version control: 08/2022

Information Security Policy

1. Introduction

1.1. UK GDPR and the Data Protection Act 2018 contain key provisions which all organisations that process people's personal data, such as The Midcounties Co-operative ("**the Society**"), must comply with.

1.2. Such provisions mean that:

1.2.1. the Society must have in place appropriate organisational and technical measures to ensure that the security and privacy of people's personal data are embedded into the lifecycle of its products, services, applications, and business and technical procedures. This is known as *privacy by design*;

1.2.2. only necessary personal data is collected, stored or processed; and personal data is not accessible to an indefinite number of people, but instead access to personal data is granted on a need-to-know basis. This is known as *privacy by default*.

1.3. *Privacy by design* and *privacy by default* are key principles underlying data protection legislation.

2. Objectives

2.1. The objectives of this Policy are to:

2.1.1. Provide a framework for establishing suitable levels of information security for the Society's information systems and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

2.1.2. Ensure that all colleagues, suppliers, third party processors, contractors, agency workers, temporary staff and any other authorised users processing personal data on behalf of the Society (the "**Authorised Users**") are aware of, and comply with, this Policy and all applicable legislation.

2.1.3. Provide the principles by which a safe and secure information systems working environment can be established for Authorised Users.

2.1.4. Ensure that Authorised Users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

2.1.5. Protect the Society from liability or damage through the misuse of its IT facilities.

2.1.6. Maintain research data and other confidential information provided by suppliers and other third parties at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

2.1.7. Respond to changes in the context of the Society as appropriate, and to implement improved security and organisational measures as and when required.

2.2. This Policy should be read in conjunction with other applicable Society's policies and procedures, particularly the **Acceptable Use of IT Facilities Policy** and the **Data Protection Policy**.

3. Scope

3.1. This Policy is applicable to all Authorised Users, which include the Board of directors and the Executive management.

The scope of this Policy includes, but is not limited to:

3.1.1. cloud systems developed or commissioned by the Society
3.1.2. any systems attached to the Society's data or telephone networks
3.1.3. any other systems managed by the Society
3.1.4. mobile devices used to connect to the Society's networks
3.1.5. data over which the Society holds the intellectual property rights
3.1.6. data for which the Society is the data controller or the data processor
3.1.7. any electronic communications sent/received within the Society's IT environment.

4. Information Security Principles

4.1. The following information security principles provide overarching governance for the security and management of information within the Society:

4.1.1. Information will be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements.

4.1.2. Authorised Users will handle information in accordance with its classification level, and will comply with any contractual requirements, policies, procedures or systems put in place by the Society to meet those responsibilities.

4.1.3. Information will be both secure and available to those with a legitimate need for access in accordance with its classification level. Therefore, access to information will be assigned to Authorised Users on a *need-to-know* basis.

5. Legal and Regulatory Obligations

5.1. The Society has an obligation to comply with all applicable legislation in relation to data security, as well as with a variety of regulatory and contractual requirements applicable to its business groups.

5.2. All Authorised Users are responsible for ensuring the Society remains compliant by adhering to policies, procedures and guidance documents, which may detail other applicable requirements or provide further detail on the Society's obligations.

6. Suppliers, Cloud Providers and Third-Party Processors

6.1. All Society's suppliers, Cloud providers and third-party processors will abide by this Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. It is the responsibility of the Society, as data controller, to seek such assurance and ensure it is adequate.

6.2. The Society retains responsibility, as the data controller, for any personal data it shares or grants access to, and can consequently be fined for any personal data breach that may occur even when the service provider, supplier or third party processor is at fault, the consequences of which would be detrimental to the Society from a financial, commercial and reputational point of view.

6.3. Each business area within the Society will ensure that adequate data sharing agreements are in place with all its suppliers and third-party processors, where adequate means that the agreement contains all the required clauses to be compliant with applicable legislation in relation to the processing of people's personal data.

6.4. Business areas are responsible for maintaining adequate record-keeping of the agreements in place with their suppliers and third-party processors, to ensure these are regularly reviewed and updated as and when necessary.

6.5. The Society's legal team (legal@midcounties.coop) can provide business groups with a full template agreement, or with the relevant additional clauses to be added, as an Addendum, to existing data sharing agreements.

7. Compliance, Policy Awareness and Disciplinary Procedures

7.1. Any data security breach of the Society's information systems could lead to the loss of confidentiality, integrity and availability of personal data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the GDPR and contravenes the Society's applicable policies.

7.2. All Authorised Users will be informed of the existence of this Policy and the availability of other supporting policies, procedures and guidelines.

7.3. Colleagues must be aware that any breach will be handled by the Society's management in accordance with all relevant policies, including the Acceptable Use of IT Facilities Policy. Depending on the level of risk to which a breach may expose the Society, and the circumstances surrounding the breach, a disciplinary process may be initiated.

7.4. Any breaches of this Policy must be reported to the Society's Data Protection Manager ("**DPM**")[1] without delay.

7.5. Personal data breaches will be reported to the Information Commissioner's Office ("**ICO**"), where applicable, by the Society's DPM.

8. Access Rights to Personal Data

[1] The GDPR introduced an obligation, for certain organisations, to formally appoint a Data Protection Officer (DPO) depending on a number of criteria. Within the Society, this requirement is applicable to the Healthcare business. The DPO role for that business is held by the Society's Data Protection Manager (DPM).

8.1. The Society will monitor unnecessary system privileges or data access rights where the impact of misuse or compromise of personal data could result in a data breach.

8.2. The Society operates a policy of “least privilege”. That means Authorised Users will be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges will be carefully controlled and managed to ensure access privileges are assigned on a *need-to-know* basis.

8.3. Each of the Society’s business group is responsible to control and manage its staff’s access privileges. Failure to effectively manage such privileges could result in several risks:

8.3.1. **Misuse of privileges**: Authorised Users could either accidentally or deliberately misuse the privileges assigned to them. This may result in unauthorised access to personal data to either the Authorised User or a third party, or to unauthorised system changes having a direct security or operational impact on the Society.

8.3.2. **Increased attacker capability**: Attackers may use redundant or compromised Authorised Users’ accounts to carry out cyberattacks on the Society’s systems and, if able, they may return to reuse the compromised account, or possibly sell access to others. The system privileges provided to the original Authorised User of the compromised account will be available to the attacker to gain access to highly privileged or administrative data within the Society’s systems and servers.

8.3.3. **Negating established security controls**: Where attackers have privileged system access, they may make changes to security controls to enable further or future cyberattack or might attempt to cover their tracks by making changes to audit logs.

8.4. The Society will:

8.4.1. Establish effective account management processes to manage Authorised Users’ accounts from creation through-life, and to revoke access privileges when a member of staff leaves or changes role.

Redundant accounts, eg. provided for temporary staff or for testing, should be removed or suspended when no longer required.

8.4.2. Establish policies and standards for user authentication and access control, through the implementation of corporate passwords and, where necessary, an additional authentication factor.

8.4.3. Limit access privileges of Authorised Users to the reasonable minimum rights and permissions to systems, services and information that they need to fulfil their business role, or tasks, for and on behalf of the Society.

8.4.4. Strictly control the granting of highly privileged system rights, reviewing the on-going needs regularly. Highly privileged administrative accounts must not be used for high risk or day-to-day Authorised Users' activities, for example web browsing and e-mail monitoring.

8.4.5. Monitor Authorised Users' activity and the use of privileged account actions, and respond where activities are outside of normal, expected bounds, for example access to large amounts of personal data outside of standard working hours.

8.4.6. Limit access to activity logs from network devices, and ensure such logs are sent to a dedicated accounting and audit system that is separated from the core network. Access to the audit system and the logs must be strictly controlled to preserve the integrity of the content and all privileged user access recorded.

8.5. No individual should be able to access personal data to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual must knowingly contravene this Policy, nor allow others to do so.

9. Ownership and Responsibilities

9.1. While the Society retains ultimate responsibility, as the data controller, for any personal data it shares or grants access to, different levels of ownership and responsibility rest with its management, who holds specific or overarching responsibilities for preserving the confidentiality, integrity and availability of personal data.

9.1.1. **Executive Management's responsibilities** – each business group owns the personal data it processes. As such, the relevant Executive is ultimately responsible for the security of its business' data and, through delegation to their line management, for ensuring that:

- personal data is appropriately stored;
- the risks to personal data are fully understood by any Authorised User within their business area, and either mitigated or explicitly accepted;
- the correct access rights have been put in place, with personal data only accessible to the relevant Authorised Users; and
- appropriate backup, retention, disaster recovery and disposal mechanisms in place.

9.1.2. **DPM's responsibilities** – The DPM is responsible for the oversight of the Society's compliance with applicable legislation in relation to the processing of personal data. Specifically, the DPM:

- Monitors specific processes, such as data protection impact assessments (DPIAs), processing and retention & disposal records, data breach reporting and completion of individual rights requests
- Increases employees' awareness for data protection and puts in place adequate training tools and guidance papers
- Collaborates with the supervisory authorities (in the UK, the ICO) in the course of investigations.

Notwithstanding the DPM's monitoring function, the DPM isn't it personally liable for data protection compliance. The Society, as the data controller, remains responsible for complying with data protection laws and ensuring all its third-party data processors are equally compliant.

The DPM plays a crucial role in helping the Society to fulfil its data protection obligations, so the DPM must be involved in all issues which relate to the protection of personal data within the Society.

9.1.3. **Line Management's responsibilities** - In accordance with the directions established by the Society's policies and procedures, and with oversight from the Executive, line management is responsible for specific area of the Society's work, for example to produce supporting information and documentation that may include working documents/contracts etc. containing colleagues', members', customers or other parties' personal data the business area processes to carry out its functions.

Line management, as Authorised Users, must comply with the relevant Society's policies and procedures when processing data, particularly personal data, and ensure this is always adequately safeguarded.

9.1.4. **IT Management's responsibilities** – Information security management is understood as tool of the information confidentiality, availability and integrity assurance. An effective information security management system reduces the risk of crisis occurring within the Society, and in turn reduces the potential adverse effects of crisis happening outside the Society's IT environment.

- Create and manage the Society's information security strategies.
- Oversee information security audits, whether performed in-house or via third-parties.
- Manage the Society's security team members and other relevant information security personnel, providing adequate training during onboarding and evaluating the department's budget and costs associated with required training.
- Assess current technology architecture for vulnerabilities, weaknesses and for possible upgrades or improvement.
- Implement and oversee technological upgrades, improvements and major changes to the Society's information security environment.
- Serve as a focal point of contact for the information security teams, as well as the Society's wider management and personnel.
- Manage and configure physical security of relevant locations within the Society's premises, disaster recovery and data backup systems.
- Communicate information security goals and new programmes effectively with the wider Society's management and the Board of directors, as necessary.

10. Information classification

10.1. In order to comply with its information security obligations, the Society has adopted the use of Azure Information Protection ("**AIP**") within its IT environment. AIP is a cloud-based solution to help the Society classify and protect its documents and emails by applying labels, pre-defined with rules and conditions.

10.2. When documents and emails are classified and protected, its use can be tracked and controlled, data flows can be analysed to gain insight into the use of information across the Society, risky behaviours can be detected to allow for corrective actions to be put in place, and access to data can be monitored to prevent data leakage or misuse.

10.3. This protection technology uses encryption, identity, and authorisation policies. Similarly, to the labels that are applied, protection stays with the documents and emails, independently of their location - inside or outside the Society, networks, file servers and applications, and whether it is shared with other parties.

10.4. The following policies are applied by the Society:

Public	Protection Rule: No Action
	General Protection Rule: Rule does not apply External/Internal
	Criteria: Anything
General	E-mail is logged External/Internal
Confidential	Protection Rule: External/Internal
	Criteria: Credit Card Driving Licence NI Number
	Formatting Rule: Apply Confidential Header
Highly Confidential	Protection Rule: Internal Only - No Offline Access - Authentication Required - with bypass available (override option for e-mails only)

	Criteria: 'Highly Confidential' “Strictly confidential”, “Strictly private and confidential”
	Formatting Rule: Apply Watermark

10.5. These policies will be reviewed from time to time, to ensure they remain aligned with the Society’s business needs, and in compliance with the information security requirements imposed on the Society by relevant laws and regulations.

11. Who to contact?

11.1. Each business group has a Data Protection Champions (DPC). A list of DPCs and contact details is available on colleagues connect.

11.2. The Society’s DPM/DPO can be contacted by email: data-protection@midcounties.coop; and by post: The Midcounties Co-operative, Co-operative House, Warwick Technology Park, Warwick CV34 6DA.

12. Changes to this Policy

12.1. This Policy will be reviewed by the Society’s DPM, working alongside IT management, and updated regularly to ensure that it remains appropriate in the light of any relevant changes to laws, organisational policies or contractual obligations.