Data Protection GDPR POLICY

Title of Policy Document **Issue Date and Version**	Data Protection GDPR September 2022 (Version 1)
Author / Department	Executive Management Team / Health and safety
Signed off by	 Director
Next review date	September 2024
Has Equality Impact Assessment been completed?	N/A
Distribution	All services
First issue date	September 2022

DATA PROTECTION AND INFORMATION GOVERNANCE
Corporate Policy

1. Data Protection Legislation and Information Governance Standards

Data is a vital asset, both in terms of the effective provision of care and support to individual service users and the efficient management of services, resources and performance management. It is therefore of paramount importance that the appropriate policies, procedures and management accountabilities are in place to provide a robust governance framework for information management and data protection.

The European Union's General Data Protection Regulation (GDPR) comes into force on 25th May 2018 and the UK's Data Protection Act 2018 comes into force on the same date. The terms of the GDPR and the Data Protection Act 2018 will remain legally applicable to the UK, irrespective of the UK's exit from the European Union.

Practice covering the processing of personal information in social care is governed by the following legislation and guidance:

- The *Data Protection Acts 1998* and *2018*
- The *General Data Protection Regulation* (GDPR) (Regulation (EU) 2016/679)
- *Data Protection (Processing of Sensitive Personal Data) Order 2000*
- *Freedom of Information Act 2000*
- *Computer Misuse Act 1990*
- *Privacy and Electronic Communications Regulations 2003*
- *Caldicott Recommendations*
- NHS Codes of Practice, including; *Confidentiality: NHS Code of Practice (DOH 2003)*
- *Human Rights Act 1998*
- *Public Records Act 1958*
- *Records Management Code of Practice for Health and Social Care* (DOH, 2016)
- *A Guide to Confidentiality in Health and Social Care* (HSCIC, 2013)
- The HSCIC *Checklist Guidance for Reporting, Managing and Investigation Information Governance and Cyber Security Serious Incidents Requiring Investigation (SIRI)*.

2. Corporate Responsibility for Data Protection and Information Governance

Senior Information Risk Owner

The SIRO for Nurse24 Ltd is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality functions. The role includes briefing the Board of Trustees and providing assurance through the Finance and Audit Committee that the IG approach is effective, that all IG-related incidents are reported and followed up appropriately and that where appropriate, SIRI's are reported through the IG Toolkit.

Nurse24 Ltd is not legally required to have a Data Protection Officer but the SIRO fulfils this function.

Caldicott Lead

The Caldicott Lead has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles

Information Governance Lead

The Information Governance Lead has day-to-day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation.

The Information Governance Lead is responsible for coordinating and chairing the Information Governance Management Group and for the implementation of the IG Annual Improvement Plan.

3. Personally Identifiable Information

"Personal data", or "personally identifiable information" (PII) is defined as any data that can be used to identify an individual person, either on its own or in conjunction with other accessible data on that individual. This definition includes digital information (such as an IP address) and can also extend to pseudonymised data, where this can still be linked to an individual.

As a social care provider and employer, Nurse24 Ltd processes PII on its employees. The control and processing of all such data is regulated by the Data Protection Act and GDPR.

4. Individual Rights under Data Protection Legislation

Under the GDPR, all individuals have the following rights in relation to the processing of their personal information:

1. ***The right to be informed*** - Individuals have the right to be informed how and for what purposes their personal data will be processed.
2. ***The right of access*** - Individuals have the right to access their personal data and supplementary information, and to be made aware of and verify the lawfulness of the processing.
3. ***The right to rectification*** - Individuals have the right to have their personal data rectified if it is inaccurate or incomplete.
4. ***The right to erasure*** - Also known as 'the right to be forgotten'. This is the right of individuals to request the deletion or removal of personal data where there are no compelling reasons for its continued processing.
5. ***The right to restrict processing*** - Individuals have the right to permit the storing of their personal data, but to restrict any further processing; for example, when an individual contests its accuracy.
6. ***The right to data portability*** - Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
7. ***The right to object*** - Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interests/exercise of official authority (including profiling), direct marketing, and the processing of their personal data for purposes of scientific/historical research and statistics.
8. ***Rights in relation to automated decision making and profiling*****.** - These rights protect individuals from any automated decision making (i.e. decisions made solely by automated means without any human involvement, and profiling (i.e. automated processing of personal data to evaluate certain things about an individual.

Further information on these rights is available via the Information Commissioner's Office at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Nurse24 Ltd have issued comprehensive privacy statements to all employees which explain how their rights will be protected, and the procedures that will be followed to ensure that the privacy of their personal data is protected at all times. The privacy statements are appended to this policy (Appendix 2) and can also be downloaded from www.nurse24.uk

5. The Legal Bases for Processing Data

The GDPR (Article 6) requires data controllers to specify their lawful basis for processing of personal data. Under the Data Protection Act 1998, Nurse24 Ltd was able to process data on the basis of consent, with staff having given their express permission for us as a social care provider/employer to do so. Under the GDPR (Article 7 and Recital 43), however, it is no longer permissible to use consent as a legal basis when this is given as a condition for the provision of a service or employment. This is because the consent cannot be regarded as freely given, "where there is a clear imbalance between the data subject and the controller" as exists between Nurse24 Ltd and its employees.

From September, 2018 Nurse24 Ltd will, therefore, use the following legal bases for the processing of personal data:

1. Pursuant to GDPR Article 6(1)(b) that the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract
2. With respect to sensitive categories of personal data, as defined in Article 9(1) of the GDPR, pursuant to GDPR Article 9(2)(h) that the processing is necessary for the provision of health or social care
3. With respect to the processing of personal data relating to criminal convictions and offences, pursuant to GDPR Article 10, processing is authorised by State law; namely the UK Data Protection Act 2018, Schedule 1, thatthe processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.
4. For all other information held, eg. Ex-employee information we will rely upon legitimate interests of the organisation pursuant to GDPR Article 6(1)(f)

Article 9 of the GDPR places restrictions on the processing of personal data revealing any of the following:

1. Racial or ethnic origin
2. Political opinions
3. Religious or philosophical beliefs
4. Trade union membership
5. Genetic data
6. Biometric data for the purpose of uniquely identifying a natural person
7. Data concerning health
8. Data concerning a natural person's sex life or sexual orientation

These categories are classed as "special categories of data" that can be processed only if one or more of the following applies:

A. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes
B. Processing is necessary for the purposes of carrying out the obligations of and exercising specific rights of the controller or of the data subject in the field of employment
C. Processing is necessary to protect the vital interests of the data subject (i.e. it is necessary to project their life) or of another natural person where the data subject is physically or legally incapable of giving consent
D. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
E. Processing relates to personal data which are manifestly made public by the data subject
F. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
G. Processing is necessary for reasons of substantial public interest
H. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the

provision of health or social care or treatment or the management of health or social care systems and services

I. Processing is necessary for reasons of public interest in the area of public health
J. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The legal basis for processing these special categories of employee data is outlined below.

Processing Special Categories of Employee Data

The special categories of personal data processed by Nurse24 Ltd on its employees are; racial and ethnic origin, trade union membership, gender, and sexual orientation. Wherever employees are asked to disclose data about these special categories of their data, the right to withhold this from Nurse24 Ltd will be made explicit to them at the point of collection, and the consent to process it will likewise be requested when it has voluntarily been disclosed.

As an employer committed to the promotion of equal opportunities, Nurse24 Ltd will request the consent of employees to process information on their sexual orientation, gender identity or expression, should they choose to disclose it. Employees are under no legal or professional obligation, however, to disclose their sexual orientation, gender identity or expression to Nurse24 Ltd, and their right to privacy in these matters will be respected and upheld.

Information on employees' trade union membership is accessed only by the Payroll department for the purposes of processing subscription fees, and may be disclosed to members of the Human Resources department in disciplinary or grievance cases where employees have been offered the opportunity for union representation.

6. Data Protection by Design

Any employee processing personally identifiable information for Nurse24 Ltd must ensure that:

- only the minimum necessary personal data is processed
- that pseudonymisation is used wherever possible
- that processing is transparent (where feasible, allowing individuals to monitor what is being done with their data)

"Pseudonymisation" refers to the use of other identifying data in place of individuals' names (such as an employee number) where it is not necessary for that processing activity to disclose names, e.g. for the purposes of compiling reports or statistical information.

More details on the process of data protection by design can be found in the *Procedure for the Management of Personal and Sensitive Information* policy document.

7. Processing Data in Services: Principles of Privacy and Confidentiality

Employee data

Supervision files in services must be kept in a locked filing cabinet, with access restricted to the line manager, service manager and relevant administrative staff where appropriate.

Staff telephone numbers and addresses must not be kept in any accessible phone books or card indexes on view in the service. If enquiries are made about a member of staff the enquirer's name should be taken and the member of staff informed. Staff are instructed never to give out staff telephone numbers or addresses where there is doubt as to the enquirer's identity, or to whether the individual has consented to their personal information being shared. If staff have any doubts as to what action they should take, they should pass the query to their line manager or a member of the Human Resources Team during normal office hours, or to the relevant on call or the Out of Hours service at any other time.

Sick notes are confidential documents and should be handed to a line manager, Payroll, or a member of the Human Resources Team, in a sealed envelope marked "Private & Confidential".

Enquiries from statutory authorities for information about staff (e.g. Police), should always be referred to the Human Resources Department or the relevant line manager/Service Director.

8. Subject Access Requests

Nurse24 Ltd is committed to working in an open and honest manner with our employees. As per Article 15 and Recital 63 of the GDPR, data subjects have, "the right of access to [their] personal data...and to exercise that right easily and at reasonable intervals, in order to be made aware of, and verify, the lawfulness of the processing". This right will be protected and upheld for all employees as described below.

Employee Data

Employees may request to see their personal data that is processed by Nurse24 Ltd, and to know our reasons for doing so. This is called a "subject access request", which an employee can make by submitting a *Request for a Copy of Information Held on an Individual* form (Appendix 1) to the organisation's the Data Protection Lead or the Personnel Manager.

Information requested by the employee will be provided as soon as possible and no later than one month after the receipt of the form named above. We aim to provide a copy of the data requested within five working days of receipt of the written request. If you have any particular needs, we will endeavour to provide the information you have requested in an accessible format (e.g. providing large print copies for those with sight loss).

Employees making subject access requests must specify when making their request specifically which items of personal data it is they wish to see.

There will be no charge to the employee for making a subject access request, unless the request is manifestly unfounded, excessive or repetitive, in which case a fee may be charged.

Employee data contained in confidential references or Disclosure and Barring Service (DBS) Checks

Nurse24 Ltd uses the Disclosure & Barring Service (DBS) to help assess the suitability of applications for positions of trust. Nurse24 Ltd complies fully with the DBS code of practice and care standards recruitment requirements.

Confidential references received by Nurse24 Ltd are not exempt from data subject access requests. However, in deciding whether to disclose information, it is necessary also to consider the data privacy rights of the referee. Information contained in or about a confidential reference need not be provided if the release of the information would identify an individual referee unless:

- The referee has given his or her consent
- The identity of the referee can be protected by anonymising the information
- It is reasonable in all the circumstances to release the information without consent.

Even if a referee states that they do not want their comments to be shared, we are obliged to provide the reference to the subject if it is reasonable in all the circumstances to comply with the request without the referee's consent. In considering whether it is reasonable, the Information Commissioner's Office (ICO) advises that, as data controllers, we should take account of factors such as:

- Whether the referee was given express assurances of confidentiality ● Any relevant reasons the referee gives for withholding consent
- The potential or actual effect of the reference on the individual
- The fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
- That good employment practice suggests that an employee should have already been advised of any weaknesses
- Any risk to the referee.

Nurse24 Ltd cannot refuse to disclose information from a confidential reference without giving a reason.

If disclosure of a reference would identify only the organisation that has given the reference rather than a specific individual, disclosure would not be an issue.

9. Principles of Information Governance

Nurse24 Ltd recognises the need for an appropriate balance between openness and confidentiality in the management and use of information, while seeking to work within the legal framework as outlined above. Nurse24 Ltd recognises the duty to share accurate information with other health organisations and other agencies in a secure and legally compliant manner consistent with the interests of employees and in some circumstances, the public interest. Equally important is the need to ensure high standards of data protection and confidentiality to safeguard personal and sensitive (including commercially sensitive) information. Underpinning this is the integrity needed for electronic and paper information to be accurate, relevant, and available to those who need it.

Staff must ensure at all times that high standards of data quality, data protection, integrity, confidentiality and records management are met in compliance with the relevant legislation and NHS guidance. It is the responsibility of all staff to familiarise themselves with this policy and adhere to its principles.

There are four key interlinked strands to the Information Governance policy:

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

Openness

Non-confidential information on Nurse24 Ltd and its services will be made available to the public through a variety of media, in line with Nurse24 Ltd's code of openness.

Nurse24 Ltd will establish and maintain policies to ensure compliance with the Freedom of Information Act.

Nurse24 Ltd will have clear procedures and arrangements for liaison with the press and broadcasting media.

Legal Compliance

Nurse24 Ltd regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

Nurse24 Ltd will establish and maintain policies to ensure compliance with the GDPR, the Data Protection Act, Human Rights Act, common law confidentiality and other relevant legal codes and requirements.

Information Security

Nurse24 Ltd will establish and maintain policies for the effective and secure management of its information assets and resources.

Nurse24 Ltd will promote effective confidentiality and security practice to its staff through policies and training.

Nurse24 Ltd will undertake an annual review of its information security and business continuity arrangements and this will be reported to the Board of Trustees.

Nurse24 Ltd will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

10. Information Governance Management

The framework for the management of Information Governance combines both corporate and clinical governance, and as such is wider in scope than data protection, also incorporating records management, information risk, information security, risk management, and business continuity.

The defined standards undertaken by Nurse24 Ltd in accordance to information governance are as follows:

- There is senior ownership of data security and protection within the organisation.
- There are clear data security and protection policies in place and these are understood by staff
- Individuals' rights are respected and supported (GDPR Art 12-22)
- Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30)
- Personal information is used and shared lawfully.
- The use of personal information is subject to data protection by design and by default
- Effective data quality controls are in place
- Personal information processed by the organisation is adequate (and not excessive) for the purposes.
- There is a clear understanding of what Personal Confidential Information is held.
- Personal Confidential Information is processed/shared legally and securely.
- Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.
- There has been an assessment of data security and protection training needs across the organisation.
- Staff with specialist roles receive data security and protection training suitable to their role.
- The organisation maintains a current record of staff and their roles.
- All staff understand that their activities on IT systems will be monitored and recorded for security purposes.
- All networking components have had their default passwords changed.
- Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities.
- The organisation can name its suppliers, the products and services they deliver and the contract durations.

APPENDIX 1

REQUEST FOR A COPY OF INFORMATION HELD ON AN INDIVIDUAL

REQUEST FOR A COPY OF INFORMATION HELD ON AN INDIVIDUAL

As part of Nurse24 Ltd's compliance with the Data Protection legislation, each person who has a relationship with the company has the right to be provided with a copy of the current personal information held on them for data processing.

We will endeavour to provide a copy of the data requested within five working days of receipt of the written request; some requests may require more time to collate all the information. In all instances we will respond promptly and, in any event, no later than one month from receipt of the written request, as stipulated in the legislation.

Please read the policy on *Data Protection and Information Governance* (and appended privacy statement) which lists all the types of personal data that may be held on you.

Please complete this form and submit to either Julie Cooke, Service Director, or the Personnel Manager. This request will be processed and therefore comes under the provisions for data processing, to which you are giving your explicit consent.

Your Name:

_____

The Data/information of which you require a copy:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Your signature: **Date:**

Date received by Head Office:

Considered by: **Date:**

Outcome:

APPENDIX 2

PRIVACY STATEMENTS

Privacy statement for Nurse24 Ltd employees

As of September 2018, Nurse24 Ltd exercises its right under the General Data Protection Regulation (GDPR) to control and process personal information about its employees. We process this data as it is necessary to perform the contract of employment held between Nurse24 Ltd and its employees.

Your privacy is of the utmost importance to us, and data protection is built into our processing at every stage. This means that while we do not require your consent in order to process your personal data, we will only retain and use personal data when we have a legally justifiable reason for doing so that balances our interests as an employer with your rights as an employee.

Your personal data is shared only with those departments within Head Office, and external organisations who also have a legal basis for using it in order to fulfil our obligations to you as an employee. We never sell or share your information with any organisations for marketing purposes. Nurse24 Ltd do not use your personal data for any automatic profiling or decision making.

You have the right to see what personal information Nurse24 Ltd processes about you, and to know our reasons for doing so. In turn, Nurse24 Ltd has an obligation to keep information about you accurate and up-to-date. If you become aware of any information we hold about you that is inaccurate, or if any of your personal details have recently changed, please notify us and we will update our records accordingly.

You have the right to request to see all your personal information that Nurse24 Ltd records and processes, using a “Request for Copy of Information Held on an Individual” form appended to the corporate *Data Protection and Information Governance* policy.

You have the right to “data portability” with respect to your personal information, which means that you may request for it to be sent to you in a format that can be moved, transferred or copied across different services.

The types of personal information we process include:

- personal details, i.e. names, addresses, contact numbers, date of birth
- family details, i.e. marital status, next of kin and emergency contacts (including your GP)
- nationality
- whether you have a current driver’s licence
- whether you are registered as disabled
- bank account details

We also process sensitive categories of personal information that may include: ●

- racial and ethnic origin
- trade union membership
- information about your mental or physical health, insofar as this pertains to your job role
- sexual orientation

Nurse24 Ltd will not record or process information about your political or religious opinions, philosophical beliefs, sexual orientation or gender identity, or any other categories

of personal information named in Article 9 of the GDPR, except where you have disclosed this information and given us your explicit consent to record and process it.

You have the right to “data portability” with respect to your personal information, which means that you may request for it to be sent to you in a format that can be moved, transferred or copied across different services.

Nurse24 Ltd will not transfer any of your personal data outside of the European Union.

If you have any further questions, please contact our director..

Email: gdpr@nurse24.uk

You have the right to log a complaint with the Information Commissioner’s Office (ICO) if you have any concerns about the way that Nurse24 Ltd is using your personal information. More information can be found at the ICO’s website at https://ico.org.uk/concerns/ or by calling their helpline on 0303 123 1113.