Information Security and Acceptable Use of IT Policy

Document Control	
Approved by:	MannionDaniels' Directors
Responsible Owner:	Operations Team
Created:	30 April 2016
Revised:	04 February 2020
Approved:	04 February 2020
Next Review:	03 February 2021
Version:	3

Table of contents

1 Introduction 3

1.1 Objective 3

1.2 Scope 3

1.3 Principles 3

2 Standards required 3

3 Awareness & Communication 4

4 Compliance, Legal and Regulatory Obligations 4

5 Responsibilities 4

6 Requirements 5

6.1 Physical Security 5

6.2 Computer Security 6

6.2.1 Data Storage 6

6.2.2 File Storage and Naming Conventions 6

6.2.3 Memory Sticks and removable media 6

6.2.4 Password Policy 6

6.2.5 Viruses 7

6.2.6 3rd Party Network Connections 7

6.3 WiFi usage 7

6.4 Encryption 7

6.5 Mobile Workers and Home Workers 8

6.6 Unacceptable Use 8

6.7 Blogging & social media 9

6.8 E-mail Use 9

6.9 Use of the Internet 10

6.10 Security Incident Reporting 10

Picture credits
Cover, left and on table of contents, left: Team Kenya
Cover, right: Send a Cow

1 Introduction

This document sets out the MannionDaniels Information Security and Acceptable Use of IT policy and procedures, and the responsibilities of everyone using MannionDaniels systems and IT. Information security protects individuals, our partner organisations and ensures compliance with legislation through proportionate guidance to recording, storing, processing, exchanging and deleting information. Should this not be achieved, MannionDaniels can risk, at worst, the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner. Information refers to physically held information which includes paper copies, files and records and electronic information includes data held in computers, drives, memory sticks and other portable devices. This policy is mandatory. Any breach of the policy may result in disciplinary action being taken under the MannionDaniels Disciplinary Procedure.

1.1 Objective

The purpose and objective of this Information Security and Acceptable Use of IT Policy is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities. This policy is critical for providing assurance to funders, regulators, auditors and governments that MannionDaniels takes seriously the confidentiality, integrity and availability of data placed in its care.

1.2 Scope

This document applies to all the users in MannionDaniels, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. All persons who require access to the MannionDaniels network and/or IT systems will be required to read and understand this Information Security and Acceptable Use of IT Policy and sign the Acknowledgement of Acceptance (Note: Electronic signatures are also acceptable).

1.3 Principles

There are three main principles to this policy: a) to consider the sensitivity of the information being handled, b) to protect information in proportion to its sensitivity by ensuring that information, whatever its format, is secured by physical or approved electronic means and c) to ensure that the appropriate action is taken within the procedures when there is a breach of policy.

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

2 Standards required

The purpose of this policy is to ensure that all information systems operated by MannionDaniels are secure and aspire to comply with the standards of the Data Protection Act, and the Computer Misuse Act. It is also the aim of MannionDaniels that all staff must be fully aware of the need to maintain secure systems and fully understand their responsibilities as outlined in this document to fully protect the high standard information assets, including an individual's private information, as well as client and company's confidential information.

All staff are responsible for ensuring that they understand and abide by this policy. This policy applies to all information held by MannionDaniels which includes information held on its behalf by partners, contractors such and all permanent, contract, consultants or temporary employees, including third parties who have access to MannionDaniels premises, systems or 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. The provisions of this policy are known to and accepted by the 3rdparty as part of a contract.
- That there is a fair and consistent approach to the enforcement of standards of conduct expected from employees when using social media sites. dealing with a similar subject for two different clients with competing or inconsistent interests

The policy applies to all systems, software and information created, held, processed or used on those systems or related media, electronic, magnetic, or written/printed output from MannionDaniels systems. It applies to all modes of communicating information both within the organisation and externally.

3 Awareness & Communication

Training on security issues will form part of the process for new starters. Ongoing awareness programs will be established and maintained as necessary to ensure we demonstrate a positive attitude to information security.

4 Compliance, Legal and Regulatory Obligations

MannionDaniels must adhere to all current UK and EU legislation as well as regulatory and contractual requirements. MannionDaniels operate across a number of global offices to which compliance to this policy is necessary. Compliance with this policy is vital to MannionDaniels in maintaining the ethical and integrity-based approach we have developed to all business interactions and activities and will ensure efficiency and effectiveness in managing and protecting our information. Breach of this policy is likely to have serious consequences for MannionDaniels business and any breach may result in disciplinary action.

5 Responsibilities

- **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.
- **Information Security Officer** has responsibility for information security and acting as the point of contact with our service providers and compliance.
- **Data Protection Officer** will support the Information Security Officer by ensuring effective engagement and communication of any data related issues that may compromise Information Security and reporting any risks/issues raised
- **Procurement Officer** is responsible for ensuring contracts are sufficiently robust and clear about the responsibilities of third party/partners and instigating periodical checks to assess compliance.
- **Managers** are responsible for information security 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. Contracts with external providers that allow access to information systems shall be in operation before access is allowed and shall comply with all appropriate security and related policies.

Manager responsibilities

- All Managers must give their full backing to all the guidelines and procedures as set out and agreed in this document.
- Managers must ensure that new staff who require access to ICT are provided with log-in credentials and access privileges as appropriate.
- Managers must also take responsibility to ensure:
  - All new staff receive a briefing on this policy as part of their induction and formally sign the Acknowledgement of Acceptance before they are given access to any of the MannionDaniels IT systems.
  - All staff review this Policy and re-confirm acceptance on an annual basis or when invited to do so.

Leavers -Management of User Accounts

- Managers must ensure that the leavers IT account is closed immediately and also that all IT equipment is returned for re-use.
- Managers 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.

6 Requirements

In For the avoidance of doubt, the Information Security and Acceptable Use of IT Policy requires that;

- 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 should not be shared to 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.

6.1 Physical Security

The office is vulnerable to data breach from easy access by external entities. If a computer, phone or other device gets lost or is infected with a virus, you can easily lose information.

- Access to data held on MannionDaniels information systems must be minimized by restricting physical access to the office buildings.
- Access to buildings is restricted by ensuring that security 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.
- 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.

6.2 Computer Security

- To avoid virus infection, always keep software up to date, and ensure you have anti-virus protection.
- When you're using your computer, you may see pop-ups asking you to install a new piece of software, accept a download, or similar. Stop and assess what you're being asked to do -if you say no now, you can always change your mind later.
- If you are using a laptop or desktop to store or share confidential or restricted data, it must be encrypted in case of loss or theft.
- Do not store confidential or restricted data on a tablet or phone.
- All devices must be protected by a password or PIN (if applicable)

6.2.1 Data Storage

- All information related to MannionDaniels business is to be stored on Box.com and not on your disk or removable devices. This is a secure storage area which is regularly backed up with the necessary security protocols to ensure it is resilient to failure.
- If your data cannot be stored on Box.com then 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 and the Computer Misuse Act.
- 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.
- All data should be stored in accordance to its classification. When using Box.com always ensure that data is stored in a folder with access appropriate to its classification.

6.2.2 File Storage and Naming Conventions

- All documents and files should be given clear and descriptive titles that will help others to understand what is contained within them. All documents should have classification, a date and version number clearly included.
- 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.

6.2.3 Memory Sticks and removable media

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

6.2.4 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 four random unrelated words and stringing them together. See http://correcthorsebatterystaple.netfor 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 8characters, 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

6.2.5 Viruses

- All files received on removable media from outside MannionDaniels or received via e-mail must be checked for viruses before being used on MannionDaniels equipment.
- If a virus is suspected, please report this immediately. Any disks, CD ROMS, and USB memory sticks that have been used on the suspected infected workstation should be gathered together and not used.

6.2.6 3rd Party Network Connections

- All requests for external 3rd Party network connections must be authorised by MannionDaniels and strictly governed by relevant standards and approval process. MannionDaniels equipment.

6.3 WiFi usage

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

MannionDaniels Staff and Guest WiFi networks

- Staff WiFi access must only be granted to MannionDaniels staff.
- Guest WiFi access should be granted as required to trusted individuals.
- WiFi access passwords must be changed as directed by the senior management team.
- WiFi access passwords must be changed if a security incident has occurred involving people or devices that have had access to the MannionDaniels WiFi network.
- Guest WiFi 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 WiFi access points must be set to only allow WPA2-AES security protocol

Public WiFi networks

Public WiFi is inherently insecure so treat all links with suspicion.

- Try to verify that it's a legitimate connection as cybercriminals may have set up access points with similar names to the hotel or coffee shop you are currently attempting to connect to. An employee at the location may be able to supply information to help with this.
- Consider tethering to your mobile phone instead of using the WiFi.
- Don't access any websites or services that require a password if connected to public WiFi.
- Don't access any confidential or restricted data from Box.com if connected to public WiFi.

6.4 Encryption

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

General

Data that is classified as confidential or restricted should be encrypted.

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, Bitlocker 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

6.5 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

- Manual files processed outside of the MannionDaniels property must be kept with the individual completing this work.
- When left unattended, manual files must be in a locked container and out of view.
- Computer equipment or manual files that are travelling with an employee must always be locked in the boot of the car or kept with the individual when travelling by public transport.
- 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.
- Security lock and pin protection must be used where available to protect the device and any stored data.
- Smart phone devices must be protected with a password.
- Box.com must not be used on a phone or tablet
- Disable WiFi and Bluetooth when not in use.

6.6 Unacceptable Use

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The MannionDaniels network 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 the University 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.

6.7 Blogging & 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.

Social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes e-mail, online social forums, blogs, video-and image-sharing websites and similar facilities. Employees should follow these guidelines in relation to any social media that they use.

1. Be transparent and state that you work at MannionDaniels. If you are writing about MannionDaniels, use your real name, identify that you work for MannionDaniels, and be clear about your role. If you have a vested interest in what you are discussing, be the first to say so.
2. Never represent yourself or MannionDaniels in a false or misleading way. All statements must be true and not misleading; all claims must be substantiated.
3. Post meaningful, respectful comments —no spam and no remarks that are off-topic or offensive.
4. Use common sense and common courtesy: for example, it's best to ask permission to publish or report on conversations that are meant to be private or internal to MannionDaniels. Make sure your efforts to be transparent don't violate MannionDaniels' privacy, confidentiality, and legal guidelines for external commercial speech.
5. Stick to your area of expertise and do feel free to provide unique, individual perspectives on non-confidential activities at MannionDaniels.
6. 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;
7. 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.
8. 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.

6.8 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 mail accounts nor attempt to impersonate someone else or appear anonymous when sending e-mail.
- All e-mails should be finished with an e-mail signature that includes your name, title, service and contact details.
- Encryption should be used when an e-mail needs to be sent securely.

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, hoax 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.

Attachments

- Attachments should not be included in any internal mails or meeting invites, wherever it is possible links to documents should be used instead.

6.9 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.

6.10 Security Incident Reporting

The management of information security incidents in a prompt and appropriate manner will enable MannionDaniels to efficiently mitigate the risks and any legal implications that may be associated with information security incidents. 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, provider or delivery partners.

|For example, an incident could be: A virus or malware infection, sending confidential or restricted data via email without encryption, sending an unsolicited email to a recipient without their prior consent, etc.

- Information security incidents must be reported immediately.
- Loss of any piece of ICT equipment (computer, laptop, mobile phone, USB storage device, etc), is classed as a security incident and must be reported.
- Information security incidents should be reported via the Data Breach Log on box. command by calling the Director or Operations and the Senior Digital Manager.

Appendix A REFERENCES

Legal references (This is not an exhaustive list)

- Data Protection Act 1998
- 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

Regulations - HM Government

- The Security Policy Framework
- The Government Security Classification Policy
- HMG Information Assurance Standards