INFORMATION SECURITY POLICY
STATEMENT OF INTENT

PURPOSE OF THE POLICY
Henderson & Taylor is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

This purpose of this policy is to:

- Protect against potential breaches of confidentiality.
- Ensure all our information assets and IT facilities are protected against damage, loss or misuse.
- Support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- Increase awareness and understanding in the Company of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

APPLYING THE PROCEDURE
This policy sets out the conduct expected and applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers.

It also explains the circumstances in which Henderson & Taylor may monitor your use of its systems. All staff members are required to follow this (non-contractual) policy, which may be updated or varied from time to time.

Managers have responsibility to ensure that staff members act in accordance with this policy.

Breach of this policy may be dealt with under our Disciplinary Procedures and may be considered gross misconduct if the circumstances support this conclusion.

INFORMATION MANAGEMENT
All Company information must be treated as commercially valuable and be protected from loss, theft, misuse or inappropriate access or disclosure.

The information covered by the policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of Henderson & Taylor, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

All information is owned by Henderson & Taylor and not by any individual or team and all information must only be used in connection with work being carried out for Henderson & Taylor and not for other commercial or personal purposes.

Information gathered should not be excessive and should be adequate relevant, accurate and up to date for the purposes for which it is to be used by the Company.

Information will be kept for no longer than is necessary. All confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as the need for its retention has passed.

Everyone has a part to play in ensuring data security by:
- Reporting any unauthorised personnel in entry-controlled areas to a director.
- Using secure passwords on computers and not sharing them in a manner which is inappropriate.
- Shredding paper documents as/if appropriate.
- Logging off from your computer as/if appropriate.

INFORMATION SECURITY POLICY
STATEMENT OF INTENT

HENDERSON & TAYLOR

ACCESS TO OFFICES AND INFORMATION

Visitors should be required to sign in at reception, accompanied at all times and never be left alone in areas where they could have access to confidential information.

Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains Company information, then steps should be taken to ensure that no confidential information is visible.

At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

COMPUTERS AND IT

You are also responsible for ensuring the security of the equipment allocated to or used by you. Computers and other electronic devices must be password protected. Passwords should be kept confidential, not written down or given to others.

Computers and other electronic devices should be kept safe and locked when not in use to minimise the risk of accidental loss or disclosure. Use password protection and encryption where available on Company systems to maintain confidentiality.

You must not log on using other people's username and password. You must not allow others to log on using your username and password. An exception may be made if you are directed to do so by someone suitably authorised to allow this to occur.

You should log off when leaving your computer unattended or on leaving the workplace in order to prevent unauthorised users accessing the system in your absence.

Confidential information must not be copied onto removable hard drive, CD or DVD or memory stick/thumb drive without the express permission of a director. Data copied onto any of these devices should be deleted as soon as possible and stored on Henderson & Taylor's computer network data drivers in order for it to be backed up.

All electronic data must be securely backed up in accordance with company policy.

DO NOT CORRUPT OUR EXISTING SOFTWARE

You must not download or install software or modify existing computer programs or applications or any information or other data without authorisation from your line manager or the IT Project Manager. This includes applications and software programs.

Any incoming files and data should always be virus-checked before they are downloaded. Do not open unsolicited emails which appear suspicious and/or which have files or links attached to them. Treat any file with the extension "exe" with extreme caution as it is an execution file and is commonly used to corrupt computer systems. In addition, look out for are the links/macros imbedded in word documents/excel spreadsheets etc. The general principle is to never open any files or click links if you do not recognise the sender.

IF YOU THINK YOUR COMPUTER HAS A VIRUS

If you think your computer or other electronic devices may have acquired a virus then tell the IT Project Manager immediately. Do not attempt to use it any further. Do not respond to any further prompts which pop up on the computer. In order to avoid any spread of infection to other networked devices, please make sure to shut down your IT equipment as soon as suspicion arises.

COMMUNICATIONS AND TRANSFER
Staff should be careful about maintaining confidentiality when speaking in public places.

Confidential information should be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the Company.

Confidential information must not be removed from the Henderson & Taylor's Head or site offices except where that removal is temporary and necessary.

In the limited circumstances when confidential information is permitted to be removed, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

- Not transported in see-through or other un-secured bags or cases.
- Not read in public places (e.g. waiting rooms, cafes, trains).
- Not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots, cafes).

TRANSFER TO THIRD PARTIES
Third parties should only be used to process Company information in circumstances where written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings.

Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the data protection officer or a director for guidance and authority.

HUMAN RESOURCES INFORMATION
Given the internal confidentiality of personnel files, access to such information is limited to those members of Henderson & Taylor who need access to it for operational reasons in compliance with our Data Protection Policy. Except as provided in individual roles, other staff are not authorised to access that information.

Any staff member in a management or supervisory role must keep personnel information confidential.

Staff may ask to see their personnel files in accordance with the relevant provisions of the Data Protection Act 2018.

DATA SECURITY AND DATA BREACHES
Henderson & Taylor must comply with any applicable privacy legislation requirement to notify data subjects or supervisory authorities of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to personal data (Breach).

Appropriate technical and organisational security measures must be taken to prevent a Breach. It is important that everyone ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

INFORMATION SECURITY POLICY
STATEMENT OF INTENT

REPORTING BREACHES

All staff have an obligation to report actual or potential data protection compliance failures to a director, manager or IT Project Manager. This allows the Company to:

- Investigate the failure and take remedial steps if necessary.
- Make any applicable notifications.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the IT Project Manager or your line manager as breaches and follow their instructions. You should preserve all evidence relating to the potential Personal Data Breach. For present purposes, a data breach can include loss of a device with personal data on it as well as evidence of a computer virus or a hacking incident.

CONSEQUENCES OF FAILING TO COMPLY

Henderson & Taylor takes compliance with this policy very seriously. Failure to comply puts both staff and the Company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary procedures.

Staff with any questions or concerns about anything in this policy should not hesitate to contact the IT Project Manager.

CHANGES TO THIS POLICY

Henderson & Taylor reserve the right to supplement or amend this policy from time to time by additional policies and guidelines. Any new or modified policy will be circulated to staff before being adopted.

AUTHORISED BY: _____

Matthew Lynch – Director