menstrual cup coalition

Information security and acceptable use of IT policy

Document Control	
Approved by:	MannionDaniels' Directors
Responsible Owner:	Operations Team
Created:	30 April 2016
Revised:	07 January 2022
Approved:	07 January 2023
Next Review:	06 January 2024
Version:	4

Introduction

This document sets out the MannionDaniels Information Security and Acceptable Use of IT policy. Information security is the preservation of confidentiality, integrity, and availability of information. This policy is mandatory. Any breach of the policy may result in disciplinary action being taken under the MannionDaniels Disciplinary Procedure. This policy should be read in conjunction with MannionDaniels Data Protection Policy.

Objective

The objective of this policy is to protect and maintain the security of the company's information. Information Security is critical to ensuring MannionDaniels can rely on its information to carry out its business needs and to meet its statutory and contractual requirements.

Scope

This policy applies to all the users in MannionDaniels, including temporary staff, visitors and suppliers who are granted temporary user access to MannionDaniels information. The policy applies to all information held, processed, or used by MannionDaniels and to all modes of communicating information both internally and externally. All staff are responsible for ensuring that they understand and abide by this policy.

Principles

The key principles that we advocate for protecting information, and protecting yourself are as follows:

- Handle all information with care
- Ensure critical data is stored safely
- Think before you send
- Keep your passwords safe
- Don't fall for a scam
- Secure your computer and other devices
- What you do online has repercussions

Standards required

The purpose of this policy is to ensure that all information systems operated by MannionDaniels are secure and comply with the standards of the Data Protection Act (2018), the Computer Misuse Act (1990) and UK Government Cyber Essentials Scheme. It is also the aim of MannionDaniels that all staff are aware of the need to maintain secure systems and understand their responsibilities to protect information including personal data and confidential information.

It is the policy of MannionDaniels to ensure the following standards are practiced;

- Information is protected against unauthorised access, and available to authorised users when needed.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or negligent action.
- Mitigate risk associated with the loss, misuse, theft, damage, or abuse of information systems.
- The integrity of information is maintained by protection from unauthorised modification.
- Protect MannionDaniels from any potential damage through the misuse of its IT facilities
- Regulatory and legislative requirements are met.
- Contingency plans are produced and tested as far as is practicable to ensure business continuity is maintained.
- Information Security training is provided for all staff.
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action taken.
- Ensure any incidents are reported so review can take place and feed into a cycle of continuous

improvement
- Sharing of information with other organisations/agencies is permitted providing it is done within the remit of a formally agreed information sharing protocol.
- That there is a fair and consistent approach to the enforcement of standards of conduct expected from employees when using social media sites.

Training, awareness and communication

Training on information security will form part of the induction process for new starters. Ongoing training and awareness will be implemented and maintained on an annual refresher basis for all staff.

Compliance, legal and regulatory obligations

MannionDaniels must adhere to all relevant legislation as well as meet certain contractual requirements. MannionDaniels operate across several global offices to which compliance to this policy is necessary. Where applicable laws require a higher standard of protection than that set out in this Policy, the requirements of applicable laws shall prevail. Where applicable laws establish a lower standard of protection than that set out in this Policy, the requirements of this policy shall prevail.

Relevant legislation and contractual compliance frameworks include:

- Data Protection Act (2018)
- The Computer Misuse Act (1990)
- HM Government Security Policy Framework (2018)
- HM Government Cyber Essentials Scheme

Responsibilities

Governance and oversight

- MannionDaniels Directors: hold ultimate responsibility for information security.
- Leadership team: is responsible for demonstrating their commitment to information security by ensuring effective communication and implementation of this policy (and related policies) across MannionDaniels.
- Digital Manager / Information Security Officer: has responsibility for ensuring our systems comply with the information security policy and acting as the point of contact with our service providers and compliance team.
- Data Protection Officer: supports the Directors by advising and monitoring that effective data protection processes are in place.
- Compliance Manager: is responsible for ensuring data protection measures are implemented with staff and suppliers.
- Senior Managers: are responsible for data protection in their area and must ensure all permanent and temporary staff and contractors are aware of their responsibilities and take action to instigate re-training where required.
- All Staff: must comply with this policy including the maintenance of data confidentiality and data integrity.
- Others: including third party service providers, partners, contractors, and their employees who are authorised users, have an obligation to ensure they implement adequate processes and security to protect the assets and data of MannionDaniels.

Senior Manager Team (SMT) responsibilities

- All Senior Managers must give their full backing to all the guidelines and procedures as set out and agreed in this document.
- Senior Managers must ensure that new staff who require access to information systems are

provided with the correct access privileges
- Senior managers are responsible for maintaining the data access, filing integrity and the upkeep of the data registers for their area of responsibility.

Leavers

- The HR manager must ensure that the leavers IT account is closed immediately and also that all IT equipment is returned for re-use.
- The compliance manager must ensure that the users work related information, e-mails and data is transferred, if required, to the respective working directory for future access on the system or is deleted. This will ensure that the appropriate security is maintained on leavers information and data.

Individual responsibilities

For the avoidance of doubt, all individuals have a role to play in implementing Information Security and Acceptable Use of IT Policy, as follows:

- Individuals must ensure that as far as is possible no unauthorised person has access to any data held by MannionDaniels.
- Individuals must ensure that physical security measures are properly used.
- Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to MannionDaniels. This includes the proliferation of viruses or other similar computer programmes.
- Individuals will be given access passwords to certain computer systems. Passwords are a critical part of your online identity and must never be shared with other members of staff. They provide access not just to the network, but also to your e-mail and networked file stores that may contain personal, sensitive, or confidential information.
- Individuals must not load or download software packages onto MannionDaniels devices without prior authorisation.

Information security and use

Physical security

Access to data held at MannionDaniels offices should be minimized by controlling the physical access to the office buildings and ensuring that offices are secure, as follows

- Access to buildings is restricted by ensuring that doors are closed properly, keys are only issued to authorised staff and that alarm codes are kept secure and changed regularly.
- Doors and windows must be secured at all times when the office is left unattended.
- Visitors must be escorted in and out of the office at all times.
- Workspaces must be kept clean and any non-public information locked away.
- To avoid losing your device, don’t leave it unattended.
- Always use a screen lock to avoid unauthorised access.

Computer security

MannionDaniels have systems in place to manage computer security and have appointed an IT supplier to support in the maintenance of laptops and IT systems. As a minimum we require:

- Up to date anti-virus protection
- Where possible we will restrict software download by individuals. However, we ask that staff seek approval before installing any software or accepting a download of similar.
- All laptops are encrypted when issued. We do not encourage staff to store data on laptops and we provide access to secure cloud document storage facilities for this purpose via Box.com. However, for the avoidance of doubt all data should be stored on an encrypted device.
- We do not allow confidential or restricted data to be accessed or stored on a personal tablet or

phone.
- All devices (MannionDaniels and Personal) must be protected by a password or PIN (if applicable)

Data storage

- All information related to MannionDaniels business is to be stored on Box or on Box drive on MD encrypted laptops and not on a disk or removable devices. Box provides secure storage area which is protected by security protocols to ensure it is safe and resilient. Storage of data on a PC or Laptop's hard drive is discouraged because in the event of failure, all data stored on the drive would be lost as it not backed up.
- If your data cannot be stored on Box.com please discuss your needs with the Digital Manager to ensure your data is backed-up to an encrypted device and is recoverable.
- All staff must abide by the rules of the Data Protection Act (2018) and the Computer Misuse Act (1990).
- When using Box.com always ensure that data is stored in a folder with access appropriate to its classification.
- All documents and files should be given clear and descriptive titles that will help others to understand what is contained within them.
- Information which is no longer required should be promptly disposed of by deletion or destruction. Unless an audit record of versions is explicitly required previous versions of documents should be destroyed when the new version is created.

Memory sticks and removable media

- Please seek guidance from IT should you wish to use a memory stick as only approved encrypted memory sticks should be used.
- MannionDaniels data protectively marked confidential and restricted must not be transferred to a home PC / Laptop/ tablet / phone.

Password policy

A password policy is a set of requirements to ensure that passwords are strong.

- Choose a long and secure password to log into your PC or laptop, you will not be required to change this unless a security incident has occurred relating to you or your device. You can use a scheme such as selecting three random unrelated words and stringing them together. See http://correcthorsebatterystaple.net for examples of this approach.

- You can then use an approved password manager to manage all of your online passwords. Such as: Dashlane, 1password or keepassx

For all users, a password must satisfy the following conditions to ensure a strong password is used:

- It must be more than 8 characters, ideally 20-30 characters if the above approach is adopted.
- It must not be your username
- It must not be your current password
- It must not be your initial password
- It must contain a mix of upper- and lower-case letters and at least one number. Ideally passwords should also contain random characters such as #@?!$& etc.
- It must contain at least one letter
- Don't share passwords
- Don't use shared accounts unless it is completely unavoidable. If a shared account is being used, then the password must be changed every time one of the users leaves or no longer requires access.
- Don't store passwords in public places e.g. on post it's, white boards etc.

Viruses

- All files received on removable media from outside MannionDaniels or received via e-mail are checked for viruses before being used on MannionDaniels equipment.
- If a virus is suspected, please report this immediately to IT.

3rd party network connections

- All requests for external 3rd Party network connections must be authorised by MannionDaniels Digital Manager.

Wi-Fi usage

To define minimum requirements for the usage and provision of Wi-Fi.

MannionDaniels staff and guest Wi-Fi networks

- Staff Wi-Fi access must only be granted to MannionDaniels staff.
- Guest Wi-Fi access should be granted as required to trusted individuals.
- Wi-Fi access passwords must be changed as directed by the digital Manager.
- Wi-Fi access passwords must be changed if a security incident has occurred involving people or devices that have had access to the MannionDaniels Wi-Fi network.
- Guest Wi-Fi network must be segregated from and notable to access devices on the MannionDaniels staff network.
- All access points must be kept up to date with the latest firmware security patches.
- Staff Wi-Fi access points must be set to only allow WPA2-AES security protocol

Public Wi-Fi networks

Public Wi-Fi is inherently insecure so treat all links with suspicion.

- We recommend staff to avoid public Wi-Fi as cybercriminals may have set up access points with similar names to the hotel or coffee shop you are currently attempting to connect to.
- Instead, we recommend staff tethering to your secure mobile phone hotspot instead of using public Wi-Fi.
- For staff that need Wi-Fi access whilst in transit and do not have mobile data, please discuss your needs with the Digital Manager, as a Wi-Fi dongle or MannionDaniels device may be issued.
- If you decide to connect to a public Wi-Fi from a personal device, do not access any MannionDaniels services or data and we suggest you do not access any other websites or services that require a password.

Encryption

To define the minimum requirements for the safe encryption of data.

Encryption strength and Ciphers

Only tools and products based on proven, mathematically sound cryptographic algorithms, subjected to peer review by the cryptographic community, shall be used for encryption. Approved tools are, Bit locker and ESET for Windows, File vault for Apple Macs.

- Block Ciphers: 3DES, IDEA, RC5, AES, CAST, Blowfish –minimum 128 bit, recommended 256-bit key length.
- Public Key Ciphers: RSA, Diffie-Hellman -a minimum asymmetric key length of 2048 bits should be used. For long term security an asymmetric key length of 4096 bits is recommended

Mobile workers and home workers

Laptops

- Care must be taken to avoid being overlooked whilst using MannionDaniels equipment in any public area
- Laptops must be kept in a secure location when not in use.
- Laptops must not be left unattended during the normal working day unless it is on MannionDaniels premises where there is good physical security at entrances to the building.
- When using portable equipment on the move, or outside of office hours, reasonable care should be taken to secure it.
- If the laptop is to be left unattended in a secure location the screen lock must be set.
- If the laptop is in a public location it must be turned off (not sleeping) when not in use

Manual files

Whilst manual files are not commonly used, if any information or equipment is taken by staff in hard copy, it should be treated with extra care, as follows:

- Manual files and equipment outside of the MannionDaniels property must be kept with the individual or kept in a secure place.
- Computer equipment or manual files must not be left unattended on a train or bus or left in a vehicle overnight

Mobile phones

- Staff issued with mobile phones or other personal digital equipment are responsible for safekeeping and security.
- Where personal devices are being used to access MannionDaniels systems (such as MS Teams) the device should be protected with a PIN or password.
- Box.com must not be used on a phone or tablet
- MannionDaniels email should not be installed on personal phones. Instead we request staff to access email on phones or tablets through the webmail platform.

Unacceptable use

MannionDaniels has zero tolerance to all forms of abuse, sexual exploitation, bullying and harassment. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of information and should always meet the standards of MannionDaniels code of conduct. The MannionDaniels network and equipment may not be used directly or indirectly by a User for the download, creation, manipulation, transmission, or storage of:

1. any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited "nuisance" e-mails;
4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of MannionDaniels or a third party;
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age, or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9. material that brings MannionDaniels into disrepute.

Blogging and social media

The following principles apply to professional use of social media on behalf of MannionDaniels as well as personal use of social media when referencing MannionDaniels.

Employees should follow these guidelines in relation to any social media that they use.

1. Never represent yourself or MannionDaniels in a false or misleading way. All statements must be true and not misleading; all claims must be substantiated.
2. Post meaningful, respectful comments —no spam and no remarks that are off-topic or offensive.
3. Use common sense and common courtesy and be respectful at all times
4. Ask permission before disclosing conversations that are meant to be private or internal to MannionDaniels.
5. When disagreeing with others' opinions, keep it appropriate and polite. If you find yourself in a situation online that looks as if it's becoming antagonistic, do not get overly defensive and disengage from the dialogue in a polite manner that reflects well on MannionDaniels. images or material;
6. Never participate in Social Media when the topic being discussed may be considered a crisis situation. Even anonymous comments may be traced back to your or MannionDaniels' IP address.
7. Be smart about protecting yourself, your privacy, and MannionDaniels' confidential information. What you publish is widely accessible and will be around for a long time, so consider the content carefully.

E-mail use

Sending e-mail

- Individuals must not alter the text of any received messages, including when forwarding them to others. Similarly, individuals should not assume that a forwarded message matches what was originally authored.
- Individuals must not use other people's email accounts nor attempt to impersonate someone else or appear anonymous when sending e-mail.
- All e-mails should be finished with company e-mail signatures as defined by MannionDaniels communications team.
- Where information needs to be sent securely, we do not recommend using email, which is inherently insecure. Services such as Box.com are available for secure transfer of data. Please speak to the Digital Manager or Compliance Manager about your needs.

Misuse of e-mail

- Individuals must not send or forward any abusive, threatening, defamatory or obscene messages.
- Staff must take care with any suspected malicious or nuisance e-mails received (e.g. chain e-mail, phishing and spam e-mails) and delete them. If any suspicious e-mails are received, they should be reported to IT.
- Individuals must never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

Use of the internet

- individuals must take care to ensure that files downloaded from the Internet are from a trustworthy source.
- Individuals are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any MannionDaniels work.

Security incident reporting

Reporting security incidents in a prompt and appropriate manner will enable MannionDaniels to efficiently mitigate the risks. Any incidents where there has been a deliberate attempt whether successful or not, to compromise MannionDaniels data or assets should be reported immediately. This includes any data that is in the possession of a contractor or supplier.

All information security incidents no matter how small they seem, must be reported immediately to either; the Digital Manager, Compliance Manager or Director of Operations. This includes, but is not limited to;

- Loss of any piece of equipment (computer, laptop, mobile phone, USB storage device, etc)
- Emails sent to the wrong recipient
- Data made available to individuals who should not have access to it
- Loss of password
- Attempted security threat, including scams via email or phone
- Bogus websites

Please also review the Data Protection Policy and the Data Breach procedure.

Appendix A: References

Legal references (This is not an exhaustive list)

- Data Protection Act (2018)
- Companies Act (1985)
- Copyright, Designs and Patents Act (1998)
- Computer Misuse Act (1990)
- Freedom of Information Act (2000)
- Civil Contingencies Act (2004)
- Regulation of Investigatory Powers Act (2000)
- Human Rights Act 1998 (2018)