach, non-standard and non-approved software or hardware devices to any Company IT Equipment.

E.9.8 Removing Protected, Confidential or Internal information from any New Look location without a business need, justification, or approval - this includes:

- Employee Information
- Customer Information
- Financial Information
- Any information considered Intellectual Property, including but not limited to:
  - Garment designs
  - Computer code
  - Internal communications.

E.9.9 Attempting to modify, disable, or remove any security software, device, or malware protection from any Corporate device, or Personal device secured to process Company information.

E.9.10 Storing personal files or information on the New Look company network, its corporate devices or its cloud services.

E.9.11 Using Company IT Equipment during company time to conduct inappropriate activities which may be considered "misuse", including, but not limited to:

- Any activity that's defined as "misuse" within the Computer Misuse Act 1990.
- Using a private email account for business purposes.
- Opening or sending emails known to be infected by malware.
- Deliberately propagating malware.
- Using non-approved Instant Messaging facilities.
- Using Peer-to-Peer software or other non-sanctioned file sharing tools.

E.9.12 Attempting to modify a company mobile phone or other device, including any attempt to root or jailbreak such devices, without prior authorisation from IT Services.

E.9.13 Sending, printing or otherwise distributing personal data, New Look information, trade secrets or other Protected, Confidential, or Internal information without an authorised business need to do so.

E.9.14 Sending credit and debit card numbers in unencrypted or unmasked form.

E.9.15 Any other activity likely to bring New Look into disrepute.

E.10 New Look reserves the right to deny access, without cause, including Network, Email, and Internet access, to any employee from Company IT Equipment.

E.11 Monitoring:

E.11.1 New Look reserves the right to monitor all user activities, including, but not limited to:

- Building access;
- Internet use;
- Emails and Email use;
- Instant messaging use;
- Application Audit Trails;
- Telephone use; and
- Company Mobile Telephone use.

E.11.2 Where required to do so by Law, Court Order, or other statutory instrument, New Look will disclose relevant information, content and usage statistics to assist in any investigation.

NEW LOOK

Appendix F: Information Classification and Handling Policy Extract

F.1 All New Look information must be classified into one of the following four categories:

a) Protected Information
b) Confidential Information
c) Internal Information
d) Public Information

F.2 Protected Information:

F.2.1 If Protected Information is compromised, it may cause substantial damage to New Look, its shareholders, its partners, its Customers and/or its Employees.

F.2.2 Protected Information must be kept secret and shared only with those who have authority to see or hear it.

F.2.3 Any media – document, electronic storage device, email – containing Protected Information must be marked "Protected".

F.2.4 Authorisation from the DPO and the Data owner must be provided in order to process, store or remove Protected Information outside of the New Look internal network. This includes the use of external Cloud based solutions.

F.2.5 Protected Information must not be stored in test systems nor used for systems testing purposes.

F.2.6 Examples of Protected Information include, but are not limited to:

- Special categories of Personal Data as defined by applicable data protection legislation;
- Disciplinary proceedings
- Payment Card Information;
- Bank Details;
- Financial Results pre-release;
- Company Strategy;
- Business Plans; and
- Physical Security and Information Security measures.

F.3 Confidential Information:

F.3.1 If Confidential Information is compromised it may cause significant damage to New Look, its shareholders, its partners, its Customers and/or its Employees.

F.3.2 Confidential must be kept within New Look and only shared outside New Look with the appropriate authority.

F.3.3 Any media – document, electronic storage device, email – containing Confidential Information must be marked "Confidential ".

F.3.4 Authorisation from the DPO and the Data owner must be provided in order to store or remove Confidential Information away from New Look premises. This includes Cloud based applications and services.

F.3.5 Confidential Information must be appropriately protected when stored in test systems or used for systems testing purposes.

F.3.6 Examples of Confidential Information include, but are not limited to:

- Personal data;
- Personally Identifiable Customer Information, including any data that may indirectly identify an individual;
- Personally Identifiable Employee Information, including any data that may indirectly identify an individual;
- Garment Designs;
- Financial information such as pricing and discount levels and takings;
- Information pertaining to garments, garment ranges, or season ranges not yet available in stores;
- Application program code and Database schema designs; and
- Any other information that constitutes Intellectual Property owned by New Look.

F.4 Internal Information:

F.4.1 Internal information is information that is circulated within New Look only, including Information which is only accessible to certain employees/ teams/contractors.

F.4.2 If Internal Information is compromised it may cause some damage to New Look, its shareholders, its partners, its Customers and/or its Employees.

F.4.3 Data-owners permission must be obtained before deleting or destroying Internal data.

F.4.4 Examples of Internal information include, but are not limited to:

- Internal staff communications

- Internal only intranet pages
- Press releases pre-release

F.5 Public Information:

F.5.1 Non-Sensitive Information can be found in, or is disclosed into, the Public Domain.

F.5.2 If Public data is compromised, it would cause little or no damage to New Look, its shareholders, its partners, its Customers nor its Employees.

F.5.3 Authorisation is not required to remove Public data from New Look premises.

F.5.4 Examples of Public information include, but are not limited to:

- Press releases and External communications in the public domain; and
- Images of garments, garment ranges, or season ranges which have been, or are in stores.

F.6 Mixed Information Categories:

F.6.1 Any document or data store containing information at different classification levels must be classified by the highest category of information contained therein.

F.7 Classification Changes:

F.7.1 Where information is re-classified – for example, Financial Results, which remain Protected until they are released into the public domain and become Public - they must be marked appropriately at all stages in their life cycle and re-classified when it is appropriate to do so.

F.8 Storage and transportation requirements:

F.8.1 Additional protection, up to and including Encryption, must be applied to Protected Information in electronic form when:

- At rest within and external from New Look.
- In transit within and external from New Look.

F.8.2 Additional protection, up to and including Encryption, should be applied to Confidential Information in electronic form when:

- At rest when external from New Look.
- In transit when external from New Look.

F.8.3 No additional protection needs to be applied to Internal and Public information in electronic form.

F.8.4 Protected or Confidential Information on, or attached to, Emails must:

- Not be sent to non-New Look email addresses except in exceptional circumstances with prior management and DPO approval.
- Not be auto-forwarded to an external destination.
- Not contain credit or debit card information.
- If received from another user, not forwarded on to any individual who is not authorised to receive the email.

F.8.5 Protected or Confidential Information on electronic or magnetic media must:

- Not be created without the prior approval of the DPO
- Be kept secure when not in use.
- Be kept secure in transit.
- Not be left unattended, especially where it could be taken by an unauthorised individual.
- Be assigned an appropriate retention period and destroyed after this period is up.

F.8.6 Protected or Confidential Information in paper form must:

- Be kept secure when not in use.
- Be kept secure in transit.
- Not be left unattended on desks or other work areas, especially where it could be accessed, viewed, or photographed by an unauthorised individual.
- Be cleared from printers and fax machines as soon as printed or faxed.

F.8.7 When transferring information across international borders, some types of information may have additional restrictions. Please consult the DPO, Legal team and appropriate Data owner before transferring any of the following:

- Payment Card Information.
- CCTV images.

F.8.8 Processing or using Protected or Confidential information away from the office:

F.8.9 You must take additional care and exercise vigilance if you are using or processing Protected or Confidential information away from the office environment.

F.8.10 If this use is electronic (i.e. on a Laptop or Tablet computer) then you must:

- Use a laptop privacy screen to protect your screen from being viewed by other members of the public who are not authorised to see New Look information.
- Ensure that your laptop is secure at all times, not left attended, and locked or shut down when not in use.

F.8.11 Electronic, magnetic, and paper media containing, or which have contained, Protected or Confidential information that is no longer required must be disposed of in line with the requirements of the New Look Asset Management Policy and the New Look Data Retention policy

F.9 General Data Protection Regulation (GDPR) Specific Requirements:

F.9.1 Under the GDPR and the Data Protection Act 2018, we are required to keep a record or register of all the processing operations on personal data carried out by New Look.

F.9.2 This Data Processing register is held by the DPO and must contain information explaining the purpose and conditions of all these operations.

F.9.3 All systems that hold or process personal data must be recorded in the Data Processing Register.

F.9.4 All procedures involving personal data must be recorded in the Data Processing Register.

F.9.5 All Heads Of Departments, as Data Owners, must ensure that all their systems and procedures are recorded in the Data Processing Register on an annual basis.

F.9.6 Personal data as defined by the GDPR must be handled and processed in line with the requirements of the New Look Data Protection Policy, which takes priority over the requirements of this policy.