Data Protection Policy

Safe Well Led

Document title	Data Protection Policy		
Version	**Date**	**Updated By**	**Comments**
1.0	1/8/19	V. Perrins	First Issue
2.0			
3.0			
4.0			
5.0			

Data Protection Policy Summary

The Data Protection Policy describes the values and principles underpinning the MioCare Group approach to Data Protection. This includes:

- Key data protection obligations and accountabilities
- Definitions of personal and special data
- Six data protection principles
- Roles and Responsibilities

The Companies policies and procedures are to be used within the employee performance framework which will enable the Companies to deliver the best outcomes for those who use our services, and help ensure compliance with the CQC regulatory requirements of providing a safe, effective, caring, well-led and responsive service.

The Care Quality Commission (CQC) is the independent regulator of health and adult social care in England. They monitor, inspect and regulate services to make sure they meet a specific standard of quality and safety. There are five key areas of work that are examined when the CQC carry out an inspection, these are

- Is the service 'safe'?
- Is the service 'effective'?
- Is the service 'caring'?
- Is the service 'responsive to people's needs'?
- Is the service 'well led'?

When considering the five areas above, inspectors will gather and examine various sources of information including discussions with people who use our services and discussions with the staff that deliver our services. It is important that all our policy & procedures support the key areas of examination and that staff are aware of, and comply with Company policies and procedures.

1. Objectives

MioCare Group recognises the need for legal compliance and accountability and endorses the importance of the integrity, availability, and confidentiality and security arrangements to safeguard personal data. We also recognise that there are times that personal data is shared with, and/or received from, other organisations and that this needs to be in accordance with the law.

This policy sets out the key data protection obligations and accountability to which we are fully committed.

2. Scope

In order to fulfil our statutory and operational obligations, MioCare Group is required to collect, use, receive and share personal and special personal data about living people. Examples include

- People who use our services (and their families and carers)
- Current, past and prospective employees
- Elected Members
- Contractors and suppliers

This policy covers all aspects of handling personal data, regardless of age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

This policy reflects the commitment to data protection compliance to both UK and EU legislation, in particular the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR) and the EU Law Enforcement Directive 2016 (LED). In addition, for those working in health and social care there is an obligation to follow the Caldicott Principles, National Data Guardian Standards and the law of confidentiality. These reflect and reinforce the data protection principles. (see Appendix I).

3. Policy

3.1 *Data Protection Officer (DPO)*

We will appoint a Data Protection Officer who will be the key contact for the provision of independent advice on matters relating to data protection. The DPO is ultimately responsible for ensuring that we are appropriately registered with the Information Commissioner's Office (ICO) and facilitating the mandatory Record of Processing Activities (ROPA), to be made available to the (ICO) upon demand.

3.2 Definitions of personal data:

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

In summary, anything and everything that can relate to a living person.

Special Personal data means *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*

In summary, these are the data categories that are subject to additional controls in order to prevent unauthorised collection, use, access etc.

Crime data means criminal offence data, e.g., alleged commission of offences or proceedings for an offence, (actual or alleged), including sentencing, other than where it is **USED** for Law Enforcement (LE) functions) by competent authorities within the scope of part 3 of the Data Protection Act 2018, i.e., statutory functions of the local authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

In summary this type of personal data is subject to specific conditions and controls.

Personal data for LE purposes means the processing of personal data in the local authority's own right for the *purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*

In summary, personal data used for this purpose is subject to specific data protection conditions and controls.

3.3 Data Protection Principles

There are 6 principles which provide the framework for personal data handling and for which the Council is accountable for compliance.

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner

To be lawful an appropriate condition of processing needs to be identified. To be fair and transparent a privacy notices needs to be provided/available to the data subject whose personal data is being handled (data subject) and the law specifies what information must be communicated

(b) processed for an explicit and specific purpose and not processed for other incompatible purposes. Scientific/historical/statistical research is not incompatible and nor is archiving in the public interest

Personal data should only be used other than for the stated lawful purposes, except where the law permits.

(c) adequate, relevant and limited to what is necessary for the purpose

Ensure that personal data is specific to the stated lawful purpose and is not excessive or unnecessary.

(d) accurate and, where necessary, kept up to date; ensuring that personal data that are inaccurate, are erased or rectified without delay

Ensure that personal data is correct and that any errors are rectified and where appropriate notified to recipients of the personal data.

(e) keep no longer than necessary for the purpose, but can keep for longer is solely for Scientific/historical/statistical research and archiving in the public interest purposes and is kept securely

Personal data should not be kept longer than necessary taking into account legal and operational requirements.

(f) protection of the personal data using appropriate technical or organisational measures

These measures should be selected on the basis of identified threats and risks to personal data and the potential impact on the data subjects, we and any third parties who are sources, recipients, or processors of the personal data.

3.4 Data Privacy Impact Assessments (DPIA)

These are an important vehicle in ensuring that we integrate data protection by design and default into our technical systems and day to day business operations by embedding privacy risk considerations into new and changes to systems and business processes. These privacy risk assessments must take place where there is a high risk to the privacy rights and freedoms of a data subject. Examples where these are likely to be required, include, but are not limited to, new systems and processes, new or different uses of personal data. Where a high risk is identified the DPO must be consulted before any new or changed processing is introduced to ensure adequate risk mitigation measures are implemented. Where risks are high and not adequately mitigated a referral to the Information Commissioner's Office (ICO) must be made.

3.5 Data Collection, use and disclosure

We handle personal data that has been either collected from the data subject and/or other parties, e.g. other people, public sector and regulatory organisations, private and voluntary sector organisations etc. We will:

- only handle personal data where there is a legal basis to do so.
- not unnecessarily rely on consent where an alternative legal basis is available for processing personal data. However, where consent/explicit consent, is the lawful basis, then we acknowledge that for consent to be valid it must be freely given and capable of being withdrawn. Where a particular individual is unable, due to age, capacity or other

reasons, to give consent directly, consent will be sought from an appropriate person e.g., parent, guardian, legal representative etc.

- only send promotional or marketing material with consent / or existing business relationship.
- provide data subjects with privacy notices that explain why the personal data is required and how to exercise their personal data rights.
- in the event of a personal data security breach, resulting in a high risk to the data subject(s), to notify the data subjects and / or the ICO as appropriate.
- in the event of a data subject exercising their personal data rights, we will assess the request and respond within the statutory timeline and provide a complaints process.
- ensure personal data is subject to appropriate retention and security controls taking into account the nature of the data and the information risks. Personal data may be stored for longer periods where it is for archiving in the public interest, historical or scientific research purposes, or as required by legislation or regulatory activity.
- ensure that when sharing and disclosing personal data this is undertaken within the parameters of the law to prevent unauthorised access to personal data. A record will be kept and where appropriate information sharing agreements (ISA) will developed in line with the ICO Data Sharing Code of practice. Where the sharing involves a joint controller relationship, the ISA will identify the lead controller responsible for specified processing activities and for managing individual rights. Where appropriate DPIA's will be undertaken in advance of the sharing/disclosure.
- when handling health and social care personal data, that the Caldicott Principles and National Data Guardian Standards are observed.
- when handling special category, crime conviction and offence data and data falling under the LE provisions in Part 3 of the DPA 2018, that we comply with the additional policy requirements necessary to support these particular processing activities in order to demonstrate compliance with the data protection principles and retention policies and ensure inclusion in the Records of Processing Activities (ROPA).
- ensure that processing of personal data within our supply chains includes the contractual clauses required by law and that processing is only undertaken in accordance with our instructions as data controller.
- not transfer personal data outside of the European Economic Area (EAA) to countries with lower data protection standards, unless the appropriate safeguards and controls are in place, i.e., a decision by the EU that the country has 'adequate' data protection legislation, that a company in the US is signatory to the EU/US privacy shield, binding corporate rules or model contract clauses in place, or the law prescribes this in defined circumstances.
- to co-operate and provide information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.

3.6 Offences

The data protection legislation contains specific offences:

3.6.1 It is an offence for a person knowingly or recklessly, without the consent of the data controller, to

- obtain or disclose personal data
- procure the disclosure of personal data to another person
- retain it without the consent of the original data controller

- offer to sell or buy the personal data obtained

.

3.6.2 It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller, or to knowingly or recklessly handle such data.

3.6.3 It is an offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject making the request for access or portability would have been entitled to receive.

3.6.4 It is an offence to require a data subject to provide or give access to information obtained via data subject access in relation to health, conviction/caution records for the purpose of recruitment, continued employment, in connection with provision of goods and service to the public. In summary a data subject should not be obliged to make a data subject access request for this type of information as a condition/implied condition of employment or contract.

3.6.5 It is an offence to intentionally obstruct or give false information to the ICO in the exercise of its powers under information notices and/or warrants.

4. Assessment and monitoring

4.1. An annual assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

4.2. Reports will be submitted to the Senior Management Team and Finance, Audit and Risk Committee.

5. Responsibilities and approvals

5.1. **The Senior Management Team** is responsible for ensuring that the necessary support and resources are available for the effective implementation of this policy.

5.2. **The Data Protection Officer** is responsible for the review and approval of this policy.

5.3. **The Finance, Audit and Risk Committee** is responsible for ensuring that our data protection policies and practice are effective and we are accountable.

5.4. **The Caldicott Guardian** will take a lead on confidentiality issues in relation to health and social care records.

5.5. **The Senior Information Risk Owner (SIRO)** has overall ownership of the Information Risk Policy. The SIRO is to act as champion for information risk at senior management and leadership boards and is responsible for providing written advice to the

Accounting Officer on the content of our Statement of Internal Control in regard to information risk. The SIRO is responsible for decisions in relation to any information issues or incidents.

5.6. **The Information Manager and Information Management Team** is responsible for providing specialist advice and support on all aspects of Information and Records Management and Governance.

5.7. **Employees.** All councillors and staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day to day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence.

6. Authority for this policy

This policy is owned by the Data Protection Officer on behalf of the Senior Information Risk Officer. This delegation is to establish and approve internal policies dealing with all aspects of the management of our information security, records and information governance.

7. Policy Governance

The following table identifies who is accountable and responsible with regards to this policy. The following definitions apply:

- accountable – the person who has ultimate accountability and authority for the policy.
- responsible - the person(s) responsible for developing and implementing the policy.

Accountable	Senior Information Risk Officer
Responsible	Data Protection Officer

Appendix I

Caldicott Principles

Principle 1 - Justify the purpose(s) for using confidential information
Principle 2 - Don't use personal confidential data unless it is absolutely necessary
Principle 3 - Use the minimum necessary personal confidential data
Principle 4 - Access to personal confidential data should be on a strict need-to-know basis
Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities
Principle 6 - Comply with the law
Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

National Data Guardian Standards

- Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes
- Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
- Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.
- Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to data subjects.
- Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
- Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
- Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
- Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.
- Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually. Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Please sign below to indicate that you have read and understood the contents of this policy

If you have any questions or queries about this policy document, please speak to your manager to ensure you understand the content before signing

Date	Print Name	Sign