Data Protection Policy

Version History:

Version	Date	Author	Reason for change
.01	Mar 20	Isla Kaye	Policy created for CCG DPO Service
.02	Mar 22	Isla Kaye	Policy review
.03	May 23	Isla Kaye	Policy review
.04	June 23	Jodie Stutely	Removed CCG reference and added 8th Caldicott Principle

Next review date:

June 2025

Contents:

STATEMENT OF OVERARCHING PRINCIPLES

All Policies, Procedures, Guidelines and Protocols of the NHS Suffolk and North East Essex Integrated Care Board's (SNEEICB) DPO Service are formulated to comply with the overarching requirements of legislation, policies or other standards relating to equality and diversity.

1. Introduction

The UK General Data Protection Regulation (UK GDPR) (EU) 2016/697 and the Data Protection Act 2018 (DPA) addresses the rights and freedoms of living individuals and in particular their right to privacy in respect of personal information. The Act strengthens and extends the data protection legislation originally defined by the Data Protection Act 1984 & 1998, which has now been repealed.

The GDPR has seven principles, that Personal Confidential Data (PCD) must be processed:

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.
5. For only as long as it is needed.
6. Securely.
7. Accountability

Furthermore, Data Subjects have increased rights to:

1. Information about how their information is being processed.
2. Access to their information.
3. Rectification when information is wrong.
4. Be forgotten; when it is appropriate to do so.
5. Restrict processing.
6. Data portability.
7. Object to processing.
8. Appropriate decision making.

In health and social care, the Caldicott Principles reflect these, by stating that when using PCD, staff must observe the following:

1. Justify the purpose(s).
2. Don't use it unless it is absolutely necessary.
3. Use the minimum necessary.
4. Access should be on a strict need to know basis.
5. Everyone with access to it should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality
8. Inform patients and service users about how their confidential information is used

The Practice has a legal obligation to comply with all appropriate legislation in respect of data, information and IT security. It also has a duty under the establishment order to comply with guidance issued by The Department of Health, the NHS Executive and other advisory

groups to the NHS and guidance issued by professional bodies. The Practice believes that an individual's right to confidentiality is of vital importance. This document is a statement of the policy and principles adopted by the Practice, governing the processing of personal data as specified in the DPA.

Conformance with the DPA is part of the Practice's overall duty of confidentiality towards its patients, staff and all other individuals with whom it may effectively work in collaboration.

Non-compliance with the relevant legislation could result in individuals, employees and the Practice being investigated and subsequently prosecuted for offences under the DPA.

2. Purpose

This policy aims to ensure that the Practice fully complies with current legislation and guidance in relation to the handling of person identifiable data.

This policy also aims to make staff aware of their obligations in relation to the processing of personal data.

3. Scope

This policy applies to and must be adhered to by all employees of the Practice, regardless of grade or profession, including all directly employed, bank, locum, agency, contractors, seconded staff, volunteers and any other iteration of personnel that could legitimately be considered staff.

The policy covers all aspects of business relating to personal information within the Practice and is not solely patient related.

The policy covers all methods of holding information and all media used to store this.
For the purposes of this policy confidential information shall include any restricted data relating to the Practice, its agents, customers, prospective customers, suppliers or any other third parties connected with the Practice.

4. Acronyms and abbreviations

DP	Data Protection
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
FOIA	Freedom of Information Act
GDPR	General Data Protection Regulation
ICB	Integrated Care Board
IG	Information Governance
PCD	Patient Confidential Data
SIRO	Senior Information Risk Owner
SNEE	Suffolk and North East Essex

5. Roles and responsibilities

Caldicott Guardian

The Caldicott Guardian has responsibilities for protecting the confidentiality of patients/service-user's information and enabling appropriate information sharing. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

Data Protection Officer (DPO)

The Data Protection Officer has the leadership function for IG, maintaining the confidence of patients, staff and the public, through advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle PCD. This includes ensuring that the Practice is fully compliant with all IG related legislation and that the Practice meets statutory and mandatory obligations for IG through development of strategy and implementation of IG policies.

Practice Manager

The Practice Manager is responsible for disseminating all IG policies and IG messages from the DPO to all staff in the practice. They have a key role in ensuring that the practice and all staff are compliant with their DP obligations. If necessary, the Practice Manager can delegate out any compliancy responsibilities to others in the practice. They are also the main contact for the DPO and will be responsible for raising appropriate questions or concerns with the DPO.

All Staff

The majority of staff handle information in one form or another. Staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.

The Practice policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of IG compliance within the organisation. All staff and officers, whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of IG. All staff associated with the Practice have a responsibility to ensure compliance with the DPA 2018 and to actively respond to any concerns relating to confidentiality.

6. Accountability & Governance

The Practice will appoint a DPO who will assist with internal compliance and advise on all data protection obligations.

The Practice will ensure that they are registered with the Information Commissioners Office and ensure this membership is kept up to date.

The Practice will undertake audits and maintain action plans to ensure compliance with data protection law and this policy. The audits will cover physical security spot-checks as well as system audits. The Practice is required to act on the outcomes of the audits and undertake follow-up actions. Templates for physical security spot-checks and system audits can be obtained from the IG Team.

The Practice will ensure data protection by design and by default by placing appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. Please refer to the Data Protection by Design procedure document for more information.

If anyone intends on processing PCD in a different way to normal, they must seek advice from the DPO first.

The Practice will maintain a processing log and data flow maps, and this will be updated annually.

If undertaking a new processing activity independently the Practice will need to carry out the appropriate DPIA using the correct templates supplied by the IG Team. Any DPIA's must be approved by the DPO before any processing can commence. If the processing is high-risk and the DPIA identifies unmitigated risks, then the ICO will need to be notified.

The Practice will ensure that all suppliers are compliant with DP legislation and all contracts will include DP and security requirements. These will be reviewed throughout the contracts lifecycle. In order to ensure all suppliers are compliant the Practice will undertake the appropriate due diligence. To do so they will use the Due Diligence Checklist.

All DP templates will be regularly reviewed by the IG Team.

The Practice will maintain their annual compliance with the Data Security and Protection Toolkit (DSPT).

The Practice will maintain an up-to-date Privacy Notice and make this available on their external website and within their practice waiting room.

The Practice will be aware of the legal basis they are using for each processing activity. If the processing is for direct care, then they are fine to proceed however if the processing id for anything other than direct care the IG Team need to be notified.

The Practice will maintain a Staff Matrix. A template for this can be obtained from the IG Team.

The Practice will ensure they are compliant with the National Data Opt-Out. To be compliant the Practice needs to inform patients how to opt-out via information on their website and in their practice. They also need to apply any opt-outs when required. The clinical systems will do this for them but if they have any questions around the opt-outs they must contact the IG Team.

7. Individual's Rights

The Practice will respond to all individuals exercising their rights under the DPA within one calendar month. For more information on this please see the Access to Information Policy.

This Access to Information Policy also covers Freedom of Information requests and requests made by other bodies such as the police.

8. Security

The Practice will ensure that all data is kept secure and any breaches occurring will be dealt with appropriately. For more information on this please see the Data Security Policy and Incident Reporting Policy.

9. Training, staff obligations and awareness

All Practice staff will have annual mandatory training around data protection and their responsibilities. Further training around specific subjects is available from the IG Team. It is advised that individuals undertaking Subject Access Requests undertake specialist training. Practices may also be required to undertake specific training if recurrent information security incidents occur.

Some roles, such as SIRO and Caldicott Guardian are required to undertake additional training to remain current in their role.

All Practice staff will read the GP IG Resource Guide and sign the declaration that accompanies this.

All contracts of employment include a data protection and general confidentiality clause, agency, locum, bank and contract staff are subject to the same rules.

All staff must be aware of their individual responsibilities for the maintenance of confidentiality, DP, Information Security (InfoSec) management and data quality. They are given the tools for this through undertaking annual mandatory IG training and via the GP IG Resource Guide.

A breach of the DP requirements could result in disciplinary action being taken (including dismissal). A breach of the DPA could also result in legal action being taken against those found in contravention.

Managers are expected to take ownership of, and seek to improve, the quality of data collected and held within their team.

10. Dissemination and Implementation

Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the Practice Manager.

11. Audit and Monitoring Compliance

The Practice will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following methods:

Information Governance compliance will be monitored quarterly through the review of the physical security spot-checks and clinical system audits. Staff clinical system access will be monitored. Templates for the physical security spot-checks and clinical system audits can be obtained from the IG Team.

The IG Team has responsibility to provide assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect it. The Head of Information Governance/DPO will ensure that adequate arrangements exist for:

- Reporting incidents
- Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programmes and progress reports
- Reporting Data Security and Protection Toolkit (DSPT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the IG Team may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external assessments or other sources of information and advice.

12. Related documents

This policy must be read in conjunction with the:

- GP IG Resource Guide
- Access to Information Policy
- Incident Reporting Policy
- Data Security Policy
- Records Management and Recording Policy

13. Equality and Diversity

The Practice recognises the diversity of the local community and those in its employment. The Practice aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This policy is applicable to every member of staff within the Practice irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

14. Key Contacts

Senior Information Risk Owner	Dr Malini Wace
Caldicott Guardian	Dr Malini Wace
Data Protection Officer and Information Governance Lead	Paul Cook support@sneeicbdpo.freshdesk.com