DATA PROTECTION (UK GDPR)
Gian Healthcare

Date Reviewed: May 2025

Reviewed by: B.KWANGWARI

Next Review Date: May 2026

Scope

- **Policy Statement**
- Section 1
- Overview of the Act
- Definitions
- UK Data Protection Principles
- “Lawful bases” for processing
- Consent
- Legal Obligation
- Legitimate Interests
- Individual Rights
- Privacy notices, transparency, and control
- Information Commissioner: Role and Function
- Code of Conduct and Certification Mechanisms
- Derogations and Exceptions
- Code of Practice
- **The Policy**
- Section 2
- Lawful Bases
- Subject Access Requests
- Freedom of Information requests
- Sharing information and Risk Assessment
- Information Security Management Privacy Notices
- Privacy and Electronic Communications Regulations (PECR)
- Transparency
- UK Data Protection by Design
- Privacy Impact Assessment
- Reporting Breaches
- National Data opt-out
- Harm arising from lack of transparency
- How we provide privacy and transparency information
- Data Security and Protection toolkit
- Data Security and Protection Lead
- File Retention
- Compliance
- **Related Policies**
- **Related Guidance**
- **Training Statement**
- Appendix – TEMPLATE: Privacy Notice
- What information do we collect about you?
- How information about you will be used
- How we will use this information?

- Access to your information and corrections
- Appendix - TEMPLATE: Data Breach Record

Policy Statement

On 25 May 2018 the UK Data Protection Act 2018, which is based on the UK General Data Protection (UK GDPR) replaced the Data Protection Act 1998 in its entirety. It replaced the existing Data Protection Laws to make them fit for the digital age in which ever-increasing personal data is being processed. The Act set new standards for protecting personal data. Gives people more control over the use of their data and assists in the preparation for a future outside of the EU.

There are 4 main matters provided for, these are:

- General Data Processing
- Law Enforcement Data processing
- Data Processing for National Security Purposes
- Enforcement

All the above need to be set in the context of international, national, and local data processing systems which are increasingly dependent upon internet usage for the exchange and transit of data. The UK must lock into international data protection arrangements, systems, and processes, and this Act updates and reinforces the mechanism to enable this to take place.

Given the size of the legislation and some of the media hype surrounding its introduction, this policy is written in two Sections.

- Section 1 Overview of the Act.
- Section 2 The Policy and templates

Section 1

Overview of the Act

The Act is structured in seven parts, each of which covers specific areas. These are:

Part 1: Preliminary

This sets out the parameters of the Act, gives an overview, explains that most processing of personal data is subject to the Act, and gives the terms relating to the processing of personal data.

Part 2: General Processing

This supplements the UK GDPR and sets out a broadly equivalent regime to certain types of processing to which the UK GDPR does not apply.

Part 3: Law Enforcement Processing

This covers:

- "Competent authority"
- Meaning of "controller" and "processor"
- Data protection principles
- Safeguards regarding archiving and sensitive processing
- Rights and access of the data subject, including erasure
- Implements the law enforcement directive
- Controller and processor duties and obligations
- Records
- Co-operation with the ICO commissioner
- Personal data breaches
- The remedy for such breaches
- Position of the data protection officer and their tasks
- Transfer of data internationally to particular recipients
- National security considerations
- Special processing restrictions and reporting of infringements.

Part 4: Intelligence Services Processing

This covers only data handled by the above e.g. MI5 and MI6 and includes rights of access, automated decisions, rectification and erasure, obligations relating to security, and data breaches.

Part 5: The Information Commissioner

This covers:

- General functions including publication of Codes of Practice and guidance
- Their International role
- Their responsibilities regarding specific Codes of Practice
- Consensual audits
- Information to be provided to the Commissioner
- Confidentiality and privileged communication
- Fees for services
- Charges payable to the commission
- Publications
- Notices from the Commissioner
- Reporting to parliament

Part 6: Enforcement

This covers the new enforcement regime regarding all forms of Notice issued by the Commissioner

- Powers of entry and inspection
- Penalty amounts

- Appeals
- Complaints
- Remedies in the court
- Offences
- Special purpose proceedings

Part 7: Supplementary and Final Provision.

This covers legal changes that the new Act alters concerning other legal matters, e.g. Tribunal Procedure rules, definitions, changes to the Data Protection Convention, etc., and List of Schedule(s).

As you can see, this Act is a huge piece of legislation, the majority of which is outside the remit of service providers working within the Adult Health and Social Care Sector. The I.C.O. confirms that many concepts and principles are much the same and businesses that were complying with the old law were likely to be already meeting many of the key requirements of the UK GDPR and the new Act.

The Information Commissioner says the Act represents a "step change" from previous laws. "It means a change of culture of the organization. That is not an easy thing to do, and it's certainly true that accountability cannot be bolted on: it needs to be a part of the organisation's overall systems approach to how it manages and processes personal data". It's a change of mindset regarding data handling, collection, and retention.

We need to stop taking personal data for granted, it's not a commodity we own: it is only ever on loan. Individuals have been given control and we have been given the fiduciary duty of care over it!

As an organisation handling personal data on a day-to-day basis, this policy sets out the requirements of the Act and how we, as an organisation, will meet our legal obligations. Staff awareness and understanding of their responsibilities regarding the handling, collection, and retention of data will be core to the successful embedding of this policy.

Definitions

The UK GDPR applies to "Controllers", "Processors" and "Data Protection Officers" and to certain types of information, specifically, "Personal Data" and "Sensitive Personal Data" referred to in the Act as Special Categories of Personal Data".

"Controllers"

This role determines, on behalf of the organisation, the purposes, and means of processing personal data.

"Processors"

This role is responsible for processing personal data on behalf of a controller. The Act places specific legal obligations on you, e.g. you are required to keep and

maintain records of personal data and processing activities. This role has legal liabilities if they are responsible for any breach.

Data Protection Officer**.**

This role is a must only in certain circumstances if you are:

- A public authority (except for courts)
- Carry out large-scale systematic monitoring of individuals e.g. Online behaviour tracking
- Carry out large-scale processing of special categories of data, or data relating to criminal convictions and offences e.g., Police, DBS bodies, prison service, etc.

“personal data”

This means any information relating to an identifiable person can be directly or indirectly identified in particular by reference to an identifier. So, this would include name, reference or identification number, location data, or online identifier. This reflects changes in technology that incorporate a wide range of different identifiers. Personal Data applies to both automated and manual filing systems. It can also apply to pseudonymised e.g. key-coded can fall within the UK GDPR dependent on how difficult it is to attribute the pseudonym to a particular individual’s race, ethnic origin, politics, religion, trade union membership, sex life, or sexual orientation.

“Special Categories of Personal Data”

This category of data is more sensitive and much more protected. Sensitive personal data specifically includes genetic data, biometric data, health, race, ethnic origin, politics, religion, trade union membership, and sexual orientation Safeguards apply to other types of data e.g. criminal convictions and offences; intelligence data, etc.

Data Protection Principles

The UK GDPR sets out the following principles for which organisations are responsible and must meet. These require that personal data shall be:

- Processed lawfully, fairly, and transparently about individuals.
- Be collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with purposes, further processing for archiving purposes in the public interest, scientific or historical research. purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary for the purposes for which they are processed.
- Accurate and where necessary kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Personal data may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or

historical research purposes, or statistical purposes subject to the appropriate technical and organisational measures required by the UK GDPR (the safeguards) to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of personal data. Including protection against unauthorised or unlawful processing and accidental loss. Destruction or damage, using appropriate technical or organisational measures.

"The controller shall be responsible for, and be able to demonstrate, compliance with the principles" Article 5 (2) UK GDPR

"Lawful bases" for processing

There are 6 lawful bases for processing data. These are:

- **Consent:** the individual has given clear consent for us to process their data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked us to take specific steps before entering into a contract.
- **Legal Obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital Interests:** the processing is necessary to protect someone's life.
- **Public Task:** the processing is necessary for us to perform a task in the public interest, or for official functions and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's data that overrides those legitimate interests. (This does not apply if a public authority is processing data to perform its official tasks).

"Lawful bases" must be determined by the organisation before processing any personal data and thorough consideration must be given to this decision.

Residents must be aware of the lawful base used by this organisation to process their data

Consent

The UK GDPR sets a high standard here. Consent means offering individuals real choice and control. Consent practices and existing paperwork will need to be refreshed and meet specific requirements. These are:

- Positive opt-in, no pre-ticked boxes or other methods of "default" consent.
- A clear and specific statement of consent.
- Vague or blanket consent is not enough.
- Keep consent requests separate from other terms and conditions.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review.
- Avoid making consent to processing pre-condition to any service.

- Employers need to take extra care to evidence that consent is freely given and should avoid over-reliance on the consent.

Consent is one lawful basis to consider but organisations in a position of power over individuals should consider alternative “lawful bases”. If we would still process their data without consent, then asking for consent is misleading and inherently unfair.

Note: Consent within this policy relates only to data processing not Health or Support in a Social Care context. You must still use consent as defined within the Mental Capacity Act 2005 to deliver services

Legal Obligation

Put simply, the processing is necessary for us as an organisation to comply with the law, e.g. the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, which requires us as providers to collect, handle and process data in a prescribed manner.

Legitimate Interests

- This is the most flexible lawful basis for processing.
- It is likely to be appropriate where we process in ways that people would reasonably expect us to, with a minimal privacy impact, or where there is a compelling justification for the processing.
- There are 3 elements to consider when using this lawful base. We need to:
- Identify a legitimate interest.
- Show that the processing is necessary to achieve it: and balance it against the individual’s interests, rights, and freedoms.
- Legitimate interests can mean our organisations, the interest of third parties, commercial interests, and individual or social benefits.
- The processing must be necessary.
- A balance must be struck between our interests, and the individuals would it be reasonable to expect the processing, or would it cause unnecessary harm, then their interests are likely to override our legitimate interests.
- Keep a record of your legitimate interest assessment (LIA) to help you demonstrate compliance.

The above are the 3 most pertinent bases for Health and Social Care data processing activity.

Contract, Vital Interests, or Public Task

These apply within specific work settings and would be difficult to meet because service providers are subject to specific legislative and regulatory requirements to work within a “Regulated Activity”.

Individual Rights

The UK GDPR provides the following rights for individuals:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

Rights concerning automated decision-making and profiling.

All relevant guidance to individual rights is not yet complete, Working Party (WP)29 will continue to work and produce such guidance as is thought appropriate.
For any individual request which falls into the above categories, this organisation will follow the relevant guidance currently available on the following website.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR/whats-new/

Privacy notices, transparency, and control

To start a privacy notice, you need to tell people, as a minimum

- Who you are.
- What you are going to do with their information?
- Who it will be shared with?

Being transparent, and providing accessible information, is core to compliance and the UK GDPR Regulation 20: Duty of candour - Care Quality Commission (cqc.org.uk)

Privacy notices are the most common way to meet UK GDPR requirements.

Transparency, in governance or business context, is honesty and openness, and the more transparent we can be the more easily understood and access our services become to the people who use them. In the context of data processing is simply that:

“It should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of their data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processor and further information to ensure fair and transparent processing in respect of the confirmation and communication of personal data concerning them which is being processed.”

Information Commissioner: Role and Function

The Information Commission Office is the UK’s supervising authority.

Within the Enforcement Toolbox, the Information Commissioners Office known as the I.C.O. can now issue substantial fines of up to 20 million, or, 4% of an organisation's global turnover for certain data protection infringements. Fines, when appropriate, will be of the discretion of the I.C.O. with considerable variations expected to be levied. There are no fixed penalties or minimum fines, though there are different maximum fines for different breaches. The UK GDPR also empowers the I.C.O. to create tailor-made solutions to deal with infringements brought to their attention. This does not mean that organisations can relax about compliance, but diligent small and medium-sized organisations can take comfort in the fact that they are unlikely to face the sort of punitive fines that rogue tech giants could face.

Remember: the highest imposed fine limit was £500,000 under the old Act (1998) but the highest fine ever imposed was £400,000 to TalkTalk for failings in connection with a cyber-attack in 2016. The Information Commissioner is playing down the "scaremongering because of misconceptions". £20 million fines could put businesses out of business and that is not the intention of the UK GDPR, though there is a seismic shift in the number of fines that could be imposed.

The role and scope of the I.C.O. have not fundamentally changed, but rather have been expanded and enhanced via the UK GDPR.

Codes of Conduct and Certification Mechanisms

Although the use of any of the above is encouraged by the UK GDPR it is not obligatory. If an approved code of conduct or certification scheme becomes available that covers our processing activity, consideration will be given to working towards such a scheme as a way of demonstrating our compliance. The I.C.O. will develop its code of conduct as it has already worked with the Direct Marketing Commissions Code of Conduct: DMA Code.

Derogations and Exceptions

The Act provides that member states of the EU can provide their own national rules in respect of specific processing activities.

All Data Controllers must be familiar with Schedules 1-18 of the UK GDPR as these are the lawful exemptions pertinent to many other legal frameworks and Acts. These Schedules cover things such as Parliamentary Privilege, Health, and Social Work, Criminal Convictions (Additional Safeguards), Research, Statistics and Archiving, and Education, Child Abuse, and include specific provisions for data processing within the Schedule(s).

For example Schedule 15: Powers of Entry and Inspection. This Schedule sets out the powers of the Information Commissioner's Office regarding warrant(s) issued by the courts which allow the I.C.O. to enter premises and inspect data field there, including the seizure of documents. Schedule 18 is where all the legislative changes, in all pertinent primary legislation, are found, including the repeal of the Data Protection Act 1998. As the Act is embedded into the organisation, Data controllers, their roles and responsibilities, will need to be reviewed and revised to ensure compliance.

Codes of Practice

The Act enhances the role of the Information Commission's Office (I.C.O.) in the compilation of such Codes and these will be available in due course. We must be regularly checking the I.C.O. website to keep up with current guidance.

The Policy

Section 2

This organisation believes that all data, required for the delivery of the service and the lawful running of the organisation must be collected, handled, maintained, and stored following the requirements of the UK Data Protection Act 2018.

The UK General Data Protection (UK GDPR) forms the basis of the Act but to be effective and compliant with its requirements, the Related Policy list should be viewed as core to this policy, as should Section 1 and the Related Guidance links.

Note: All Guidance from the ICO should be considered "Live Documentation" and regularly checked until all Codes of Practice and Guidance are issued. Working Party 29 known as WP29 is a representative body from each of the EU member states who have developed and worked on the Act. WP29 still sits and meets in the European Parliament until all of the complexities of the Act have been clarified and amended into law.

Lawful Bases

After due consideration, this organisation has determined that the following Lawful Bases are used in the collection of data

Data Protection Principles

The UK GDPR sets out the following principles for which this organisation is responsible

and must meet. These require that personal data shall be:

- Processed lawfully, fairly, and transparently about individuals
- Be collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary for the purposes for which they are processed.
- Accurate and where necessary kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- Personal data may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject to the appropriate technical and organisational measures required by the UK GDPR (the safeguards) to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

"The controller shall be responsible for, and be able to demonstrate, compliance with the principles" Article 5 (2) UK GDPR

Individual Rights

The UK General Data Protection Regulation (UK GDPR) says that, for information to be personal data, it must relate to a living person who is identifiable from that information (directly or indirectly). The context in which we hold information, and the way we use it, can have a bearing on whether it relates to an individual and therefore if it is the individual's personal data.

The UK GDPR provides the following rights for individuals:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights about automated decision-making and profiling

Subject Access Request

The right of access, commonly referred to as a subject access request or SAR, gives someone the right to request a copy of their personal information from organisations. This includes where they got their information from, what they're using it for and who they are sharing it with.

Individuals can request the personal information held by their employer, or former employer, such as details of their attendance and sickness records, personal development or HR records.

Organisations must respond to a SAR within one month of receipt of the request. However, this can be extended by up to two months if the SAR is complex.

Whether or not a subject access request (SARs) is received on a regular basis, it is important to be prepared and take a proactive approach.

This helps to respond to requests effectively and in a timely manner and comply with our legal obligations under the UK GDPR and Data Protection Act 2018 (DPA 2018).

We refer to the ICO guidance for employers when managing requests.

To deal with SARs effectively it is necessary to have adequate information management systems and procedures in place, and the information management systems to facilitate dealing with SARs. This enables easy location and extraction of personal data and allows us to redact third-party data where necessary.

The UK GDPR does not set out formal requirements for a valid request. Therefore, an individual can make a SAR verbally or in writing, including by social media.

Details of the requests received, particularly those made by telephone or in person are recorded.

When receiving a request verbally, it is likely there will be a need to contact the individual in writing in order to confirm their identity and check with the requester that their request has been understood correctly.

Individuals do not have to tell us their reason for making the request or what they intend to do with the information. However, it may help to find the relevant information if they explain the purpose of the request.

An individual may prefer a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. The UK GDPR does not prevent this, the organisation would need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this such as a written authority, signed by the individual, stating that they give the third party permission to make a SAR on their behalf.

There are also other mechanisms that may allow a third party to make a SAR on behalf of an individual, such as powers of attorney. If there is no evidence that a third party is authorised to act on behalf of an individual, there is no requirement to comply with the SAR.

Anyone has the right to make a complaint to the ICO about an infringement of the data protection legislation in relation to their personal data.

Subject Access Request Process

Step 1 Check that the Request is within the scope of the Data Protection Act

Step 2 Verify the identity of the data subject

Step 3 Clarify the request (if necessary)

Step 4 Calculate the deadline for the response

Step 5 Acknowledgement of receipt of Subject Access Request

Step 6 Search for information

Step 7 Review information considering possible exemptions

Step 8 Third Party consultation if needed

Step 9 Review and Approval by manager/ director/information governance team

Step 11 Respond to the Applicant

Step 12 Update Subject Access Request monitoring log

Freedom of Information requests

The Freedom of Information (FOI) Act gives any person the right to obtain information held by public authorities unless there are good reasons to keep it confidential.

Refer to the separate Freedom of Information Policy for further details

If the information required is their data the request must be made through a Subject Access Request under the UK Data Protection Act 2018 and not under the Freedom of Information Act 2000.

Sharing Information and Risk Assessment

Before sharing information we consider four key questions

- What is the purpose of information sharing — is there a clear objective that can best be achieved by sharing the information?
- What is the risk to individuals (both the subject of the information or any third parties) of sharing the information and is this risk proportionate to the benefits to the individual that will be achieved? This includes considering if there is a risk to individuals if the information is not shared.
- How will the information be shared?
- Is the information sharing going to be in line with the requirements of the UK Data Protection Legislation?

Refer also to the Co-operating with other providers Policy.

Information Security Management

Information security is essential for all types of confidential records, whether manual or electronic. We ensure staff takes basic precautions against information security breaches, such as not leaving portable computers, service user notes, or files in unattended cars or easily accessible areas.

Staff are made aware of data protection policies and procedures during their induction and receive further training on an annual and when-required basis.

Staff supervision, staff meetings Resident meetings, and guidebooks clearly emphasise the importance we put on the security of personal and sensitive information that we are required to collect by our regulators.

All files and portable equipment should be stored under lock and key when not being used. Staff should not take service user records home.

We use a secure Email system or equivalent for all our communications of sensitive personal data**.**

All staff receives training on information security management and how to share information safely.

Privacy Notices

This is a new requirement for data processing, it is an accessible information declaration that should set out clearly how we will gather, use handle, store, and process personal data.

The Code uses the term “Privacy Notice” to describe all the privacy information that you make available or provide to individuals when you collect information about them. It is often argued that people’s expectations able personal data are changing, particularly through the use of social media, the use of mobile apps, and the willingness of the public to share personal information via these platforms.

However, as an organisation, we are increasingly aware of the fragile trust which can be easily broken through data breaches and is therefore seeking transparency as a means of building trust and confidence with users of our services. It is in the spirit of the Act that privacy, transparency, and control become a given for users.

Being transparent by providing a privacy notice is an important part of fair processing. When planning a privacy notice, we need to consider the following:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

The Privacy notice must be easily understood by users of the service and include all of the above, it must also be easily visible so in this organisation, it will be displayed

[**SEE EXAMPLE** of Privacy Notice in Related Guidance]

Privacy and Electronic Communications Regulations (PECR)

This guide issued by the ICO covers specifically electronic marketing messages i.e. phone, fax, email, or text, and includes the use of cookies. It introduces specific roles on the above keeping such communication services secure and user’s privacy regarding traffic and location data, itemised billing, line identification, and directory listings

The UK Data Protection Act 2018 still applies if you are processing personal data. The PECR sets out some extra rules for electronic communications and please be mindful of electronic schedule systems which will also come under PECR

Transparency

We routinely handle information about the most detailed aspects of a person's health and personal life. This information is provided in confidence. Some of this information will be classed as a special category, which is sensitive information that needs more protection. Data protection legislation recognises the importance of this special category information. We have additional controls in place to protect it.

Acquiring and maintaining public trust and confidence is important to us. This ensures people feel comfortable in sharing their information so that practitioners can use it. This relationship of trust also sets expectations about how we inform people about the use of their personal information. It is therefore important that we provide transparent information, about what is happening to people's personal information, to build up their trust and confidence in our health and social care systems. We do not just assume people understand why information is collected and we ensure that we inform people of the reasons why certain information is collected.

We make it clear to people why certain information is shared inside and outside of our organisation. For example, the sharing of information for planning health and social care services or medical research purposes may not be obvious to people but being transparent about the use of personal information for secondary purposes can help inform people's expectations and build trust.

Necessity and proportionality – we have a clear reason for why it is necessary to use the information. We explain why we are processing the information, our legal basis and, if relying upon legitimate interests, what those interests are.

Data Protection By Design

This organisation has a general obligation to implement appropriate technical and organisational measures to demonstrate that we have considered the principles of data protection in our processing activities.

Any new systems of work or changes to our operational processes will involve consideration of how by default we as an organisation will have the necessary safeguards in place to prevent personal data from being disclosed in breach of the law. Explaining the steps we have taken to protect people's privacy within our transparency information (eg pseudonymising or anonymising information where possible) increases the levels of trust people have in our system.

Privacy Impact Assessment

It will be assessed whether a Privacy Impact Assessment is required, including assessing whether there is a high risk to people's data rights and taking into account the requirements of the UK Data Protection legislation.

A Privacy Impact Assessment may be required when the processing could result in a high risk to the rights and freedoms of individuals

A privacy Impact Assessment will include:

- Identification of data
- Evaluate the risks or breach
- Assess the Impact – the individual and organisation
- Devise Measures to mitigate risks
- Monitor review and update

The Data Controller is responsible for identifying when a Privacy Impact Assessment might be required.

Reporting Breaches

The designated data lead or data controller will assess whether there is a risk to people's data rights and freedoms and if there is, they will notify the ICO.

If personal data has been breached the designated data lead or data controller must ensure that the Data Breach Plan is followed.

Breaches must be reported to the ICO within 72 hours of their discovery even if the nature of the breach is not yet fully known.

In line with Regulation 20 of CQC Fundamental Standards, all persons affected by the breach should be notified as soon as possible after the breach has been identified. Support and advice should be provided where there is a risk present due to the breach. Regulation 20: Duty of candour - Care Quality Commission (cqc.org.uk)

If there has been a deliberate breach by staff, then the company's disciplinary processes will be invoked which could include treating the alleged breach up to and including an allegation of gross misconduct.

Deliberate or malicious breaches could result in legal proceedings and prosecution. See Appendix.

National Data Opt-Out

Under the national data opt-out planned to be implemented in April 2022, 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 care. For example, if this information is used for research or planning purposes.

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

As care providers, we do not share confidential patient information except to manage or deliver care. The new opt-out should not have a major impact on our Residents, but it is always important to treat people's confidential information sensitively. So, if someone has opted out of sharing their data, we will not use confidential patient information for planning or research purposes, to ensure we comply with opt-out legislation.

We are using the term “confidential patient information” as this is the term already used by the NHS where the opt-out is already in force. “Confidential patient information” applies to information about someone’s health *or* social care that can identify them. https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out

Harm arising from a lack of transparency

We understand that it is important to anticipate potential harms in the context of transparency when planning how to use people’s information.

Harm can be difficult to identify and quantify. However, it is clear that when people do not understand how we are using their personal information, this can cause anxiety or a loss of trust. This is particularly true given the sensitivities around the use of people’s health and social care information.

Psychological harms - when people do not understand the intended use of their health and social care information, this can result in fear, anxiety and embarrassment.

Loss of control of personal information - If people do not know what is happening with their information, they lose control of it. They are then less likely to share further important information

Lack of trust in services - a lack of transparency about how we use personal information might create anxieties that lead to people being reluctant to engage with our services. This, in turn, may negatively impact the health and social care they and others receive.

Potential societal harms are:

Damage to public health – if people choose not to share their personal information, this might lead to a general lack of availability of health and social care information. This might negatively impact medical research.

Failure of programmes with significant public benefit - where people are aware of a programme for the proposed use of their health and social care information but do not fully understand what will happen to it, this can lead to the spread of false or inaccurate information.

To prevent or reduce harm resulting from a lack of transparency, we identify the risks of failing to provide sufficient transparency material when using health and social care information.

How we provide Privacy and Transparency information

1. We publish privacy information and a privacy notice on our website and make every effort to inform people where they can find our privacy information either by email or within our service user guide. We notify people when we make

significant changes by signposting people to our website or notifying them directly.

2. We provide transparency information by making additional information available to people to demonstrate our openness and honesty. This gives us a prime opportunity to clearly explain how we will use people's information and to build trust and confidence. This information is in an accessible format where required and is given in the person's preferred format.
3. We use a variety of methods to provide transparency information
    - posters and leaflets
    - letters
    - emails
    - texts
    - social media and other advertising campaigns
    - website pop-ups and just-in-time notifications
4. We seek feedback from people who receive this information to ensure it is in a format they can easily understand, the quantity of information is acceptable and whether people are finding it overwhelming or too time-consuming. We review this feedback and adjust the amount or frequency as necessary.
5. We review and evaluate whether we are acting transparently under data protection law, based on our use of personal information and our transparency measures at regular intervals to

- Check that it actually explains what we do with people's personal data
- Ensure that it remains accurate and up to date.
- Ensure that people who use our service and their families are part of this review and that we respond to their feedback

6. We ensure that all staff members can provide people with or direct them to relevant information at the appropriate time.

Remember – if you have received information about someone from a third party, you still need to tell them you have the information and what you intend to do with it (see our detailed guidance below). In these circumstances, you may be more limited in the way you choose to inform people, as you may not be able to provide that information in person.

Data Security and Protection Toolkit (DSPT)

We update annually or when changes occur, our Data Security and Protection Toolkit (DSPT) to ensure it reflects our current data and cyber security arrangements, taking into account any changes and how we manage data throughout the year. We ensure the relevant staff are trained and competent to complete the toolkit.

Data Security and Protection Lead

This person takes overall senior responsibility for our data security and protection work. The Data Security and Protection Lead is **the Director.**

The core role of the Data Security and Protection Lead is to champion data security and protection good practice and ensure that it is implemented.

Staff at all levels complete basic data security and protection training. Senior staff with specific data security responsibilities complete enhanced training**.**

See the Confidentiality Policy for information on Caldicott Guardians who are responsible for protecting the confidentiality of people's health and social care records and making sure that they are used correctly. Any health and social care organisation which receives public funding should have a Caldicott Guardian**.**

File Retention

The UK GDPR sets out Guidance on files and retention including archiving, specifically Health and Social Care personal data is generally exempt.

As a provider of services, file and retention guidelines are in place from our Regulator which includes CQC and the NHS as well as Local Authorities via the Service Specification within any contractual arrangements.

A periodic check of the Regulator's Guidance should be part of the review of this policy.

Compliance

To meet the requirements of the Act a thorough knowledge of the Guidance should be the priority for the Data Controller.

It is also important that the Act is placed in the context of other compliance requirements namely The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 and all other lawful requirements such as Regulation 18 Staffing to name but one.

In recognition of the complexities of the Act, the ICO has set up an advice service for small organisations.

Related Policies

Adult Safeguarding

Accessible Information and Communication

Access to Records and Files

CCTV

Confidentiality

Consent

Cyber Security

Duty of Candour

Record Keeping

Related Guidance

Smaller Organisations ICO:
https://ico.org.uk/global/contact-us/contact-us-sme/

Guide to the UK General Data Protection (UK GDPR):
https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR-1-0.pdf
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR/

Records Management Code of Practice for Health and Social Care 2016:
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

ICO Data Protection Self-Assessment:
https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/data-protection-self-assessment/

Direct Marketing Guidance:
https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/

Guide to privacy and Electronic Communications Regulations (PECR):
https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/

Data Protection and the use of Criminal Offence Data for Employment and Education Purposes:
https://www.nacro.org.uk/

Regulation 20: Duty of candour - Care Quality Commission (cqc.org.uk)
https://www.cqc.org.uk/guidance-providers/all-services/regulation-20-duty-candour

Right of Access
https://ico.org.uk/right-of-access

Digital Care Hub: DSPT
https://www.digitalcarehub.co.uk/dspt/?mc_cid=7496c11fbb&mc_eid=2bc19b00d4

Transparency in Health and Social Care
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/transparency-in-health-and-social-care/

Training Statement

All staff, during induction, are made aware of the organisation's policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff is made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one-to-one, online, workbook, group meetings, individual supervisions, and external courses sourced as required.

Date Reviewed: May 2025

Person responsible for updating this policy: **B.KWANGWARI**

Next Review Date: May 2026

Appendix - TEMPLATE: Privacy Notice

[Company_Name] is a **[INSERT]** business, (owned by the…… family, part of the ……. Group) **[AMEND AS NECESSARY]**. This privacy notice explains how we use any personal information we collect about you, during the information gathering process known as an Assessment of Need. Topics covered are:

- What information do we collect about you?
- How do we use such information?
- Access to your information and correction

What information do we collect about you?

The nature of our service means that very personal and sensitive information is discussed, openly and honestly, to ensure we can meet your health and social care needs in ways that are unique to your circumstances. The specific type of information is required for us to meet our legal and regulatory obligations as a registered provider.

The Lawful Bases which we use are contained within the UK Data Protection Act 2018.

How information about you will be used

We may share information regarding your care with those who need to know, namely Health Professionals, such as GPs, District Nurses, Hospitals, etc., and Local Authorities, including departments such as Social Services, Housing, Day Centres, etc. Any relevant person identified by you, such as an L.P.A., and our staff. We would like to contact you about the services we provide, please indicate below your preferred contact method.

Post Email Phone SMS

We will not share your information with anyone except those indicated above unless required by law. If you do not wish this information to be shared, please indicate below.

Yes No

Personal information supplied to us is used in several ways, for example.

- To agree on a Care Plan
- To review your care needs
- To monitor your medication
- To help us improve our services

How will we use this information?

Upon completion of your Assessment of Need, we compile a Care Plan which sets out tasks, aspirations, and outcomes to meet all your identified needs and this is regularly reviewed and updated. This includes liaising with all those involved in your

care such as family, your representative relevant health and social care colleagues, and other professionals.

Access to your information and corrections

All files held in your name are available for your perusal and you can ask us to remove inaccurate information. Please email or write to us at (Insert contact details here). Where you use our website, cookies are text files that collect log-on information and visitor behaviour information. Cookies track visitor use and compile statistical reports on website activity. You can set your browser to accept or decline cookies. Please be aware that a decline in preference may mean a loss of function in some of our website features.

For further information on cookies visit: www.aboutcookies.org or www.allaboutcookies.org

NAME/SIGNATURE [Resident] TEL:

ADDRESS:

POSTCODE: D.O.B.

Appendix 2 Data Breach Plan

Preparing for a personal data breach

Allocated responsibility for managing breaches

The designated data lead or data controller will assess whether there is a risk to people's data rights and freedoms and if there is, they will notify the ICO.

Responding to a personal data breach

What data has been breached and whom does it affect?

What is the likely risk to individuals as a result of a breach?

Inform affected individuals about a breach when their rights and freedoms are at high risk.

Confirm names below.

***Affected individuals must be informed without undue delay**.

We have informed the relevant supervisory authority of our processing activities.

YES NO

If not, you must do so as soon as possible

Notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

Confirm that ICO has been informed within 72 hours

YES the ICO was informed within 72 hours	
NO, the ICO was not informed within 72 hours	
If NO – what action was taken?	

What information was given to the ICO about a breach?

What advice and Support have been provided to individuals to help them protect themselves from its effects?

Note - all breaches, even if they don't all need to be reported have been recorded.

Lessons learned and actions taken to prevent further breaches of this nature.

Signed:……

DP lead

Date:……