Executive Summary	The lawful and proper treatment of personal information by The Practice Group is extremely important to the success of our business and, in order to maintain the confidence of our service users and employees, we must ensure that The Practice Group treats personal information lawfully and correctly. This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information. This Policy has been reviewed and updated in line with the requirements of GDPR and the Data Protection Act 2018.
Key Messages	The Practice Group (TPG) needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, clients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal 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) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018.
Owner	Information Governance Lead
Next Review Date	One year from Policy approval date
Consultation Process	Head of Quality Assurance, Data Protection Officer

Date Policy Approved	30 August 2018
Approving Committee	**Policy Authorising Committee**
Related Policies or Documents	Information Governance Policy Access to Medical Records Policy Disclosure of Medical Records after Death Policy Records Retention Standard Operating Procedure
Target Audience	**All Staff**
Distribution to Target Audience	**Intranet (myTPG)**
Equality Impact Assessment	The Practice Group is committed to promoting equality as a commissioner and provider of services, as a partner with the NHS and as an employer. This Policy has been assessed with regard to the Public Sector Race, Disability and Gender Duties.

Policy Review History

Version	Date	Changes	By Whom
1	June 2017	New Policy	Lizzie Bayley
2	August 2018	Policy updated for GDPR and Data Protection Act 2018 compliance	Louise Fox

Contents

Data protection policy

1. Introduction

The Practice Group (TGP) needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, clients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal 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) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018.

The lawful and proper treatment of personal information by The Practice Group is extremely important to the success of our business and, in order to maintain the confidence of our service users and employees, we must ensure that The Practice Group treats personal information lawfully and correctly.

This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

2. Data Protection Principles

The Practice Group supports fully and complies with the six principles of the Act which are summarised below:

1 Personal data shall be processed fairly and lawfully.

2 Personal data shall be obtained/processed for specific lawful purposes, and will only be used for the purpose for which it was collected.

3 Personal data held must be adequate, relevant and not excessive.

4 Personal data must be accurate and kept up to date, and every reasonable step will be taken to ensure any personal data that is inaccurate is erased or rectified without delay.

5 Personal data shall not be kept for longer than necessary.

6 Personal data shall be processed in a manner that ensures appropriate security of the personal data.

3. Responsibilities - General

3.1 All staff have responsibility for the lawful and proper treatment of personal information, its security against unauthorised access, unlawful processing and loss or destruction.

3.2 All staff should undertake the mandatory training relevant to their roles and responsibilities in relation to data protection, confidentiality and information governance.

3.3 All staff should request help from their line manager, the Information Governance Lead or the Data Protection Officer if they are unsure about any aspect of data protection, confidentiality or information governance.

4. Responsibilities of The Practice Group (TPG)

4.1 Maintain its registrations with the Information Commissioner's Office.

4.2 Provide training for all staff.

4.3 Provide clear lines of reporting and supervision for compliance with data protection and have a system for reporting breaches.

4.4 Carry out regular checks to monitor and assess new processing of personal data and ensure the Data Protection Officer is updated to take account of any changes in processing of personal data.

4.5 Develop and maintain procedures to meet the requirements of the Data Protection Act.

4.6 Take steps to ensure that individual patient or client information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's or client's consent, unless otherwise legally compliant. This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.

4.7 Maintain a system of Incident Reporting/Significant Event Reporting, through a no-blame culture to capture and address incidents which threaten compliance with the Data Protection Act.

4.8 Include data protection issues as part of its general procedures for managing risk.

4.9 Ensure confidentiality clauses are included in all contracts of employment.

4.10 Ensure that all aspects of confidentiality and information security are promoted to all staff.

4.11 Remain committed to the security of patient, client and staff records.

4.12 Ensure annual compliance with NHS Data Security and Protection (DSP) Toolkit.

5. Responsibilities of Managers of Surgeries and Services within The Practice Group

5.1 Supervise and ensure compliance with systems for reporting and managing data breaches.

5.2 Encourage staff to undertake mandatory training and monitor staff compliance with training to meet Data Protection and NHS DSP Toolkit requirements.

5.3 Ensure staff understand the lines of reporting and supervision for compliance with data protection and significant event/incident reporting.

5.4 Carry out regular checks to monitor and assess new processing of personal data and ensure the Data Protection Officer is updated to take account of any changes in processing of personal data.

5.5 Take steps to ensure that individual patient or client information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's or client's consent, unless otherwise legally compliant. This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.

5.6 Promote Incident Reporting/Significant Event Reporting for their Surgery or Service through a no-blame culture and manage incidents to capture learning, including discussion of incidents in regular meetings.

5.7 Remain committed to the security of patient, client and staff records.

5.8 Ensure compliance with NHS Data Security and Protection (DSP) Toolkit and, for Practice Managers, complete and submit the annual Toolkit for their Surgery.

5.9 Ensure that all Subject Access Requests (SARs) are dealt with in accordance with Access to Medical Records Policy and the Subject Access Request Form.

5.10 Display a notice explaining to patients and clients the policy, plus a copy of the Information Commissioners Certificate.

5.11 Make available a leaflet and/or a poster on Access to Medical Records for the information of patients or clients.

5.12 Ensure that information is destroyed (in accordance with the provisions of the Act) when it is no longer required and in line with TPG's Records Retention Standard Operating Procedure.

5.13 Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian / IG Lead.

6. Staff Responsibilities

6.1 All staff will, through appropriate training and responsible management, comply at all times with the above Data Protection Act principles.

6.2 Undertake all mandatory training relevant to data protection and confidentiality.

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

6.4 Understand fully the purposes for which the practice uses personal information.

6.5 Collect and process appropriate information, only in accordance with the purposes for which it is to be used by the Surgery or Service to meet its service needs or legal requirements.

6.6 Ensure the information is correctly input into the Surgery's or Services' systems.

6.7 On receipt of a request from an individual for information held about them, by or on behalf of them, notify the Practice Manager or Service Manager.

6.8 Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian / IG Lead.

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

7. Disclosing of Personal Data – Subject Access Requests

7.1 Subject Access Requests – patients and clients:

Patients and clients are entitled to request and receive information held on them by The Practice Group and its Surgeries and Services. For guidance on Subject Access Requests from patients and clients of The Practice Group, you should refer to the Access to Medical Records Policy.

7.2 Subject Access Requests – staff

Staff should submit their request to the HR Department.

8. Disclosing Data for Other Reasons

8.1 In certain circumstances, the Data Protection Act 2018 allows personal data to be disclosed to law enforcement and external agencies without the consent of the data subject. Under these circumstances, The Practice Group will disclose requested data, following review of the request by the Data Protection Officer, who will ensure the request is legitimate, seeking assistance from the board and from The Practice Group's legal advisers where necessary.