St Michael's Clinic

Policy Description	**Confidentiality Policy**		
Target Audience	All Staff		
Version	V 1.4		
Review By	Paul Haycox		
Review Date	June 2027		
Next Review			
2nd Level Approval	Graham White	Approval Date	May 2025
3rd Level Approval	N/A	Approval Date	N/A

Version History

Version	Date	Amendments	By
1.4	May 2025	Updated staff confidentiality agreement. Minor organisation changes	Paul Haycox
1.5	June 2026	Organisation changes	

Contents

Policy Objective

The reasons for the policy:

a) All information about the organisation (in particular user data) is confidential, whether held electronically or in hard copy
b) Other information about St Michael's Clinic (for example its financial matters) is confidential
c) Staff will of necessity have access to such confidential information from time to time.

A duty of confidentiality arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. This duty of confidence is derived from:

- Common law – the decisions of the Courts
- Statute law which is passed by Parliament.

Definitions

The Registered Manager	The CQC Registered Manager within the clinic
Staff	All employed, locum, contract staff and consultants, including visiting medical staff with practicing privileges
Clinical Staff	Staff who are in direct contact with patients within a clinical setting including but not limited to nurses, consultants and medical staff, practitioners, therapists and health care assistants
Clinic	Any clinic or practice within St Michael's Clinic where patients attend for consultations or treatment

Relevant CQC Fundamental Standard/H+SC Act Regulation (2014)

- Regulation 10: "Dignity and Respect".

Responsibilities

Local Implementation of the policy; audit of the policy; managing breaches of the policy

St Michael's Clinic

St Michael's Clinic has overall responsibility for ensuring that the Clinic meets its statutory responsibilities, however day to day responsibility is devolved as set out below.

Data Controller

The data controller has overall accountability for establishing and maintaining a safe and effective data management system that adheres to all statutory and regulatory guidelines.

Caldicott Guardian

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. St Michael's Clinic Caldicott Guardian is Adele Veldsman

Senior Information Risk Owner (SIRO)

The SIRO is responsible for identifying and managing the information risks to the organisation and its business partners. This will include oversight of the organisation's information security incident reporting and response arrangements. The SIRO for St Michael's Clinic is Mr. Paul Haycox.

Data Protection Officer (DPO)

The Data Protection Officer will be responsible for monitoring compliance of the clinic against the GDPR. Specifically they will be responsible for:-

- Advising management and staff on their obligations in relation to the GDPR
- Monitor compliance with the GDPR in relation to policies, processes and staff awareness
- Advise on the requirement for, and completion of, Data Protection Impact Assessments
- To be first point of contact for Data Access Requests
- To be first point of contact for the Information Commissioners Office

All Managers

All Managers are responsible for ensuring that all Clinic imperatives, relating to confidentiality issues, are acted upon by their staff. Additionally, managers are responsible for:

Assessing, and reporting as necessary, on any confidentiality risks in their areas.

Ensuring that staff complete risk event forms for all confidentiality breaches.

Ensuring that all patient data is secure in their areas and that "safe haven" procedures are in place particularly in relation to patient records and fax machines.

Staff

All Staff are responsible for:

Making themselves aware and fully understand their legal obligation to keep personal information obtained through their work confidential.

Participating in induction, training and awareness raising sessions carried out to inform/update staff on confidentiality issues.

Challenging and verifying where necessary, the identity of any person who is making a request for confidential information and to determine the validity of their reason for requiring that information.

Reporting any actual or suspected breaches of confidentiality to their line manager.

The declaration in Appendix A or equivalent should be signed by all relevant members of staff at St Michael's Clinic as part of their contract of employment/Contract for Service, or otherwise as appropriate.

Procedure

a) Members of staff must not under any circumstances disclose patient information to anyone outside St Michael's Clinic, except to other health professionals on a need-to-know basis, or where the user has provided written consent, or for some other legal reason (e.g., Court Order regarding disclosure).

b) All information about users is confidential: from the most sensitive diagnosis to the fact of having visited the clinic or being registered with the organisation.

c) Members of staff must not under any circumstances disclose other confidential information about the company to anyone outside St Michael's Clinic unless with the express consent of the CQC Registered Manager or representative.

d) Members of staff should limit any discussion about confidential information only to those who need to know within St Michael's Clinic.

e) The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.

f) All patients can expect that their personal information will not be disclosed without their permission (except in the most exceptional circumstances when disclosure is required when somebody is at grave risk of serious harm).

g) Electronic transfer of any confidential information must be encrypted. Members of staff must take particular care that confidential information is not transmitted in error by email or over the Internet.

h) Members of staff must not take data from the organisation's computer systems (e.g., on a memory stick or removable drive) off the premises unless authorised to do so.

i) Members of staff who suspect a breach of confidentiality must inform the CQC Registered Manager or representative immediately.

j) Any breach of confidentiality will be considered as a serious disciplinary offence and may lead to dismissal.

k) Members of staff remain bound by the requirement to keep information confidential even if they are no longer employed at St Michael's Clinic.

l) Any breach, or suspected breach, of confidentiality after the worker has left St Michael's Clinic 's employment will be passed to the organisation's lawyers for action.

m) Any patient wishing to have access to their own records will be treated in accordance with statutory requirements.

Responsibilities of members of staff

All health professionals must follow their professional codes of practice and the law. This means that they must make every effort to protect confidentiality. It also means that no identifiable information about a user is passed to anyone or any agency without the express permission of that user, except when this is essential for providing care or necessary to protect somebody's health, safety, or well-being.

All health and social care professionals are individually accountable for their own actions. They should, however, also work together as a team to ensure that standards of confidentiality are upheld, and that improper disclosures are avoided.

Additionally, the organisation:

a) is responsible for ensuring that everybody employed or engaged by St Michael's Clinic understands the need for, and maintains, confidentiality.
b) has overall responsibility for ensuring that systems and mechanisms are in place to protect confidentiality.

Standards of confidentiality apply to all staff who are bound by contracts of employment, Contracts for Service or other forms of engagement to maintain confidentiality. They must not reveal to anybody outside the organisation personal information they learn in the course of their work, or due to their presence in the surgery, without the user's consent.
Nor will they discuss with colleagues any aspect of a user's attendance at the surgery in a way that might allow identification of the user unless to do so is necessary for the user's care. These requirements will be conveyed to all staff as part of their induction when first joining the organisation.

General Principles

The general principle to remember is that nothing is to be revealed to an enquirer. The identity of callers must be established and, if necessary, return calls made to confirm this.

Personal visits from either the police or press should be handled with courtesy.
Following confirmation of their identity, they should then be referred to the CQC Registered Manager or deputy.

Any clinical details or personal information contained within the user's medical records must not be discussed with friends or relatives. This includes confirming a user has attended the

clinic for whatever reason. A user's reason to attend the clinic may be something they do not wish to discuss with their family or require others to know about.

It is important to note that individual users are not identified for purposes of training or any other activity.

Personal Information

Personal information may relate to patients, members of staff, visitors, carers and other members of the public. To ensure the confidentiality of personal information, the following must be adhered to:

Information must be kept up to date and accurate. Checks to maintain accuracy when patients attend appointments will be made. Any inaccuracies will be noted and amended.

Any records that are found to have inaccurate information in them (such as incorrectly filed photographs or reports) will be immediately corrected upon identification and noted in the record.

Access to areas, departments or offices containing confidential information must be restricted to authorised personnel only.

Information of a personal nature must not be left unattended in a public area, this includes patient records, faxes, and telephone messages.

Staff must not access any patient, employee of other record for which they have no proper reason to do so in the course of their duties within St Michael's Clinic Ltd.

Staff must never access patient records for their personal interest (this includes their own health records or those of another staff member).

Compliance with all the relevant IT policies that exist to keep information secure.

Corporate Information

Staff must ensure that corporate/business information is only viewed by those who need to see in line with their role.

Staff Resignation

When a member of staff leaves their former manager must ensure that:

Rights of access to computer systems are rescinded.

Identity badges are returned.

All keys are returned

Uses of patient health data

All processing of data must be lawful. The clinic has mapped data flows and noted the legal basis for each data set being held and processed. The main patient facing basis are:

Article 6 of the GDPR outlines the lawful basis upon which personal data can be processed. Article 9 outlines the legal basis for processing of special categories of personal data.

The legal basis for processing NHS patient data under Article 6 of the GDPR is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The legal basis for processing private patient data under Article 6 of the GDPR is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract

The legal basis for processing NHS data under article 9 is necessary to protect the vital interests of the data subject

The legal basis for processing private patient data under article 9 is necessary to protect the vital interests of the data subject

There are a number of other times at which data has to be shared and these are laid out in articles 6 and 9 and can be expanded upon by the Data Protection officer.

Only persons who are directly involved in the above and have legal right to view the data can have access. In all cases the minimum amount of information should be disclosed and accessed.

Where it is possible to do so, data must be anonymised or pseudonymised.

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 NHS 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 clinics 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 there is explicit consent to share information or if the information is appropriately anonymised.

Where patient information is being accessed for research or education, each access will require explicit and informed patient consent unless the research is being managed centrally and the Health & Social Care Act 2001 (section 60) applies.

If disclosure to third parties is required

If a user or another person is at grave risk of serious harm which disclosure to an appropriate person would prevent, the relevant health professional should take advice from the CQC Registered Manager or representative, and/or from a professional / regulatory / defence body, in order to decide whether disclosure without consent is justified to protect the user or another person. If a decision is taken to disclose, the user should always be informed before disclosure is made, unless doing so could be dangerous.

Any decision to disclose information to protect the health, safety or well-being of an individual will be based on the degree of current or potential harm, not the age of the user.

In addition, there may be instances where disclosure is necessitated by reason of legal process (e.g., Court Order). In addition, on occasions the Police may approach St Michael's Clinic for information about a user e.g., in case of serious crime. Such situations will call for careful judgement and will normally need to be subject to confirmation by a Director. Medical staff involved will also be well advised to consult their professional indemnity organisation in advance of any disclosure.

Information relating to a user may be disclosed for the following reasons:

a) Information relating to a user may be disclosed provided the user has given his/her written authorisation for his/her legal representative to obtain it.
b) Where a user has died, consent to release information should be sought from the Executor of the estate.
c) Where the user has died intestate, consent to release information should be sought from the next of Kin.
d) When healthcare professionals involved with the users' care require to share clinical information in the strictest confidence.
e) When adverse drug reactions may be reported by any authorised professional staff to the Committee on Safety of Medicines.

Release of Information as A Legal Requirement

a) Certain infectious diseases must be notified under the Public Health (Infectious Disease) Regulations 1968. Failure to comply is a criminal offence (Infection Control Office).
b) If a user is suspected of addiction to a scheduled drug, a doctor is required to inform the Chief Medical Officer of the Home Office Drugs Branch (Misuse of Drugs Notification & Supply to Addicts Regulation 1985).
c) The Road Traffic Act 1972 requires information to be given to the police, which may lead to the identification of the driver of a vehicle. Only the name and address may be given.
d) Any individual must give information to the police which may prevent an act of terrorism or lead to the apprehension of a person involved in such an act (The Prevention of Terrorism (Temporary Provisions) Act 1989).
e) A professional member of staff's duty of confidentiality may be overridden when failure to disclose information would expose the user, or someone else, to the risk of death or serious harm. Where a professionally qualified person feels unable to disclose, the police or Crown Prosecution Service may apply for a Court Order under the Police & Criminal Evidence Act 1984.
f) In the event of sudden, suspicious, or unexplained deaths, the coroner may wish to investigate. Information should be disclosed, to determine whether an inquest should be held.
g) Any person must obey a written legal order to attend court and produce confidential evidence.
h) Identifiable information, relating to users being treated for sexually transmitted diseases, shall not be disclosed, except for the purpose of treatment or prevention.
i) If a healthcare professional has reason to suspect child abuse, it is legitimate to supply information to appropriate authorities, to ensure the safety of the child is maintained.
j) Access to computer held information under the Data Protection Act 2018.

.

Informing People on the Use of their Information

The GDPR makes it clear that personal data should be processed in a transparent manner.

Each clinic requires a Privacy Notice that outlines

The type of data collected

The purpose for which it is being used.

Other parties that it may be shared with.

Security measures applied.

The rights of the individual

The Privacy notice will be referenced in all letters for new appointments, is available on-line at the clinics website and is displayed in the waiting area.

No individual's identifiable information will be used without explicit consent for audit and research purposes.

Patients have the right to be informed how their information is used and to record their consent, dissent and objections.

Patients may also contact the clinic about a number of issues related to the use of their personal information which may include requests for certain disclosures of their information to be restricted. A good example of this is requests by patients not to have their summary health record available on the national "spine". The individuals' wishes would be respected unless there are exceptional circumstances.

All staff who receive communications from patients about disclosures of their records or are considering new uses or disclosures of records must first contact the Business Manager, IT manager or the Caldicott Guardian to ensure appropriate action is taken.

Information Sharing with other Agencies who are not IG toolkit compliant

It may be necessary for essential personal information to pass between a clinic and other NHS services. This may happen where one of these services is contributing towards a programme of care.

In any cases of "routine" data sharing, where the sharing is not associated with direct patient care and the bodies are not compliant with the Data Security and Protection Toolkit, then all parties involved in the data sharing should set up a data sharing protocol.

All personal information that is used in the protocol must meet the conditions for processing as laid down in the GDPR and Data Protection Act 2018 and the Caldicott review recommendations. If the information is to be shared for a different purpose to that for which it was given, it should only be disclosed if a legal basis for sharing can be established under Article 6 and Article 9 of the GDPR.

Each case will be judged on its merits as to whether a disclosure without consent is justified.

Information which has been aggregated and/or anonymised, can generally be shared for justified purposes. Care must be taken that an individual cannot be identified from this type of information as it can be possible to identify individuals from limited data e.g. numbers of patients suffering from a very rare health condition.

Access to Health Records

Medical Records do not belong to the patient, but patients have a right under the GDPR to request access to the records that a clinic holds on them. This can involve the clinic providing them with either manual or electronic copies or in some cases arranging for the patient to view their records.

When requesting access to their own records, no unnecessary barriers should be placed in front of the individual.

The request can be made in person, by letter or by e mail. All requests should be sent to the Data Protection Officer.

If the patient is known to the clinic and identity is not in question, then no additional identification is needed. However, if identification is not certain, then photo identification will be required.

The request should provide enough proof to satisfy the clinic of their identity. Where requests are made on behalf of the individual patient, the clinic must be satisfied that the individual has given consent to the release of their information.

It would be helpful if the form at Appendix B is completed and signed by both the requesting party and the authorising clinic officer. However, this is not mandatory, and the patient has the right to refuse.

At all times, the request should be logged on receipt. A note of the exact information shared must be made in the patients record – along with the date and mode by which it was sent. This should also be logged with reception onto the Data Access Request log.

The data must be supplied within 28 days of receipt of

No charges can be made for copies of records, unless further requests are made that are considered excessive in their nature.

If the records contain information supplied by a third party who clearly would not have provided the information had they thought that their contribution would be disclosed, then the name of the contributor and their information should not be supplied to the data subject and the information redacted.

In the event that a clinic receives a request from a patient who has suffered significant trauma, e.g. major accident disfigurement or serious burn, the treating clinicians will be informed of the request to ensure that disclosure is in the best interests of the patients particularly as the records are likely to contain distressing clinical photography. The treating consultant or a member of their team will supervise these disclosures or partial disclosures. However, the purpose of this is to disclose as much as possible not to prevent legal access and to achieve this as safely as possible and act at all times in the best interests of the patient.

Clinics will not manage the records of the deceased differently than they manage the records of the living.

Requests to correct errors in, or delete, records

Any requests from data subjects to amend or erase records that are brought to the attention of the clinic will be reviewed by the Data Protection Officer and the Caldicott Guardian within 14 days of the matter being raised. The request must be in writing (an e mail is sufficient).

Any amendments to records will be considered against the requirements of the General Data Protection Regulation and the Data Protection Act 2018 – alongside the legal requirements relating to medical records.

The data protection officer will write to the data subject with a decision regarding the request – this will include consideration of correcting the record if inaccurate, rectifying it and/or erasure (subject to the outcome of the review and the reason the data is held).

Requests to restrict or cease processing of data

At the request of an individual, made in writing, the Data Protection Officer will review any request to restrict or cease the processing of personal data. The Data Protection Officer will respond to the request within 28 days of receipt.

Telephones, Answering Machines, Faxes and Overheard Conversations

Telephone Enquiries. Always be sure that the caller is who they say they are, unless it can be verified beyond doubt, do not give patient identifiable information.

Telephone conversations may be recorded if that call is deemed to be of a such a nature that review of the conversation may be required. Notice that calls may be recorded is provided as part of the recorded message for all telephone calls.

Answering Machines. Staff may only leave a message on a patient's home landline if it is absolutely necessary and then leave name and number. Ideally permission will have been obtained from the patient to leave messages on a home landline. It is better to use answering machine function on mobile phones as more detailed information can be left as there is a reduced risk that uninvolved others can access the call details.

Email. Patient identifiable information should never be included in the main body of an email, unless password protected using an accredited software package – such as Winzip, Ironport, etc or using nhs.net to nhs.net e mail accounts. If password protected, then the password must be agreed with the recipient in advance of sending.

Fax machines. All faxes must be sent to a safe location where only staff who have legitimate right to view the data can access it. The sender must be certain the correct person will receive it. Care must be taken dialling the right number; setting up simple number codes for routine faxes will help.

Overheard Conversation. Where conversations are conducted by staff relating to a clinics business either over the phone, face to face, or in the close proximity of public or reception areas, then care must be taken that person identifiable information is not overheard by persons who do not have a right or need to hear such information.

Confidential Waste

All paper that contains sensitive patient or Clinic information must be disposed of in line with the Document, Record and Lifecycle Management Policy and Credit Card Policy.

Training

Training in information governance, which includes confidentiality, is mandatory for all staff.

Data Protection Impact Assessments (DPIA)

A data protection impact assessment will be undertaken on any project that will have a significant impact on how data is processed. That could be as a result of:-

- Implementation of new technologies
- Any change in processing that could be considered “high risk” for the individuals data i.e. change in the level of processing, the type of processing, a third party processor becoming involved or if a processor starts to use services in a non-EU country

The Data Protection officer will be informed and support the DPIA.
The project should not commence until the DPIA has been signed off by the DPO and Caldicott Guardian
A template for the DPIA is available on the ICO website:- https://ico.org.uk/

Confidentiality guidelines for members of staff

a) Be aware that careless talk can lead to a breach of confidentiality – discuss your work only with authorised personnel, preferably in private.
b) Always keep confidential documents away from prying eyes.
c) Verbal reporting about users should be carried out in private. If this is not possible, it should be delivered in a volume such that it can only be heard by those for whom it is intended.
d) When asking for confidential information in circumstances where the conversation can be overheard by others, conduct the interview in as quiet and discreet a manner as possible and preferably find somewhere private for the discussion.
e) Information should be given over the telephone only to the user or, in the case of children, to their parent or guardian. Precautions should be taken to prevent the conversation being overheard. Care must be taken to ensure that the duty of confidentiality to a minor is not breached, even to a parent.
f) The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.
g) When using computers, unauthorised access should be prevented by password protection and physical security such as locking the doors when offices are left unattended. Where possible, VDU screens should be positioned so that they are visible only to the user. Unwanted paper records should be disposed of safely by shredding on site and computer files on hard or floppy disks should be wiped clean when no longer required.
h) If unsure about authorisation to disclose, or a person’s authorisation to receive confidential information, always seek authorisation from the CQC Registered Manager or representative before disclosing any personal health information.

Legislation

All relevant staff must understand their responsibilities relating to confidentiality, and where appropriate be aware of the following legislation:

The General Data Protection Regulation (GDPR).
The GDPR is a European Law, which is enshrined in English Law alongside the Data Protection Act 2018. It lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. It also enshrines the legal basis upon which data can be processed and the individual's right to transparency in data processing and their rights to review and challenge data held by organisations

The Data Protection Act 2018 (DPA).
The DPA supplements the GDPR and gives legal rights to the Information Commissioners office as the regulator. It defines the UK law in certain areas on the processing of data.

***Human Rights Act 1998*.**
This Act was passed as a result of the European Convention on Human Rights. This is intended to protect certain rights of individuals. In terms of Confidentiality, the key part is Article 8; "the right to respect for private and family life, home and correspondence". This gives an individual the right to live their life with personal privacy in a way that does not infringe on the rights of anyone else. This could include information held about them in the form of diaries or personal records and correspondence aspect is equally as broad.

The Health & Social Care Act 2001 (section 60).
This section gives the Secretary of State, powers to permit the use of patient data in certain special cases without the necessity of gaining consent. An example of these powers has been to allow disclosure of patient data to support activities for cancer registries. It is this section that will usually apply to nationally managed research activity.

Freedom of Information Act 2000.
This Act is part of the Government's commitment to make more public sector information available to the public. It does however outline several exemptions to protect certain information which includes patient identifiable information. For more information see the Freedom of Information Policy.

***Regulation of Investigatory Powers Act 2000*.**
This Act is intended to combat cybercrime. It ensures that any interceptions do not breach an individual's human rights and requires that appropriate authorisations are obtained when required. The Act also supplements existing legislation, for example, any information collected under this Act still falls under the Data Protection Act and its principles.

***Information Governance*.**
Provides a framework to bring together all the requirements, standards and best practice that apply to the handling of personal information. One of the aims is to support the provision of high quality care by promoting the effective and appropriate use of information.

Caldicott Reviews.
The 1997 review of the uses of patient identifiable information by Dame Fiona Caldicott devised six general principles of information governance that could be used by all NHS organisations with access to patient information. The further Information Governance Review in March 2013 set out 26 recommendations to improve information governance nationally and after the 2020 review another principle was added.

General Medical Council;
Confidentiality: Good practice in handling patient information.2018

***Nurses and Midwives Council*;**
The Code 2015

The Mental Capacity Act 2005
This provides a legal framework to empower and protect people who may lack capacity to make some decisions for themselves. The assessor of an "individual's capacity to make a decision will usually be the person who is directly concerned with the individual at the time the decision needs to be made" this means that different health care workers will be involved in different capacity decisions at different times.

The Computer Misuse Act 1990
This Act secures computer programs and data against unauthorised access or alteration. Authorised users have permission to use certain programmes and data. If the users go beyond what is permitted, this is a criminal offence.

Disclosure

Disclosure means the giving of information. Disclosure is only lawful and ethical if the individual has given consent to the information being passed on. Such consent must be freely and fully given. Consent to disclosure of confidential information may be:

a) Explicit
b) Implied
c) Required by law or
d) Capable of justification by reason of the public interest.

Disclosure with Consent
Explicit consent is obtained when the person in the care of a professional staff agrees to disclosure having been informed of the reason for that disclosure and with whom the information may or will be shared. Explicit consent can be written or spoken. Implied consent is obtained when it is assumed that the person understands that their information may be shared within the clinical team. Professional staff should make the people in their care aware of this routine sharing of information, and clearly record any objections.

Disclosure without Consent
The term 'public interest' describes the exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader social concern. Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation, and punishment of serious crime and/or to prevent abuse or serious harm to others. Each case must be judged on its merits. These decisions are complex and must consider of both the public interest in ensuring confidentiality against the public interest in disclosure. Disclosures should be proportionate and limited to relevant details.

Professional staff should be aware that it may be necessary to justify disclosures to the courts or to the appropriate statutory regulator and must keep a clear record of the decision-making process and advice sought. Courts tend to require disclosure in the public interest where the information concerns misconduct, illegality, and gross immorality.

Disclosure to Third Parties
This is where information is shared with other people and/or organisations not directly involved in a person's care. Professional staffs must ensure that the people in their care are

aware that information about them may be disclosed to third parties involved in their care. Users generally have a right to object to the use and disclosure of confidential information. They need to be made aware of this right and understand its implications. Information that can identify individual people in the care of a nurse, doctor or dentist must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a wider public interest.

Confidentiality after Death
The duty of confidentiality continues after the death of an individual to whom that duty is owed.

Information Disclosure to the Police
In English law there is no obligation placed upon any citizen to answer questions put to them by the police. However, there are some exceptional situations in which disclosure is required by statute.

Police Access to Medical Records
The police have no automatic right to demand access to a person's medical records. Usually, before the police may examine a person's records, they must obtain a warrant under the Police and Criminal Evidence Act 1984. Before a police constable can gain access to a hospital, for example, in order to search for information such as medical records or samples of human tissue, he or she must apply to a circuit judge for a warrant. The police have no duty to inform the person whose confidential information is sought but must inform the person holding that information.

This Act allows healthcare professionals to pass on information to the police if they believe that someone may be seriously harmed or death may occur if the police are not informed. Before any disclosure is made healthcare, professionals should always discuss the matter fully with other professional colleagues and, if appropriate consult their statutory regulator or professional body or trade union. It is important that healthcare professionals are aware of their organisational policies and how to implement them. Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. If disclosure takes place without the person's consent, they should be told of the decision to disclose and a clear record of the discussion and decision should be made as stated above.

Special Considerations to be Considered when Disclosure is Being Considered
In some circumstances it may not be appropriate to inform the person of the decision to disclose, for example, due to the threat of a violent response. The professional staff may feel that, because of specific concerns, a supplementary record is required containing details of the disclosure. The Data Protection Act 1998 does allow for healthcare professionals to restrict access to information they hold on a person in their care if that information is likely to cause serious harm to the individual or another person. A supplementary record should only be made in exceptional circumstances as it limits the access of the person to information held about them. All members of the healthcare team should be aware that there is a supplementary record and this should not compromise the persons' confidentiality.

Acting as a Witness in a Court Case
If summoned as a witness in a court case he/she must give evidence. There is no special rule to entitle healthcare professionals to refuse to testify. If the individual refuses to disclose

any information in response to any question put to him/her, then a judge may find the individual in contempt of court and may ultimately send him/her to prison.

Risk or Breach of Confidentiality
If a member of staff identifies a risk or breach of confidentiality, they must raise their concerns with someone in authority if they are unable to take affirmative action to correct the problem and record that they have done so. A risk or breach of confidentiality may be due to individual behaviour or as a result of organisational systems or procedures.

Confidentiality is a fundamental part of professional practice that protects human rights. This is identified in Article 8 (Right to respect for private and family life) of the European Convention of Human Rights which states:

The common law of confidentiality reflects that people have a right to expect that information provided is only used for the purpose for which it was given and will not be disclosed without permission. This covers situations where information is disclosed directly and also to information obtained from others. One aspect of privacy is that individuals have the right to control access to their own personal health information.

a) All staff will respect people's right to confidentiality.
b) Staff must ensure people are informed about how and why information is shared by those who will be providing their care.
c) Staff must disclose information if they believe someone may be at risk of harm, in line with the law of the country in which you are practicing.

The Data Protection Act 1998 requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO) unless they are exempt. Failure to do so is a criminal offence. Further details and registration forms can be found on: http://ico.org.uk/

Appendix A

DECLARATION BY MEMBERS OF STAFF

I understand that all information about users held by St Michael's Clinic is strictly confidential, including the fact of a particular user having visited the organisation.

I will abide by the confidentiality guidelines and principles set out in the organisation's Confidentiality Policy.

I have read the Staff Confidentiality Policy above and fully understand my obligations and the consequences of any breach of confidentiality. I understand that a breach of these obligations may result in dismissal.

I understand that any breach, or suspected breach of confidentiality by me after I have left St Michael's Clinic employment will be passed to the Company's lawyers for action.

If I hold a professional qualification and my right to practise depends on that qualification being registered with a governing body, it is my responsibility to have read and understood their advice on confidentiality.

Name: _____

Signature: _____

Date: _____

Appendix B

Access to Health Records under the General Data Protection Regulation (Subject Access Request)

It is not mandatory to complete this form, but it will help us administratively

I am applying for access to view my health records:

FULL NAME	
DATE OF BIRTH	
ADDRESS	
CONTACT NUMBER	

You do not have to give a reason for applying for access to your health records. However, to help us save time and resources, it would be helpful if you could provide details below, informing us of periods and parts of your health records you require, along with details which you may feel have relevance i.e. consultant name, location, written diagnosis and reports etc.

DATE AND TYPES OF RECORDS:	

IN CASES WHERE IDENTIFICATION IS UNCERTAIN WE REQUIRE PHOTO ID

Access to Health Records under the General Data Protection Regulation (Subject Access Request)

It is not mandatory to complete this form, but it will help us administratively

PRINT NAME:	
SIGNED:	
DATE:	

……..

OFFICE USE ONLY

RECEIVED BY:	
SIGNED:	
DATE:	

IN CASES WHERE IDENTIFICATION IS UNCERTAIN WE REQUIRE PHOTO ID