Professional Carers
221 Seaview Road, Wirral, CH45 4PD

Review Sheet

Last Reviewed	Last Amended	Next Planned Review
09 Jul '25	09 Jul '25	in 12 months, or sooner as required.

Business impact	 HIGH IMPACT — These changes require action as soon as possible.
Reason for this review	Scheduled review
Were changes made?	Yes
Summary:	This policy outlines the key principles of UK GDPR. It is the overarching policy in the suite of data protection policies It has been reviewed and updated throughout in line with current legislation. References have been checked and updated.
Relevant legislation:	• HSCA 2008 (Regulated Activities) Regulations 2014 • UK GDPR (as defined in section 3(11) Data Protection Act 2018 • The Data Protection Act 2018
Underpinning knowledge - What have we used to ensure that the policy is current:	• Author: Information Commissioner's Office (ICO), (2018), *Special Category Data - What are the conditions for processing?*. [Online] Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/ [Accessed: 16/6/2023] • Author: GOV UK, (2017), *National Data Guardian Review of Data security, consent and opt-outs*. [Online] Available from: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs [Accessed: 16/6/2023] • Author: Information Commissioner's Office, (2018), *UK GDPR guidance and resources*. [Online] Available from: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed: 16/6/2023]

Professional Carers
221 Seaview Road, Wirral, CH45 4PD

1. Purpose

1.1 The purpose of this policy is to ensure that Professional Carers understands the key principles of UK GDPR.
1.2 This policy sets out the steps that need to be taken by Professional Carers to ensure that Professional Carers handles, uses and **processes personal data** in a way that meets the requirements of UK GDPR.
1.3 This policy applies to all staff at Professional Carers who process personal data about other staff, Service Users and any other living individuals as part of their role.
1.4 To support Professional Carers in meeting the following Key Lines of Enquiry/Quality Statements (New):

Key Question	Key Lines of Enquiry	Quality Statements (New)
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?	QSW5: Governance, management and sustainability
WELL-LED	W3: How are the people who use the service, the public and staff engaged and involved?	QSW3: Freedom to speak up

1.5 To meet the legal requirements of the regulated activities that {Professional Carers} is registered to provide:

- HSCA 2008 (Regulated Activities) Regulations 2014
- UK GDPR (as defined in section 3(11) Data Protection Act 2018
- The Data Protection Act 2018

2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following Service Users may be affected by this policy:

- Service Users

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

3. Objectives

3.1 The objective of this policy is to ensure staff have a working knowledge into the principles and requirements of UK GDPR.
3.2 Alongside the suite of policies, procedures and guidance available, Professional Carers can demonstrate that appropriate steps are taken to ensure it complies with UK GDPR when handling and using personal data provided by both staff and Service Users.
3.3 This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.
3.4 This policy will assist with understanding the obligations of Professional Carers in respect of the rights of the staff and Service Users who have provided personal data and the steps Professional Carers should take if there is a personal data breach.

4. Policy

4.1 GDPR Background
GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998.
Following the UK's departure from the EU, UK GDPR was incorporated into domestic law that applies in the UK.
UK GDPR provides greater protection to individuals and places greater obligations on organisations than the pre GDPR data protection regime, but can be dealt with in bite-size chunks. Compliance with data protection laws should enhance service provision and care provided by engendering trust between Professional Carers and Service Users.
4.2 All staff must ensure the ways in which they handle personal data meet the requirements of UK GDPR.
4.3 The Approach of Professional Carers to UK GDPR
Professional Carers is required to take a proportionate and appropriate approach to UK GDPR compliance. Professional Carers understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. Professional Carers understands that if significant volumes of personal data are processed, including **special categories of personal data**, or it has unusual or complicated processes in place in terms of the way personal data is handled, Professional Carers will consider obtaining legal advice specific to the processing conducted and the steps that may need to be taken.
4.4 UK GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.
4.5 Process for Promoting Compliance at Professional Carers
To ensure Professional Carers complies with UK GDPR, a suite of data protection policies and resources are available and should be read in conjunction with this overarching policy to provide a framework for compliance.
4.6 Overview of Key Terms, Key Principles and Documents
The key principles and themes of each of the documents listed above are summarised below:
Key Terms
UK GDPR places obligations on all organisations that process personal data about a data subject. A brief description of those three key terms is included in the Definitions section of this document and are expanded upon in the Key Terms Guidance.
The requirements that Professional Carers need to meet vary depending on whether Professional Carers is a data controller or a data processor. In most cases Professional Carers will be a data controller. The meaning of 'data controller' and 'data processor', together with the roles they play under UK GDPR, are explained in the Key Terms Guidance. Professional Carers understands that it may be a data controller in some circumstances and a data processor in others.
Special categories of data attract a greater level of protection, and the consequences for breaching UK GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This information is also covered in more detail in the Key Terms Guidance.
Key Principles
There are 7 key principles of UK GDPR which Professional Carers must comply with. They are:

- Lawful, fair and transparent use of personal data

- Using personal data for the purpose for which it was collected
- Ensuring that the personal data is adequate and relevant
- Ensuring that the personal data is accurate
- Ensuring that the personal data is only retained for as long as it is needed
- Ensuring that the personal data is kept safe and secure
- Accountability - taking responsibility for what you do with personal data and how you comply with the other principles

Professional Carers must have appropriate measures and records in place to be able to demonstrate compliance.
These key principles are explained in more detail in the guidance entitled 'UK GDPR – Key Principles'.
Professional Carers recognises that, in addition to complying with the key principles, it must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. Professional Carers understands that a 'privacy by design' approach must be adopted. This means that data protection issues should be considered at the very start of a project, or engagement with a new Service User. Data protection should not be an after-thought. These ideas are also covered in more detail in the Key Principles Guidance.

Processing Personal Data

The provision of health or social care or treatment or the management of health or social care systems and services is expressly referred to in UK GDPR as a lawful basis upon which an organisation is entitled to process special categories of data.
In terms of other types of personal data, Professional Carers must only process personal data if it is able to rely on one of a number of grounds set out in UK GDPR. The grounds which are most commonly relied on are:

- The data subject has given their consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract with the data subject; and
- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the data subject or another living person
- The processing is necessary to perform a task carried out in the public interest

The grounds set out above are explained in more detail in the guidance entitled 'UK GDPR – Processing Personal Data'.

Data Protection Officers

Professional Carers understands that some organisations will need to appoint a formal Data Protection Officer under UK GDPR (a "**DPO**"). The DPO benefits from enhanced employment rights and must meet certain criteria, so it is recognised that it is important to know whether Professional Carers requires a DPO. This requirement is outlined in the Appointing a Data Protection Officer Policy and Procedure.
Whether or not Professional Carers needs to appoint a formal Data Protection Officer, it will appoint a single person to have overall responsibility for the management of personal data and compliance with UK GDPR. This person is: Gary Nagle – Director of Operations.

Data Security and Retention

Two of the key principles of UK GDPR are data retention and data security.

- Data retention refers to the period for which Professional Carers keeps the personal data that has been provided by a data subject. At a high level, Professional Carers must only keep personal data for as long as it needs the personal data
- Data security requires Professional Carers to put in place appropriate measures to keep data secure

These requirements are described in more detail in the Data Security and Data Retention Policy and Procedure.

Website Privacy and Cookies Policy and Procedure

Where Professional Carers collects personal data via a website, it understands that it will need a UK GDPR compliant website privacy policy. The privacy policy explains how and why personal data is collected, the

purposes for which it is used and how long the personal data is kept. A template website policy is provided.

Subject Access Requests

One of the key rights of a data subject is to request access to, and copies of, the personal data held about them by an organisation. Where Professional Carers receives a subject access request, it understands that it will need to respond to the Subject Access Request in accordance with the requirements of UK GDPR. To help staff at Professional Carers understand what a subject access request is and how they should deal with a subject access request, a Subject Access Request Policy and Procedure is available to staff. A Professional Carers process map to follow when responding to a subject access request, as well as a subject access request letter template is also included.

The Rights of a Data Subject

In addition to the right to place a subject access request, data subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by Professional Carers. Not all rights apply in all circumstances. Rights of the data subject are covered in detail in the corresponding guidance.

Breach Notification Under UK GDPR

In certain circumstances, if there is a personal data breach (i.e. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data), the ICO must be notified and potentially any affected data subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to all staff, together with a process map for Professional Carers to follow if a breach of UK GDPR takes place is available.

Professional Carers understands that this requirement is likely to have less impact on NHS organisations that are already used to reporting using the NHS reporting tool.

Data Privacy and Consent Form

Organisations are required to provide data subjects with certain information about the ways in which their personal data is being processed. This is detailed in a data privacy policy / statement. The privacy policy sits alongside a consent form which can be used to ensure that Professional Carers obtains appropriate consent, particularly from the Service User, to the various ways in which Professional Carers uses the personal data (where Professional Carers needs to rely on consent as a basis for the processing). The Consent Form contains advice and additional steps to take if the Service User is a child or lacks capacity.

Transfer of Data

If Professional Carers wishes to transfer personal data to a third party, an agreement must be put in place to set out how the third party will use the personal data. If the third party is processing data on the instruction of Professional Carers, the contract must cover specific points set out in UK GDPR. Professional Carers must consider carrying out due diligence investigations on third party recipients of personal data of which Professional Carers is the controller.

Transfers of personal data outside of the UK and EEA (and other countries with an adequacy decision in place for such data transfers) may only be made under specific circumstances. This includes where a data processor processes personal data in such jurisdiction. For such transfers, Professional Carers recognises that further protection will need to be put in place and other aspects considered before the transfer takes place. Guidance has been produced to explain the implications of transferring personal data in more detail.

Compliance with UK GDPR

Professional Carers understands that there are two primary reasons to ensure that compliance with UK GDPR is achieved:

- It promotes high standards of practice and Care, and provides significant benefits for staff and, in particular, Service Users
- Compliance with UK GDPR is overseen in the UK by the ICO. Under UK GDPR, the ICO has the ability to issue a fine of up to 20 million Euros (approximately £17,000,000) or 4% of the worldwide turnover of

an organisation, whichever is higher. The potential consequences of non-compliance are therefore significant.

Professional Carers appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance and offers guidance to organisations about how to comply. A one-off, minor breach may not attract the attention of the ICO but if Professional Carers persistently breaches UK GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special category personal data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of Professional Carers and its data protection policies and processes and to issue instructions for Professional Carers to comply or put right its data processing practices including requiring Professional Carers to stop providing services, or to notify data subjects of the breach, delete certain personal data held or prohibit certain types of processing.

5. Procedure

5.1 All staff must review the UK GDPR policies and procedures and guidance that are communicated to them.
5.2 Julie Harrison [the Managing Director] will nominate a person to be the Data Protection Officer/Privacy Officer. This is currently Gary Nagle - Director of Operations.
5.3 Mrs Carly Peckham [Registered Manager] will support Gary Nagle in ensuring all staff understand the policies and procedures provided, including how to deal with a subject access request and what to do if a member of staff breaches UK GDPR.
5.4 The Directorship team will consider providing training internally about UK GDPR (in particular, the Key Principles of UK GDPR) to all staff members, or may outsource this if deemed fit.
5.5 Professional Carers will delete any personal data that Professional Carers no longer needs, based on the results of the audit conducted, taking into account any relevant guidance, such as the Records Management Code of Practice - NHSX www.nhsx.nhs.uk/information-governance/guidance/records-management-code/.
5.6 Professional Carers will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with UK GDPR.
5.7 Professional Carers will ensure it has privacy policies in place and will circulate them to data subjects as relevant.
5.8 Professional Carers will ensure that, where required, proper consent to the UK GDPR standard is obtained from each Service User, (this may be via a care plan and assessment agreement). Professional Carers will review the additional steps that it should take to ensure that it obtains consent from parents, guardians, carers or other representatives where Professional Carers works with children or those who lack capacity.
5.9 Professional Carers will ensure that processes and procedures are in place to respond to requests made by data subjects (including subject access requests) and to deal appropriately with any personal data breaches.
5.10 A log of decisions taken and incidents that occur in respect of the personal data processed by Professional Carers using the Data Protection Impact Assessment template at Professional Carers.

6. Definitions

6.1 Data Subject

- The individual to whom personal data relates

6.2 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament

6.3 Personal Data

- Any information about a living person from which that person can be identified directly or indirectly including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV, online identifiers and special categories of data, defined below

6.4 Process or Processing

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending, deleting or transferring it. You do not need to be doing anything actively with the personal data – at the point you collect it, you are processing it

6.5 Special Categories of Data

- Special categories of data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation, genetic and biometric data, trade union membership and political views

6.6 UK GDPR

- The UK GDPR is the retained EU law version of GDPR that forms part of English law

6.7 Information Commissioner's Office

- The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- This is the overarching policy and provides a high level reference to all areas that are important for compliance with UK GDPR
- Understanding of the content of this policy should be embedded with all staff at Professional Carers
- Professional Carers must appoint a person with overall responsibility for managing UK GDPR. This person may be an official Data Protection Officer (DPO) or a person appointed to oversee privacy, governance and data protection
- UK GPDR provides a high level of protection for staff and Service Users in respect of their personal data
- Professional Carers has adopted an appropriate and proportionate approach what is right and necessary for Professional Carers may not be right for another organisation
- Compliance is mandatory, not optional
- Achieving compliance with UK GDPR will not only reduce the risk of ICO enforcement or fines but will also promote a better quality service for Service Users and an improved working environment for staff

Professional Carers
221 Seaview Road, Wirral, CH45 4PD

Key Facts - People affected by the service

People affected by this service should be aware of the following:

- Your personal data will be protected
- You have a right to see what information we hold about you
- You will be asked for your consent before we obtain your personal data in line with UK GDPR requirements
- In addition to the UK GDPR regulations, our staff will continue to follow confidentiality policies in relation to all aspect of your Care

Further Reading

As well as the information in the 'underpinning knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

ICO - Appropriate Policy Document template:
https://ico.org.uk/media/for-organisations/documents/2616286/appropriate-policy-document.docx
GOV.UK - New Health Data Security Standards and Consent/opt-out Model:
https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care
NHS England - Transformation Directorate - Records Management Code of Practice 2021
(provides guidance on how to keep records, including how long to keep different types of records.
https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/