GDPR Policy

Author:	ED	Distribution:	All staff
Reviewed by:	GSC	Date of review:	January 2026
Approved by:	ED	Next Review due:	December 2027

1. Purpose

The purpose of this policy is to ensure the collection, processing and storage of data is compliant with the terms of the Data Protection Act 2018 (the "DPA"). The DPA contains the UK's implementation of the General Data Protection Regulation (GDPR). This Policy outlines the data protection principles and the responsibilities of those working for or on behalf of Shipston Home Nursing (SHN) to comply with GDPR.

This Policy also demonstrates SHN's commitment to obtaining and sharing information in accordance with the common law duty of confidence, Article 8 of the Human Rights Act 1998 (right to respect for private and family life) and the Caldicott Principles.

To ensure that everyone who works within SHN (including any volunteers who have access to personal data) is clear that it is a requirement within the common law duty of confidence and the GDPR to safeguard confidentiality and preserve information security.

2. Scope

This policy applies to all staff who work on behalf of SHN including bank staff, contractors and private providers as well as volunteers.

3. Background

Personal data is information relating to an individual, which enables that person to be identified. As well as including information about name, address, email address, date of birth, NHS and National Insurance numbers, private and confidential information which includes clinical information. It includes any expression of opinion or intention towards the individual. It also includes sensitive personal data, which is information relating to the person's racial or ethnic origin, political opinions, religious or similar

beliefs, trade union membership, physical or mental health, sexual life, the commission of offences or criminal proceedings.

SHN needs to collect personal data about patients, their families, staff, volunteers, complainants, supporters, and enquirers (past, present and prospective). The contents of this policy relate to people living and deceased.

All users of personal data within SHN have a legal obligation to comply with all appropriate legislation about processing personal data, including maintaining the confidentiality of that information. SHN will use all appropriate and necessary means to ensure that it complies with the GDPR and any associated Codes of Practice issued by the Information Commissioner's office and guidance issued by the Department of Health, the NHS Executive, other advisory groups to the NHS. GDPR gives individuals the right to know what information is held about them and provides a framework to ensure that personal data is handled correctly and legally.

The GDPR requires that all personal data be processed by a Data Controller according to the six principles outlined below. A data controller is a person who determines the purposes for which, and the way, personal data is to be processed. For the purposes of the Data Protection Act 1998, GDPR 2018. SHN has appointed a Trustee as the Data Controller who is registered as such with the Information Commissioner's Office.

GDPR legislation states that anyone who processes personal data must comply with the six data protection principles defined within it as follows:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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;
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which 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 periods insofar 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 implementation of the appropriate technical and organisational measures

required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

4. Procedures - Employees (and others connected with SHN, including volunteers)

All employees and others connected with SHN must understand the purposes for which SHN uses personal information and must obtain, process, and use personal data in a fair and lawful way.

5. Confidentiality

SHN attaches great importance on the confidentiality of the personal information collected. Personal information includes clinical information and therefore:

- Access to personal information must be on a need-to-know basis.
- All person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted, or disposed of.
- Personal information, wherever possible, must be anonymised by removing as many identifiers as possible.
- Personal data is held together in the Nurse Coordinator (NC) handover file which is always in the possession of a Nurse Coordinator or the Head of Nursing Services who individually remain responsible for ensuring its contents remain confidential when in their possession.
- All staff have a clause in their contract which includes a commitment to confidentiality and have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff within SHN will be expected to sign a Confidentiality and Data Protection Agreement obligating them to adhere to this Policy.
- Deliberate unauthorised use of (including access to, copying, destruction, or alteration of or interference with) any computer equipment or data is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

The functional heads are responsible for ensuring that all staff receive appropriate training.

6. Personal Responsibilities

All staff and volunteers may encounter information which is confidential. Everybody is expected to protect and keep anonymous all personal information, only retaining that information whilst necessary and never divulging that information to people other than those who need to know it within SHN or those directly responsible for the healthcare or wellbeing of a person (such as another nurse caring for that patient).

All confidential information must be carried and transported in a non-transparent container i.e., windowless envelope, suitable bag, etc. prior to being taken out of a patient's home. All confidential information must be kept out of sight whilst being transported. To ensure the safety of confidential information it must always be kept on the person whilst travelling. The member of staff is responsible for ensuring the information is kept secure and confidential in their home and elsewhere. This means that other members of the household or friends/colleagues must not be able to see the content or have any access to the information. No person-identifiable or confidential information should be left unattended.

You must not talk about person-identifiable or confidential information in public places or where you can be overheard.

All staff and those connected with SHN that have access to personal data must ensure that PC's, laptops, tablets, phones and any other equipment can only be accessed by themselves. All equipment must be password protected. SHN staff must use their SHN and or NHS e-mail address, and where using shared equipment their own user accounts. Passwords, logins or other information which would allow access for an unauthorised person, should not be saved or stored on any equipment. Equipment should never be left unattended whilst logged on to any application through which access may be gained to confidential information.

Loss of any information or equipment containing personal data or the discovery that unauthorised access to personal data has taken place must be reported to the Head of Nursing Services or the Nominated Individual as soon as it is discovered

SHN clinical staff are expected to participate in induction, training and awareness sessions intended to inform and update the nursing bank on confidentiality issues.

Social media must not be used to share personal data online. SHN Nurses must be familiar with and at all times act in accordance with the recommendations from the NMC. This can be viewed or downloaded on the following link:

http://www.nmc-uk.org/Nurses-and-midwives/advice-by-topic/a/advice/social-networking-sites/

7. Storage of Confidential Information

If personal data in paper form exists and not required to be kept in the patient's home, is held together in the Nurse Coordinator's handover file, which is always in the possession of Nurse Coordinator or the Head of Nursing Services who individually remain responsible for ensuring its contents remain safe and confidential when in their possession.

The Head of Nursing Services remains responsible for ensuring the safe storage and destruction of personal information once it is no longer required in the Nurse Coordinator handover file.

Staff employment records are held digitally on the appropriate cloud based system.

8. Disclosing Confidential Information

Clinically relevant information will be shared on a 'need to know' basis within our clinical team so that those involved in providing care are aware of the things they need to know before they start to provide that care. All clinical information will be communicated to clinical staff in clinical meetings or individually by telephone in addition to the information contained within the patient's notes on EMIS.

SHN recognises the need to share personal information with other health organisations in a controlled manner consistent with the interests of the person it concerns. Information must only be shared with the appropriate people in appropriate circumstances and care must be taken to check they have a legal basis for access to the information before releasing it.

Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required and only the minimal amount necessary should be disclosed. Recipients of disclosed information must be aware that it is given to them in confidence.

There are several exemptions in GDPR legislation which allow for disclosure to third parties in the public interest even where this would otherwise contravene the Act.

Those of most relevance to SHN include:

- Where disclosure is necessary for the prevention or detection of crime;
- A limited exemption for research unconnected to the individual;
- Where reporting improper conduct or malpractice to a regulator; and
- Where necessary in connection with legal proceedings or obtaining legal advice.

This is not an exhaustive list and there are other exemptions within the Act which may be applicable. The decision to use an exemption from the non-disclosure provisions will be made on a case-by-case basis; therefore, you must seek advice before disclosing information on this premise.

Patients have a right to access their records held by SHN. A patient must be allowed to read the records or have a copy of the documents provided to them on request. Any such request should be passed to the Head of Nursing for discussion and approval.

The relatives of deceased patients may have a right of access to patient's records on request. The patient's relative must be an Administrator of the patient's estate or have power of attorney for the patient's affairs. Any such request must be made in

writing and passed to the Executive Director and or Executive Committee for approval.

If the decision is taken to disclose information, that decision must be justified and documented and with the permission of the relevant licence holder, for example South Warwickshire University NHS Trust. Relatives will be required to sign a formal handover document.

Information can be disclosed when effectively anonymised or when the information is required by law or under a court order. In this situation you must discuss this in the first instance with the Executive Director/Nominated Individual before disclosing.

If you have any concerns about disclosing information you must discuss this with the Executive Director/Nominated Individual. Where appropriate, advice should be sought from other sources including the Caldicott Guardian or Data Controller.

9. Monitoring and Reporting Policy Breaches

Any act which results in the disclosure of personal information to anybody not strictly entitled to that information will be in breach of this policy and could result in disciplinary action. If you are unsure, do not disclose any information and discuss your concerns with the your line manager and the Executive Director

Any person who suspects that there has been a breach in confidentiality or any of the data protection principles defined by GDPR must report it to the Executive Director in the first instance who will initiate an incident report. It is important that if anybody is aware of any vulnerability in our policy and processes which could potentially result in confidentiality breaches, they raise their concerns with the Executive Director/Nominated Individual or the Data Controller.

10. Monitoring the Effectiveness of this Policy

SHN's GDPR Policy will be monitored by the Quality and Development Lead. This will include compliance with the defined KPIs and any resultant improvement plans.

11. Related Policies

Privacy Policy

Social Media Policy

Record Keeping Policy

12. References

UK GDPR

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

Guidance relating to The Caldicott Principles –
www.hpa.org.uk/web/HPAwebandHPAwebStandard/HPAweb_C/1195733746440