Data Protection Policy

Version Control

Date	Version Number	Stage	Author
16th September 2014	1.0	Creation	Tim Crowson
30th October 2014	1.1	Review before presentation to Clinical Governance Group	Paul Haycox
5th November 2014	2.0	Inclusion of comments from Sharon Leach	Paul Haycox
29th March 2016	2.1	Change of IT manager	Paul Haycox and Jamie Darlington
26th August 2016	2.2	Minor changes and added reference to EU GDPR	Paul Haycox
19th January 2018	2.3	Reviewed in readiness for GDPR, but requires review in April 2018 when Information Alliance Guidance on GDPR and Data Protection Act 2018 is made available	Paul Haycox
4th May 2018	3.0	Amended Data Protection Principles in line with GDPR; amended the Roles and Responsibilities in line with the GDPR; inserted section on GDPR; amended employee responsibilities and monitoring section.	Paul Haycox
23rd May 2018	3.1	Name change. Addition regarding Privacy Notices	Paul Haycox
12th December 2019	4.0	Added detail regarding legal right for data processing, and roles and responsibilities	Paul Haycox
4th June 2021	4.1	Added national data opt out paragraph GDPR rights	Paul Haycox

Contents

1. Background

St Michael's Clinic needs to collect personal information about people with whom it deals to carry out its business and provide its services.

Such people include patients, employees (present, past and prospective), suppliers and other business contacts.

The information includes personal data and at times special categories of information. We may occasionally be required to collect and use certain types of such information to comply with the requirements of the law.

No matter how it is collected, recorded and used (e.g. on a computer or on paper) the clinic will seek to make it transparent to individuals

- what is held,
- how it is used,
- who else has access
- the individuals rights
- the legal basis for processing and
- to keep the data as securely as possible

and ensure compliance with the General Data Regulation and Data Protection Act 2018 (the Act).

The lawful and proper treatment of personal information by St Michael's Clinic is extremely important to the success of our business and to maintain the confidence of our service users and employees. We ensure that the St Michael's Clinic treats personal information lawfully and correctly.

2. Data Protection Principles

St Michael's Clinic fully supports and complies with the principles of the GDPR and 2018 Act which are summarised below:

Personal data shall be processed fairly and lawfully and in a transparent manner in relation to the data subject.

Personal data shall be collected for specific, explicit and legitimate purposes.

Personal data held must be adequate, relevant and limited to what is necessary.

Personal data must be accurate and kept up to date. Every reasonable strep will be taken to ensure that personal data that is inaccurate is rectified. Request for personal data to be erased will be considered in line with the reason for which that data is held.

Personal data shall not be kept in a form which permits identification of data subjects for longer than necessary and in accordance with national retention schedule guidance.

Personal data must be kept secure and will be protected with appropriate technical and/or organisational measures.

Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

We uphold the personal data rights outlined in the GDPR;

The right to be informed

The right of access

The right to rectification

The right to erasure

The right to restrict processing

The right to data portability

The right to object

Rights in relation to automated decision making and profiling.

We acknowledge our accountability in ensuring that personal data shall be:

Processed lawfully, fairly and in a transparent manner;

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Accurate and kept up to date;

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

Processed in a manner that ensures appropriate security of the personal data.

3. Underpinning Policies and Procedures

This policy is underpinned by the following:

Data Quality Policy – outlines procedures to ensure the accuracy of records and correction of errors.

Confidentiality Policy – details transparent procedures, the management of records from creation to disposal, information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share.

Information Systems Security Policy – outlines procedures for ensuring the security of data and staff responsibilities.

Business Continuity Plan – outline the procedures in the event of a security failure of disaster affecting digital systems or mass loss of information necessary to the day to day running of our organisation.

Staff Data Security Code of Conduct – provides staff with clear guidance on the disclosure of personal information.

4. The General Data Protection Regulation 2018 and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 makes it incumbent on the Data Controller to be able demonstrate compliance with them.

The clinic will evidence compliance with the data protection principles in section 2 through the use of policies, procedures, assessments and plans. These will be held in the Data Protection and Security Toolkit (DSPT), which is updated annually. The responsibility for updating the DSPT will fall to the Data Controller, IT Manager and Business Manager.

The clinic processes special category data, particularly data relating to health. Data concerning health' means personal data related to the physical or mental health of

a natural person, including the provision of health care services, which reveal information about his or her health status.

Health data can therefore include a wide range of personal data, for example:

- any information on injury, disease, disability or disease risk, including medical history, medical opinions, diagnosis and clinical treatment;
- medical examination data, test results, data from medical devices, or data from fitness trackers;
- information collected from the individual when they register for health services or access treatment;
- appointment details, reminders and invoices which tell you something about the health of the individual. These fall under 'the provision of health care services' but must reveal something about a person's health status. For example, a GP or hospital appointment in isolation will not tell you anything about a person's health as it may be a check-up or screening appointment. However, you could reasonably infer health data from an individual's list of appointments at an osteopath clinic or from an invoice for a series of physiotherapy sessions; and
- a number, symbol or other identifier assigned to an individual to uniquely identify them for health purposes (e.g. an NHS number, or Community Health Index (CHI) number in Scotland), if combined with information revealing something about the state of their health.

The clinic processes data under the GDPR Article 9 (2) (h) condition of health and social care

"processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".

and the Data Protection Act Schedule 1, condition 2

"the provision of healthcare"

Article 9(3) of the GDPR contains the additional safeguard that you can only rely on this condition if the personal data is being processed by (or under the responsibility of) a professional who is subject to an obligation of professional secrecy. Section 11 of the DPA 2018 makes it clear that in the UK this includes:

(a) a health professional or a social work professional;

Where a health professional includes in its definition doctors and nurses

The clinic has issued a Privacy Notice for both patients and staff members, which outlines the legal basis for processing the data, access to personal data, the individuals rights and contact details for the Data Protection Officer (dpo@stmichaelssclinic.co.uk)

The clinic will continue to assess any guidance and clarification of the law in 2019/20. Any significant guidance will be implemented, and processes, policies, procedures and reporting refined in line with the developing understanding and interpretation of the GDPR and Data Protection Act 2018.

5. Scope

All St Michael's Clinic staff are within the scope of this document, including contractors, temporary staff, secondees and all permanent employees.

6. Roles and Responsibilities

St Michael's Clinic will: -

Ensure that there is always one person with overall responsibility for data protection and appoint a Data Controller. Currently this is Dr Stephen Murdoch. He has overall accountability for establishing and maintaining a safe and effective data management system that adheres to all statutory and regulatory guidelines.

Ensure all types of data held by the clinic is understood and logged.

Ensure all data flows are mapped.

Ensure all data is processed lawfully, with a lawful basis of processing documented and communicated.

Have methods by which the rights of individuals in relation to data held by the clinic are informed to them. This will be through a clearly worded Privacy Notices. Privacy Notices will be referenced in all clinic letters for new appointments; will be displayed in the clinics reception area; be available on the clinics internet site and through paper copies held at the clinic. Employees will be notified of the relevant notice and it will be displayed in staff areas and available on the company's intranet.

Have a process for ensuring data subjects can access their data within the time frames required. This will include the ability to log and report on the numbers of requests. No barriers will be placed on people requesting data, other than ensuring that they are the relevant person who has a right to that data.

Have a process for ensuring the data held is up to date and accurate. Any inaccuracies brought to the attention of the clinic by data subjects are reviewed, rectified and/or erased (subject to the outcome of the review and the reason the data is held).

Have a process for restricting processing of data - at the request of an individual and subject to a review and the reason the data is held

Have a process for ceasing the processing of data - at the request of an individual and subject to a review and the reason the data is held

Appoints a Data Protection Officer to support the monitoring of compliance of the GDPR

Provide training for all staff members who handle personal information

Provide clear lines of report and supervision for compliance with data protection

Carry out regular checks to monitor current systems and to assess new processing of personal data.

To ensure a Data Protection Impact Assessment is undertaken for any significant new projects which will impact of Data Protection

To hold an Information Risk log

To ensure policies are in place that relate to the security of data held and transferred. This will include formal contractual arrangements with data processors.

To ensure data breaches are reported within the required timescales.

In line with legislation we employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

7. Employee Responsibilities

All employees will, through appropriate training and responsible management:

Processed lawfully, fairly and in a transparent manner;

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

Accurate and kept up to date;

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);

Processed in a manner that ensures appropriate security of the personal data.

Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.

Understand fully the purposes for which the St Michael’s Clinic uses personal information.

Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the St Michael's Clinic to meet its service needs or legal requirements.

Ensure the information is correctly input into the St Michael's Clinic systems.

Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.

On receipt of a request from an individual for information held about them by or on behalf of immediately notify the Data Protection Officer, Mr Paul Haycox.

Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian.

Understand that breaches of this Policy may result in disciplinary action, including dismissal.

8. National Data opt-out

Under the national data opt-out everyone who uses publicly-funded health and/or care services can stop health and care organisations from sharing their "confidential patient information" with other organisations if it is not about managing or delivering their own care. For example, if this information is used for research or planning purposes.

St Michael's Clinic have no uses or disclosures which need to have national data opt-outs applied. However future uses or disclosures will be checked against the national data opt-out operational policy guidance. If it is deemed that the national opt out technical solution is required St Michael's will be ready to implement the NHS Digital MESH mail system using the appropriate spreadsheets.

This does not affect how we share information with other organisations to manage someone's care and it won't apply if we have explicit consent to share information or if the information is appropriately anonymised.

9. Distribution and Implementation

This document will be made available to all Staff via the St Michael's Clinic intranet site.

A global notice will be sent to all Staff notifying them of the release of this document.

The document will be emphasised in any training.

10. Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Senior Clinicians and Managers meeting.

The Business Manager is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises. Given the significant changes in 2018 the document will next be reviewed in February 2019.