Praxis Care
INFORMATION GOVERNANCE & DATA PROTECTION POLICY

Printed copies are for reference only. Please refer to electronic copy for most recent information.

1. INTRODUCTION

Praxis Care holds personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

Under the General Data Protection Regulations 2018, the Data Protection Act 2018 (UK and Isle of Man), and all future amendments, and the Data Protection Act 2018 (ROI) and all future amendments, Praxis Care is committed to apply all the requirements under the Regulations and the Acts.

This is the Information Governance and Data Protection Policy which describes the legal requirements which Praxis Care must adhere to. This policy should be read in conjunction with:
CONFIDENTIALITY & INFORMATION SHARING POLICY
INFORMATION SECURITY POLICY
DATA BREACH POLICY AND PROCEDURE
SUBJECT ACCESS REQUEST POLICY & PROCEDURE
RETENTION AND DISPOSAL OF RECORDS PROCEDURE
USE OF SOCIAL MEDIA, PHOTOGRAPHY & VIDEO POLICY
CCTV POLICY & PROCEDURE

2. SCOPE

This policy aims to communicate to all staff Praxis Care's commitment to good Data Protection and practices to safeguard information. It applies to all staff equally, who must be familiar with this policy and comply with its terms.

This policy is supported by our other policies and procedures relating to information and how it is managed. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3. DEFINITIONS

Six Principles

These are the six principles of Data Protection under the legislation.

Data Protection Officer
The person appointed in order to coordinate all Data protection requirements within Praxis Care.

Information Asset Owner
Each Departmental Director.

Legal Purposes
The purposes for which personal data may be used by us:
Personnel, service delivery, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following but not exclusively:

- *Compliance with our legal, regulatory and corporate governance obligations and good practice*
- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*
- *Ensuring Praxis Care policies are adhered to (such as policies covering service provision)*
- *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of personal data, commercially sensitive information, Access NI or Garda checks, and checking*
- *Investigating complaints*
- *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments*
- *Monitoring staff conduct, disciplinary matters*
- *Marketing our business*
- *Improving services*

Personal Data
Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, service users, suppliers and marketing contacts.

Personal Data Praxis Care gather may include: individuals' contact details, medical or other conditions educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Special Categories of Personal Data
Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

Legislation
General Data Protection Regulations (GDPR) 2018.
Data Protection Acts (DPA) 2018 United Kingdom and Republic Of Ireland.

Supervisory Authorities
Information Commissioners Office (United Kingdom)
Information Commissioner (Isle of Man)
Data Protection Commissioner (Republic of Ireland)

4. ROLES AND RESPONSIBILITIES

The Chief Executive Officer has overall responsibility for Data Protection throughout Praxis Care.

The Data Protection Officer has overall responsibility for the day-to-day implementation of this policy.

Each Departmental Director is responsible for Data Protection within their assigned Departments. They are deemed Information Asset Owners.

Managers are responsible for the operational requirements and related procedures are applied.

All staff and volunteers must adhere to this policy and all related governance policies and procedures.

As the Data Protection Officer (DPO), has overall responsibility for the day-to-day implementation of this policy, staff should contact the DPO for further information regarding this policy if necessary.

Data Protection Officer
Praxis Care
25 – 31 Lisburn Road
Belfast
BT9 7AA

Tel: 02890234555 (from UK and Isle of Man)
0482890234555 (from ROI)

4.1 Praxis Care's Responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

4.2 Directors Responsibilities

- Ensuring Data Protection Policy and Procedure is adhered to within their Departments
- Ensure all Departmental Procedures adhere to good Data Protection Practices
- To cooperate fully with the Data Protection Officer in the pursuance of their role
- Where there are major projects inbound which relate to large volumes of personal information, ensure a Data Protection Impact Assessment is undertaken
- Champion Data Protection within their Department

4.3 Staff Responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions. This applies equally to hard copies (paper based) and soft copies (stored in a computer based system)
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

4.4 Responsibilities of the Head of IT

- Ensure all systems, services, software and equipment meet acceptable security standards

- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

4.5 Data Protection Officer's Responsibilities

- Keeping the Board of Trustees updated about Data Protection responsibilities, risks and issues
- Reviewing all Data Protection procedures and policies on a regular basis in conjunction with each Directorate within the Group.
- Arranging Data Protection training and advice for all staff members and those included in this policy
- Answer questions on Data Protection from staff, Trustees and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Praxis Care (Subject Access Request).
- Checking and approving with third parties that process Praxis Care's data, any contracts or agreement regarding data processing in conjunction with the relevant Directorate.
- Maintaining a Data Asset Register with information drawn from all parts of the Group.
- Investigation of any actual or suspected breach plus liaison with all effected parties and applicable Supervisory Authority.

5. THE SIX PRINCIPLES

Praxis Care shall comply with the six principles of data protection (the Principles), which are:

1. Lawful, fair and transparent
Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose
Data can only be collected for a specific purpose.

3. Data minimisation
Any data collected must be necessary and not excessive for its purpose.

4. Accurate
The data we hold must be accurate and kept up to date.

5. Retention
We cannot store data longer than necessary.

6. Integrity and confidentiality
The data we hold must be kept safe and secure.

6. RIGHTS OF INDIVIDUALS

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed
- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access
- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification
- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

4. Right to erasure
- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing
- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data if it is incompatible with the requirement to provide a service.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest only or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

7. ACCOUNTABILITY AND TRANSPARENCY

Praxis Care must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the Accountability and Transparency Principle of the Data Protection Acts, Praxis Care must demonstrate compliance. All staff are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing

- Creating and improving security and enhanced privacy procedures on an ongoing basis

8. ACCURACY AND RELEVANCE

Praxis Care will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you must record the fact that the accuracy of the information is disputed and inform the DPO.

9. LAWFUL BASIS FOR PROCESSING DATA

Praxis Care must establish a lawful basis for processing data in accordance with individuals' rights under the first Principle. If the organisation cannot apply a lawful basis (explained below), its processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Ensure that any data we are responsible for managing has a written lawful basis for doing so. It is the responsibility of each Departmental Information Asset Owner to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis.

At least one of the following conditions must apply whenever we process personal data:

1. Consent

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose. For children, rules apply under the legislation to assess and request consent on their behalf from an adult.

2. Contract

The processing is necessary to fulfil or prepare a contract for the individual.

3. Legal obligation

We have a legal obligation to process the data (excluding a contract).

4. Vital interests

Processing the data is necessary to protect a person's life or in a medical situation.

5. Public function

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. Legitimate interest

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

When making an assessment of the lawful basis, Praxis Care will first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose.

The following considerations will be undertaken:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Is Praxis Care able to stop the processing at any time on request if it is not legal or relevant?

Praxis Care's commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions. This will be reflected on the Information Asset Register.

Praxis Care ensures that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

10. DATA CONTROLLER AND DATA PROCESSOR

Praxis Care is classified as both a Data Controller and Data Processor.

As a Data Controller, Praxis Care is the body which determines the purposes and means and processing of personal data.

As a Data Processor, Praxis Care processes personal data on behalf of a controller.

As such we will maintain our appropriate registration with the relevant Supervisory Authority, i.e. Information Commissioners Office in order to continue lawfully controlling and processing data.

As a Data Processor, Praxis Care must comply with all legal obligations and act only on the documented instructions of the Data Controller.

As a Data Processor, we must:

- Not use a sub-processor without written authorisation of the Data Processor
- Co-operate fully with the ICO or COI or other Supervisory Authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If you are in any doubt about how we manage data, contact the DPO for clarification.

11. SPECIAL CATEGORIES OF PERSONAL DATA

Previously known as **sensitive personal data**, this means data about an individual which is more sensitive requires more protection. This type of

data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, employment legislation or the provision of services). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If there is no lawful basis for processing special categories of data that processing activity must cease.

12. DATA SECURITY

Staff should refer to both the CONFIDENTIALITY & INFORMATION SHARING POLICY and the INFORMATION SECURITY POLICY

All staff must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

12.1 Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed

- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords
- Data stored on a computer must be done so in a file management system in line with Praxis Care procedure to minimise the risk of loss or inadvertent transmission
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used in line with Praxis Care procedure
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the Praxis Care's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones which are not issued by Praxis Care
- All servers containing confidential and special category data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

13. DATA RETENTION AND DISPOSAL

Staff should refer to the RETENTION AND DISPOSAL OF RECORDS PROCEDURE

Praxis Care must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but must be determined in a manner consistent with our data retention guidelines.

14. TRANSFERRING DATA INTERNATIONALLY

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.

15. PRIVACY NOTICES

It is a requirement of the GDPR that a data processer tells data subjects about how their information is processed. In order to comply with this requirement, Praxis Care is required to provide all data subjects (or their

representative) with a Privacy Notice, which explains to them how and why Praxis Care collects personal information about them.

15.1 When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. For example, all service users or their representatives should be given a YOUR INFORMATION - PRIVACY NOTICE - ADULT (or equivalent) at the commencement of a service being provided to them.

If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

15.2 What will be included in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the Data Processor and the Data Protection Officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data (who we must share it with)
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the appropriate Supervisory Authority and internal complaint procedures

- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

16. SUBJECT ACCESS REQUESTS

16.1 What is a Subject Access Request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

16.2 How to deal with a Subject Access Request

Staff should refer to the SUBJECT ACCESS REQUEST POLICY & PROCEDURE

Praxis Care must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must advise the DPO of all Subject Access Requests.

Praxis Care can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a Subject Access Request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

16.3 Data Portability Requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the Data Processor they have requested it be sent to. This must be done free of charge and without delay and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

17. DATA BREACHES

Staff should refer to the DATA BREACH POLICY AND PROCEDURE.

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Praxis Care has a legal obligation to report any data breaches to the relevant Supervisory Authority within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

18. USING THIRD PARTY CONTROLLERS AND PROCESSORS

As a Data Controller and a Data Processor, Praxis Care must have written contracts in place with any third party that it uses. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

For Controllers - As a Data Controller, Praxis Care must only appoint processors who can provide sufficient guarantees under the Data Protection Acts and that the rights of data subjects will be respected and protected.

For Processors - As a Data Processor, Praxis Care must only act on the documented instructions of a controller. Praxis Care acknowledges its responsibilities as a Data Processor under the Data Protection Acts and will protect and respect the rights of data subjects.

19. CONTRACTS

Praxis Care contracts must comply with the standards set out by the Supervisory Authorities and, where possible, follow the standard contractual clauses which are available. Contracts with [Data Processors (and/or) Data Processors] must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, contracts must include terms that specify:

- Acting only on written instructions.
- Those involved in processing the data are subject to a duty of confidence.
- Appropriate measures will be taken to ensure the security of the processing.
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract.
- The controller will assist the processor in dealing with Subject Access Requests and allowing data subjects to exercise their rights under Data Protection Acts.
- The processor will assist the controller in meeting its Data Protection obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments.
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on the Data Protection Acts.

20. CRIMINAL OFFENCE DATA

Criminal Record Checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. Praxis Care cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

21. AUDITS, MONITORING AND TRAINING

21.1 Data Audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Data audits will be conducted regularly as defined by the DPO and normal procedures.

21.2 Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. Praxis Care will keep this policy under review and amend or change it as required. Staff must notify the DPO of any breaches of this policy. All staff must comply with this policy fully and at all times.

21.3 Training

All staff will receive adequate training on provisions of data protection law specific for their role. Staff must complete all training as requested. If staff move role or responsibilities, they are responsible for requesting new data protection training relevant to the new role or responsibilities.

If staff require additional training on data protection matters, they should contact the DPO.

22. FAILURE TO COMPLY

Praxis Care takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.