Version	Date	Modified by	Description
0.1	15/5/24	Cazz Ward	First Draft
	10/11/24	Adrian Ball	Published

Information Security Policy

1. Purpose

The purpose of this policy is to establish the requirements for maintaining the security and confidentiality of information, information systems, applications and networks owned or held by Manchester Settlement and protect its information assets from security threats that may have an adverse impact on the organisation.

It covers security which should be applied through technology but also encompasses the required behaviour of people in relation to the information they are responsible for.

2. Information security objectives

The objectives of the information security management system are:

- To provide the necessary policies, procedures and governance structure that will protect Manchester Settlement's information assets from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met
- To ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents
- To preserve the appropriate level of confidentiality, integrity and availability of Manchester Settlement's information assets and critical activities

These terms are further defined below:

- **Availability:** Information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and Manchester Settlement must be able to respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans in place

- **Confidentiality:** Information should only be accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to Manchester Settlement's information assets and its systems

- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods, and therefore preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency and data backup plans and security incident reporting. Manchester Settlement must comply with all relevant data-related legislation in those jurisdictions within which it operates

Controls shall be commensurate with the risks faced by Manchester Settlement.

3. Information security principles

The following principles underpin this policy:

- Information will be protected in line with all relevant Manchester Settlement policies
- It is the responsibility of all individuals to be mindful of the need for information security and to be aware of and comply with this policy including sub-policies and all current and relevant UK and EU legislation
- Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset
- All information assets will be classified according to a level of risk
- Information will be protected against unauthorised access and made available solely to those who have a legitimate need for access, applying a principle of least privilege
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification

4. Scope

The policy applies to all Manchester Settlement employees. The term "Employee" also includes those who work on a non-permanent basis, including volunteers, independent contractors, consultants, trustees, students, professional advisors and other third parties engaged to carry out work for Manchester Settlement and who have access to our premises or our internal systems. This categorisation is for convenience and does not demonstrate any particular employee, worker or other status.

5. Policy statement

It is the responsibility of every employee member to ensure that they have read and understood this document in order to safeguard the organisation's information assets and systems. This policy applies regardless of whether the user is office based or working remotely.

The use of the Manchester Settlement's information assets and information systems indicates acceptance of this Information Security Policy.

6. Roles and responsibilities

Chief Executive Officer
The Chief Executive Officer has overall responsibility for information security.

They are responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure Manchester Settlement's systems, assets and infrastructure have adequate security measures to comply with data protection and data security legislations and regulations.

They collaborate with the National Cyber Security Centre on matters relating to incident reporting,

All employees
All employees are responsible for information security and therefore must understand and comply with this policy and associated policies and guidance. All staff will receive information security awareness training and more specialised staff will receive appropriately specialised information security training.

Contractors and third parties
Contractors and third parties are also required to comply with this framework, associated policies and business-level operational procedures and to report any incidents. All third parties must undergo a process of due diligence before being given access to our information assets and systems or processing data on our behalf.

7. Information Risk Framework

The information security risk management process is integrated into the business risk management process. All information assets and risks are maintained in the Information Risk Register. Where the risk rating exceeds the threshold score of 20 this is then fed into the Charity Risk Register in line with the thresholds set out in Manchester Settlement's Risk Management Policy. Roles and responsibilities are set out as follows:

- **Chief Executive Office**r: Responsible for ensuring risks are assessed and mitigated to an acceptable level. Provides focus on information risks at board level with assurance they are being managed
- **Board:** Monitors the management of information risks that exceed the risk threshold score and satisfies itself that less significant risks are being managed

8. Confidentiality

It is vital that confidentiality requirements are complied with to prevent breaches of data protection legislation and potential legal claims as well as loss of Manchester Settlement's proprietary information and intellectual property.

- Confidential or personal information must not be disclosed to persons outside of Manchester Settlement without the prior written authorisation of the Chief Executive Officer.
- NDAs and/or Data Sharing Agreements including confidentiality provisions should be entered into as necessary, prior to the sharing of confidential or personal information outside Manchester Settlement
- Confidential information must not be stored outside of Manchester Settlement systems and/or network or on personal devices e.g. USBs and other removable media, personal email accounts or hard drives of non company devices. It should also not be stored within WhatsApp.
- Access to confidential information should be restricted to employees on a need to know basis.
- When sharing confidential information, employees must be mindful of the consequences should the data be lost or stolen. Additional protection, such as encryption or passwords, should be applied wherever technically feasible. Where confidential information does need to be shared externally, secure file transfer methods should be used.

9. Asset management and disposal

All company owned hardware and software assets are procured and managed by Greenlight Computers Ltd. They will maintain an asset inventory and ensure that all assets are identified, owned, registered and physically protected from threats.

Employees are responsible for protecting any equipment they have been supplied with and ensuring it is not left unattended and is always locked away and out of sight when not in use.

On termination of employment or when an employee no longer requires an asset, it must be returned to your team manager in order that it can be securely stored, data wiped, the asset inventory updated and the asset can be reassigned as required.

All user data should be deleted from Manchester Settlement systems according to the agreed retention schedules or at user request, so far as is reasonably practicable or unless Manchester Settlement is required to retain for compliance with applicable laws or regulatory requirements.

10. Mobile devices/BYOD

Employees have a responsibility to employ reasonable security measures to prevent theft, loss or damage to devices.

Manchester Settlement acknowledges that employees may occasionally use their own devices for work. Employees are expected to adhere to the same security protocols when connected to non-company equipment.

The following measures must be applied:

- Prevent theft and loss of data (using biometric/PIN/strong password/passphrase lock)
- Keep information confidential, where appropriate
- Maintain the integrity of data and information
- Activate and use encryption services and anti-malware protection
- Device use software and operating systems that have active security support and updates and patches are applied as soon as possible and no later than 14 days from release
- Allow Manchester Settlement to install and configure tracking and remote wipe services if required
- Remove any Manchester Settlement information stored on the device once they have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets
- Remove all Manchester Settlement information from the device and return it to the manufacturers' settings before selling, exchanging or disposing of the device
- Where personal data is being processed, comply with the principles of data protection legislation

Employees agree to Manchester Settlement monitoring compliance with the above measures and potentially wiping data from the device in the case of a loss or breach of the device where company data is at risk.

11. Management of removable media

Removable media, such as USB memory sticks and SD cards, are particularly vulnerable to loss or theft. Care must be taken with the use of any removable media for storage of data classified as confidential, such as sensitive or personal data, as they may not provide adequate protection.

Removal media should only be used where there is no other secure method of transferring data and where the employee role permits this. If it is necessary to use removal media, then the data must be securely encrypted and/or password protected.

All media should be stored in a safe, secure environment when not in use.

Once transferred, the data should be deleted from the removable media. On termination of employment, data should be deleted or the media returned.

12. Access control

Access to information and systems should be controlled and restricted to those authorised users who have a legitimate business need. Authorisation should be granted by the Chief Executive Officer.

An audit trail of system access and employee data use is maintained and reviewed on a regular basis. Manchester Settlement reserves the right to monitor activity where it suspects there has been a breach of policy.

Generic identities or user accounts should not be used to access Manchester Settlement information assets and systems, unless agreed by the Chief Executive Officer and in exceptional circumstances. Using unique user accounts enables users to be linked to and held responsible for their actions.

Employee accounts should only be created, changed or removed according to the documented Starter and Leaver process.

All third party access must be requested via Chief Executive Officer. All third parties must have a signed contract, and where appropriate a data sharing agreement in place before access is granted.

Administrator and special privilege accounts will only be granted to those users who require such access to perform their job function. Administrator accounts must be strictly controlled, and their use will be logged, monitored and regularly reviewed. High privileged or administrator accounts should not be used for day to day activities in the course of normal business operations, such as accessing external email or browsing the internet.

13. Password protection

Passwords are an important aspect of computer security in preventing unauthorised access and/or exploitation of the organisation's resources. All employees with access to information assets and systems are responsible for taking the appropriate steps to select and secure their passwords.

The following principles are applied in password management:

- Where possible, single sign on will be used to minimise the number of passwords an employee needs to remember
- Multi factor authentication will always be used when account authentication takes place and systems support it
- Regular password expiry will not be enforced. Whilst all systems will be password protected, technical controls and security monitoring will be used to protect our systems rather than relying on passwords
- Passwords must be changed immediately upon issuance for the first use
- Passwords must never be stored in clear, readable format (encryption must always be used)
- Common passwords, such as a pet's name, common keyboard patterns or passwords that have been have used elsewhere should not be used

14. Protection from malicious software

Manchester Settlement implements procedures, user awareness, and change controls to detect and prevent the introduction of malicious software. Employees are responsible for ensuring anti-virus and anti-malware software is installed on BYOD devices to protect against computer viruses. Employees are responsible for ensuring that software is kept up to date and should regularly check for and proactively installing updates within 14 days.

All company devices are protected against malware and viruses, and technical controls are in place to detect and remove threats that may be transferred by email or through internet browsers.

All employees receive training on virus, malware and phishing attack awareness and control procedures.

15. Business continuity

In the event of a disruption to business-critical technology services, processes are in place to ensure that those information assets or systems are recoverable to the right level and within the right timeframe to deliver a return to normal operations, with minimal impact on the business. Refer to Business Continuity Policy (Technology).

16. Security incident reporting

It is the responsibility of each employee to report any suspicious activity or incident as quickly as possible to the Chief Executive Officer, or to a member of SMT if the CEO is not available. All breaches of information security or data, actual or suspected, shall be reported and investigated.

Where the breach involves personal data, the Personal Data Breach Notification Procedure should be referenced.

The Chief Executive Officer will co-ordinate the investigation and will manage Manchester Settlement's response in a timely manner and according to the procedure set out in the Business Continuity and Backup Plan. They will document all relevant issues identified and containment actions taken.

Where relevant, the Chief Executive Officer will work with Greenlight Computers Ltd and/or the response line and incident manager from their cyber insurance company to investigate:

Whether a genuine information security or data breach has occurred
If so, the nature and cause of that breach and the sensitivity of the affected information
Where personal data may have been affected, the identity of the data controller (if not Manchester Settlement), the number of individuals affected and the possibility of harm or distress caused to individuals. In this case, reference should be made to the process in the Personal Data Breach Notification Procedure
The risk involved
If necessary, whether any back-ups of the data exist and, if so, how easily Manchester Settlement can recover the data
Whether to inform or consult any external third parties to contain the risk or limit potential harm (such as external lawyers, IT forensics experts, regulators, the police, individuals, insurers or financial institutions)
The Chief Executive Officer will only involve and inform people who need to be informed and share information about the breach on a need-to-know basis and with appropriate confidentiality and data protection measures in place (such as Non-Disclosure Agreements or Data Processing Agreements)

Where the Chief Executive Office establishes that a genuine information security or data breach has occurred, it will promptly draw up and implement a plan to contain it and mitigate actual or potential harm that may happen as a consequence, including an appropriate communication plan. Where a notifiable personal data breach has occurred, Manchester Settlement will inform the Information Commissioner's Office within 72 hours.

17. Supplier relationships

All contracts and relationships with suppliers should ensure that acceptable levels of information security compliance are in place to protect Manchester Settlement information. Expectations will differ depending on the nature of information being shared and any known risks to that information.

All parties who are given access to Manchester Settlement systems, whether supplier, contractor or otherwise, must agree to follow Manchester Settlement information security policies or demonstrate that their own are functionally equivalent. A signed non-disclosure agreement, data processing agreement or contract must be in place before information is shared or processed. Where the employee is required to disclose personal data, a data sharing agreement must be in place. Where a supplier provides or supports a technology system, they must have relevant cyber security accreditation in place such as ISO 27001 or Cyber Essentials Plus

All contracts must be reviewed before renewal.

18. Other policies

This policy should be considered in conjunction with other policies and documents that form part of Manchester Settlement's information risk management framework including:

- Data Protection Policy
- Appropriate Policy Document

- Privacy Notices
- Record of Personal Data Processing and Retention
- Confidentiality Policy
- Acceptable Use Policy
- Personal Data Breach Notification Procedure
- Business Continuity and Backup Plan
- Risk Management Policy
- Information Risk Register
- Non Corporate Communications Channels Policy