Data Protection (UK GDPR) (v2.0.0)

Date Reviewed: 13/01/2025 | **Next Review Date:** 13/01/2026

Person responsible for updating this policy: Hayley Southern

The Policy

The UK General Data Protection Regulation (UK GDPR) sets standards for protecting personal data and gives people more control over the use of their data.

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.

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

The Local Care believes that all data, required for the delivery of the service and the lawful running of The Local Care must be collected, handled, maintained, and stored following the requirements of the UK General Data Protection Regulation (UK GDPR).

TheUK General Data Protection Regulation (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 the Related Guidance links.

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 individual's, and 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 most pertinent bases for Health and Social Care data processing activity.

Lawful Bases

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

- **Consent:** the individual has given clear consent for us to process their personal 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 personal data which overrides those legitimate interests. (This does not apply if a public authority is processing data to perform its official tasks).

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

Consent and Individual Rights

Consent

Consent means offering individuals real choice and control. Consent practices and existing paperwork used within The Local Care meets UK General Data Protection Regulation (UK GDPR) 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 overreliance on the consent.

Note: Consent within this policy relates only to data processing not Health or Support in a Social Care context. The Local Care still uses consent as defined within The Mental Capacity Act 2005 to deliver our services. Refer to our Consent Policy for further details.

Individual Rights

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 Requests (SAR)

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.

The Local Care 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 General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

We refer to the Information Commissioner`s Office (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 General Data Protection Regulation (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.

Service Manager

An individual may prefer a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. TheUK General Data Protection Regulation (UK GDPR) does not prevent this, The Local Care 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 Information Commissioner`s Office (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 2018
- 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 data controller/ 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 Act 2000 gives any person the right to obtain information held by public authorities unless there are good reasons to keep it confidential. If the information required is their data the request must be made through a Subject Access Request under the UK General Data Protection Regulation (UK GDPR) and not under the The Freedom of Information Act 2000.

Refer to the separate Freedom of Information Policy for further details.

UK Data Protection Principles

The UK General Data Protection Regulation (UK GDPR) sets out the following principles for which The Local Care 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 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) GDPR.

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 service user 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 (Microsoft Outlook) 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 and Privacy and Electronic Communications Regulations (PECR)

Privacy Notices

Privacy notices are 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, The Local Care 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 The Local Care it will be displayedon our website www.thelocalcare.co.uk

Privacy and Electronic Communications Regulations (PECR)

The Local Care does not fall under the scope of the Privacy and Electronic Communications Regulations (PECR). Therefore, we focus on adhering to other applicable data protection laws and ensuring transparency and responsibility in our data handling practices.

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 The Local Care. 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

The Local Care 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

Hayley Southern is responsible for identifying when a Privacy Impact Assessment might be required.

Reporting Breaches

Hayley Southern will assess whether there is a risk to people's data rights and freedoms and if there is, they will notify theInformation Commissioner`s Office (ICO) .

If personal data has been breached Hayley Southern must ensure that the Data Breach Plan is followed.

Breaches must be reported to the Information Commissioner`s Office (ICO) within 72 hours of their discovery even if the nature of the breach is not yet fully known.

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.

If there has been a deliberate breach by staff, then the The Local Care 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.

National Data Opt-Out

Under the national data opt-out, everyone who uses publicly-funded health and/or care services can stop health and care organisations from sharing their 'confidential patient information' with other organisations if it is not about managing or delivering their 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 the service user, 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.

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

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.

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.

We use a variety of methods to provide transparency information

- posters and leaflets
- letters
- emails
- texts
- social media and other advertising campaigns

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.

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

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

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.

File Retention and Records Management

File Retention

The UK General Data Protection Regulation (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 Care Quality Commission (CQC) and the NHS as well as the Local Authority (LA) 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.

Records Management Code of Practice for Health and Social Care 2016

This Code of Practice is for **providers working under contract to the NHS** and the storage and disposal times are different from those above. Appendix 3 of the code (which can be accessed via the related guidance section of this policy) contains the detailed retention schedules. It sets out how long records should be retained, either due to their ongoing administrative value or because of statutory requirements.

Refer to the Record Keeping Policy for details.

Compliance and Codes of Conduct

Compliance

To meet the requirements of the Act a thorough knowledge of the Guidance should be the priority for our data controller, Hayley Southern .

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

We will ensure we refer to the Information Commissioner`s Office (ICO) for the latest updates, changes and recommendations.

Codes of Conduct and Certification Mechanisms

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 Information Commissioner`s Office (ICO) will develop its code of conduct as it has already worked with the Direct Marketing Commissions Code of Conduct: DMA Code.

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 are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one to one, online, group meetings, individual supervision and external courses are sourced as required.

Related Policies

- Access To Records And Files (Domiciliary)
- Adult Safeguarding (Domiciliary)
- Confidentiality (Domiciliary)
- Consent (Domiciliary)
- Cyber Security (Domiciliary)
- Duty Of Candour (Domiciliary)

Related Guidance

- ICO: Smaller Organisations
- ICO: Guide to the General Data Protection Regulation (GDPR)
- ICO: Data Protection Self-Assessment
- ICO: Direct marketing Guidance
- ICO: Guide to privacy and Electronic Communications Regulations (PECR)
- Data Protection and the use of Criminal Offence Data for Employment and Education Purpose
- NHS England - Transformation Directorate
- CQC: Regulation 20 - Duty of Candour
- NHS England: Data Security and Protection Toolkit
- ICO: Rights of Access
- NHS England: Records Management Code of Practice for Health and Social Care
- Digital Care Hub: DSPT
- ICO: Transparency in Health and Social Care

Policy Legal Statement