

# Trust Policy and Procedure Document Ref. No: PP(19)110

###### Data Protection Policy

|  |  |
| --- | --- |
| **For use in:** | All Areas |
| **For use by:** | **All Staff Members** |
| **For use for:** | **Guidance to Staff on the General Data Protection Regulation** |
| **Document owner:** | **Head of Information Governance** |
| **Status:** | **Approved** |

**Contents Page**

1. Introduction 2
2. Scope 2
3. Summary 2
4. Key Principles 3
5. Responsibilities 3
6. Data Protection Overview 4
7. Data Protection Guidance 5
8. Staff Training & Support 12
9. Monitoring 12
10. Reporting 12
11. INTRODUCTION

Like all NHS organisations, West Suffolk NHS Foundation Trust ("the Trust") holds and processes information about its employees, patients and other individuals for various purposes (for example, the effective provision of healthcare services or to operate the payroll and to enable correspondence and communications). To comply with the General Data Protection Regulation (GDPR) EU 2016/679, information must be collected and used fairly, stored safely and not disclosed to any unauthorised person. The GDPR applies to both manual and electronically held data.

1. SCOPE OF THE POLICY

This policy relates to all personal data held by the Trust relating to patients and employees. The Trust is responsible for its own records under the terms of the GDPR, and it has registered as a Data Controller with the Information Commissioner’s Office - registration Z6947094 covering:

1. Staff Administration
2. Accounts & Records
3. Health Administration and Services
4. Research
5. Crime Prevention and Prosecution of Offenders
6. Public health
7. Advertising Marketing & Public Relations for Others
8. SUMMARY

The lawful and correct treatment of personal information is vital to the successful operation of the Trust. It helps maintain confidence within the Trust, and the individuals with whom it deals. Therefore, the Trust will demonstrate its compliance with the GDPR by ensuring personal information is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) 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; and

f) 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.

1. KEY PRINCIPLES

* All staff must complete Information Governance training every year.
* New processes or systems involving the use of person-identifiable information must have a Data Privacy Impact Assessment completed and approved.
* All information processing and assets must be recorded by the IG team.
* The Data Security & Protection Toolkit records evidence and demonstrates compliance with GDPR.
* Only authorised staff should have access to person-identifiable information.
* All confidentiality breaches must be reported via Datix and notified to the IG team within 72 hours.
* The Information Governance Team will answer all queries on confidentiality issues in the first instance.

1. RESPONSIBILITIES

**Chief Executive**

The Chief Executive has overall accountability and responsibility for Information Governance and is required to provide assurance that all data protection risks are effectively managed and mitigated.

**Senior Information Risk Owner (SIRO)**

The SIRO is the Director of Finance & Resources. The SIRO ensures that identified information security incidents/risks are followed up and incidents managed. They ensure that the Board is briefed on all GDPR issues. The role is supported by the Trust’s Data Protection Officer.

**Caldicott Guardian**

The Caldicott Guardian’s role is to actively support the implementation of processes and procedures to ensure confidentiality and Data Protection are properly embedded within the organisation.

**Data Protection Officer / Head of Information Governance**

The Head of Information Governance is the appointed Data Protection Officer for the Trust and has responsibility for confidentiality and security issues for all patients and staff.

**Directors, Senior/Line Managers**

Responsible for ensuring that all staff undertake annual mandatory Information Governance training and are aware of and understand their obligations and duties in line with this policy.

**Information Asset Owners**

The Information Asset Owner (IAO) will be a member of staff who is responsible for information assets in their department. All information assets within the organisation must be identified and risk managed.

**All employees**

All West Suffolk NHS Foundation Trust employees are responsible for ensuring that they undertake annual mandatory Information Governance training and that they understand and comply with their duties and responsibilities in line with this policy.

6 DATA PROTECTION OVERVIEW

The Trust must comply with the 6 principles of the General Data Protection Regulation. Personal information will be :

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) 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; and

f) 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.

**Individual’s Rights**

The GDPR gives rights to individuals in respect of their own personal data held by others. These are:

* Right of subject access
* Right to prevent processing
* Right to be forgotten
* Right to erasure
* Right to have information rectified
* Rights in relation to automated decision taking

**Responsibilities of Individual Data Users**

All employees of the Trust who record/process personal data must ensure that they comply with the requirements of the GDPR. Any personal data should be kept securely.

Personal data must not be disclosed verbally or in writing or otherwise to any unauthorised third party.

A breach of the GDPR or the Trust's Data Protection Policy may result in disciplinary proceedings.

Contact the Head of Information Governance for data protection advice when unsure.

**Legal Basis**

Under GDPR there must be a legal basis to process personal information.

To process any personal information you must agree a legal basis under Article 6 of the GDPR. These are explicit consent, performance of a contract, legal obligation, vital interests of the data subject or processing in the public interest.

In addition, if sensitive information is being processed eg health records you must comply with further legal obligation. These are explicit patient consent, employment law, vital interests of the data subject, information is in the public domain, defence or exercise of legal claims, public interest, Health & Social Care, Public Health, archiving purposes in the public interest, scientific or historical research.

All Trust information processes must be recorded with the IG team to ensure a legal basis has been determined.

**Guidance to staff**

**7.1 Authorised employees**

Staff should only have access to personal data in the following circumstances:

* Where they are involved in that person’s healthcare.
* For personnel/HR issues, where the employee is authorised to access personnel files.
* Where the employee is authorised to access personal data in specific circumstances eg: Legal services in medico-legal cases and complaints
* Clinical auditors
* Clinical coding
* Medical records team
* Investigating officers
* Finance staff for recharging CCGs for patient treatment at the Trust
* **Employees must never access their own medical record – copies of records need to be applied for from the Medico Legal Team.**
* **Employees must not access records of people they know (whether a relative or not) without a legitimate clinical reason for doing so.**

**7.2 Telephone**

* Do not make telephone calls concerning confidential information where you can be overheard.
* Turn the volume down on your answer phone so messages cannot be overheard.
* The trust sometimes receives bogus calls - people who attempt to glean information to which they are not entitled. If you suspect a caller is bogus, check to ensure that you are speaking to the correct person, by verifying date of birth or GP or calling back a number that you can check independently. If you suspect a caller is fake, do not release any information and report the incident to IG.
* Recorded telephone messages containing person identifiable or sensitive information should only be accessed by to those who have a legitimate reason to listen to them.
* Do not leave messages containing person identifiable or sensitive information on answering machines.
* Do record a personalised message on your answer phone so that people can be sure they have dialled the right number before leaving a message.

**7.3 Fax**

The use of fax at the Trust is only permitted in order to receive faxes as approved by the Head of Information Governance. A fax machine will remain in the switchboard area for use in a Majax situation only.

**7.4 Email**

Where email is used to send sensitive information, this should be clearly indicated in the subject header, for example marked ‘Confidential’. If communicating with a patient via email, always gain consent.

Follow these rules:

* Don’t send bad news via e-mail.
* Keep information to an absolute minimum.
* Use only the email address that is on email communication from the patient.
* When you are away from your desk please use your out of office message with alternative contact details.

# Do not communicate with a third party unless it is the representative of a child and they have signed a consent form.

# Please always check the email address as part of the standard demographic checks when a patient attends the trust.

**External email**

NHS.net email is currently the only encrypted method for sending personal information by email. This is automatically encrypted between NHS.net and

* + - NHS.net
    - gsi.gov.uk
    - pnn.police.uk
    - gcsx.gov.uk
    - scn.gov.uk
    - mod.uk

To send an email from NHS.net to another email address, please add [secure] to the start of the subject line to send an encrypted message to any email address.

# 7.5 Social Media

You must consider the potential impact on confidentiality, your own reputation, that of the Trust and the NHS in general. You are expected to behave responsibly, professionally and in accordance with your professional codes of conduct and the Trust’s values and policies.

**You must not:**

* Make personal comments about patients, colleagues, your role, the Trust or NHS.
* Be pictured in activities, or make comments that may be open to misinterpretation
* Post any information relating to patients, colleagues or visitors or any other personal identifiable data
* Use your Trust email address or NHS.net account on any of these sites
* Engage in activities that could bring the Trust or your profession into disrepute
* Provide new or updated information relating to yourself as a Trust employee or other staff or any services relating to the Trust on non NHS websites without first obtaining written approval from your line manager
* You must not post photographs or videos of yourself or your colleagues taken at work in the Trust, nor of patients or visitors within the Trust. Approved Trust staff can take photographs for media purposes with the appropriate consent.

**7.6 Post**

The chosen transfer method should be secure and cost effective.

* Ensure that if correspondence contains any person-identifiable information, it is marked ‘Private & Confidential’ and is in a sealed envelope.
* Ensure that post is sent to a named person.
* Patient identifiable information that is extensive (eg a set of copy records) or relates to more than one person should be sent by Recorded Delivery.
* Special Delivery should be used for extremely sensitive information or batches of information.

**7.7 Photography**

Photography or filming is not permitted in any public areas throughout the Trust. Approved Trust staff can take photographs for media purposes with the appropriate consent. For clinical photography please refer to the Clinical Photography Policy.

# 7.8 Confidential Waste

Confidential paper waste is shredded. The Trust has a contract with an external supplier for shredding of confidential paper waste and blue confidential waste bins are available in key areas. **Ensure that all confidential waste is disposed of in the confidential waste bins.**

**7.9 Cyber Security**

**Do:**

* Set a strong password
* Lock your computer when not in use
* Use an encrypted memory stick/USB device
* Do read, understand and comply with the IT Security Policy
* Do seek advice from the IT Department if any aspects of the policy or procedures are unclear.
* Do store your digital devices securely when not in use.
* Do report any lost or stolen device to the Information Governance Team immediately

**Don’t:**

* Share your smartcard or password
* Use your own device for business purposes unless authorised
* Use work-provided devices for personal use
* Connect your work-provided device to unknown or untrusted networks – for example, public Wi-Fi hotspots.
* Allow unauthorised staff, friends or relatives to use your work-provided device.
* Attach unauthorised equipment of any kind to your work-provided device, computer or network.
* Take personal information, including digital information off site without authorisation.
* Install unauthorised software or download software or data from the internet.

**7.10 Text Messages**

Text messages should not normally be used to convey sensitive information and the use of text messages for the transfer of personal data should be kept to a minimum. When consent is sought for appointment reminder services, users should be informed of what information will be included in standard SMS messages sent to them via the service and the option to opt out must be available on request.

# 7.11 Printers & Photocopying

# Use a confidential waste bin for spoiled prints and copying.

# Check that you have collected all your printing/copying and originals from the machine.

**7.12 Sharing Information**

**Sharing information with other health care organisations**

Care must be taken to ensure that disclosures are not made inadvertently, that those receiving the information in a professional capacity also have obligations to maintain confidentiality, that only information necessary to achieve the objective is disclosed, and it is understood that the information should only be used for the purpose for which it is disclosed.

**Sharing information with non-NHS organisations**

Employees of the trust authorised to disclose information routinely to other organisations outside the NHS must seek assurance that we have a Data Sharing Agreement in place. Information must be sent to other organisations in accordance with this policy and procedures.

**Information Sharing Agreements**

* Data Sharing Agreements are agreed at organisational level and are signed by the Caldicott Guardian.
* Non Disclosure agreements are agreed at person level (eg contract staff) and are signed by the Head of Information Governance.

**7.13 Loss of Data**

Any loss of personal information should be reported to your manager, the Information Governance Team and also reported via Datix immediately.

**7.14 Patients Right of Access to Medical Records**

An individual who wishes to exercise his/her right of access are asked to formally request this information in writing to the Medico Legal coordinator who will provide an application form.

**7.15 Staff Right of Access to Personal Records**

Employees wishing to access personal data should put their request in writing to the

Human Resources Manager.

7.16 Disclosure outside of the EEA

Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the EEA. For clarification please contact the Head of Information Governance.

**7.17 Retention of Data**

Records will be stored securely for the appropriate length of time in accordance with the Department of Health's Records Management Code of Practice 2016.

**7.18 Data Protection Breaches**

Breaches of data protection law are managed through the Incident Management and Reporting Policy. Confirmed breaches must be reported to the Information Commissioner’s Office within 72 hours of becoming aware of the incident.

**7.19 Chaplaincy**

Data concerning a person’s health, and data concerning religious or philosophical beliefs, are a class of “special category data”. The processing of special category data is prohibited, unless a ground for processing that data can be identified. The processing and sharing of data about patients for the purposes of providing chaplaincy services will involve data concerning a patient’s health or religion.

To provide a chaplaincy service we process this data using explicit consent. This must be freely given, informed and specific. Patients are asked if they would like a visit from the chaplaincy service when they are admitted to hospital. This consent can be withdrawn at any time.

If consent cannot be provided for example in end-of-life settings, where the patient is incapacitated or in circumstances where they cannot give their own explicit, informed consent a best interests decision can be made. This could include a third party who may have been empowered to act in the patient’s best interests (eg power of attorney) or a combination of clinical staff/friends/relatives.

Alternatively, there may be a substantial public interest reason for the processing of data, relating to the provision of confidential counselling, advice and support services. This would apply if data shared with the chaplaincy service related to one of those activities and consent cannot be obtained (or it would not be reasonable to obtain it) in the circumstances.

Chaplains and Chaplaincy volunteers are an essential part of the Multi-Disciplinary Team (MDT) and, in many places Chaplains personally lead assessment of the spiritual and pastoral needs of patients and their families, which in turn informs the care delivered by the team. The medical purposes legal basis is used to allow the discussion of the care of a patient at an MDT that includes the presence of a Chaplain. The patient must be informed of the composition of the MDT, and if they object to any member of the MDT being present, this must be complied with when this patient is being discussed.

Chaplains must only access records to document their visits and review previous chaplaincy notes. Access to the other sections of the patient record must not be accessed for any reason. Chaplaincy Volunteers within the NHS must not have direct access to patient records. If an entry needs to be made in the patient record this must be done by a member of staff with relevant access.

**7.20 Coroner’s Regulations – sharing of post mortem reports**

The pathologist must not share the post-mortem report with anyone but the coroner

***16-(2) Unless authorised in writing by the coroner, the suitable practitioner who made the post-mortem examination may not supply any other person with the post-mortem examination report or any copy of that report.***

The pathologist must **not** discuss the outcome of the post-mortem with any clinician, and must **not** provide a copy of the report to any person other than the coroner.

The coroner service is responsible for obtaining the information required by the pathologist for the examination. However, it may be much more efficient to allow the pathologist to make additional enquiries of fellow clinicians for information where necessary. Any additional enquiries made must be recorded in the post-mortem report, as sources of information are open to question at inquest.

**Disclosure to families**

The family/NOK must be notified of a post-mortem (Reg.13-1) and may be represented at the examination (Reg13-3) by a suitably qualified medical practitioner (Reg 13-5)

The family/NOK is entitled to a copy of the post-mortem upon request (Inquest Rules 13-1).

This coroner’s officer does not need to offer the document if not requested. It does not mean that disclosure must be made or that it must be made immediately upon request, if the investigation is incomplete (Leigh). It should be made available as soon as reasonably practicable (Inquest Rules 13-1)

**Disclosure to interested persons (IP’s)**

Where there is to be an inquest, the coroner will prepare an inquest bundle which will include the post-mortem report. The bundle will be disclosed when the coroner is satisfied that the case is ready for inquest.

Clinicians and legal representatives involved in an inquest will not to be issued with a copy of the post-mortem report until after they themselves have filed their report with the coroner. By withholding the post-mortem report the coroner will be assured that firstly, there is an opportunity to question the accuracy of the report before it is disclosed, and secondly, that independent evidence is to be given by the clinicians in their own reports.

Where the police have investigated a death, they are entitled to attend the post-mortem and the coroner will provide a copy of the report ahead of any investigation by the coroner.

**Requests for the post-mortem report by non-interested persons**

The coroner has a discretion in deciding who is a ‘proper person’ to receive copy documents and will consider each request on its own merits.

**Post-mortem reports are utilised by Trusts and GP’s in the training environment. This is not to be discouraged but training cannot include post-mortems which are currently under consideration by the coroner.**

**SECTION 8 – STAFF TRAINING AND SUPPORT**

The Information Governance Team will deliver data protection training and awareness. Support will be provided for individual information governance queries.

**SECTION 9 – MONITORING**

The Information Governance Team will undertake the following audits:

* IG compliance in all Trust areas to include CQC IG standards. Key findings and action plans to be reported to IG Steering Group.
* Completing Data Privacy Impact Assessments for existing and new processes and systems.
* Reviewing entries on Datix on a monthly basis and reporting incidents to the Information Governance Steering Group at its quarterly meetings.

**SECTION 10 – REPORTING**

* The Information Governance Steering Group will receive reports on incidents, SIRIs, complaints and near misses.
* Audit outcomes and actions to IG Steering Group.
* Quarterly report to the Corporate Risk Committee

|  |  |
| --- | --- |
| Author(s): | Head of Information Governance |
| Other contributors: |  |
| Approvals and endorsements: | Information Governance Steering Group |
| Consultation: |  |
| Issue no: | 6 |
| File name: |  |
| Supercedes: | 5 |
| Equality Assessed | Yes |
| Implementation | IG Manager will check policies. Policy number will not be issued and policy not approved unless standard contained in this policy are met. |
| Monitoring: (give brief details how this will be done) | Training will be given within the Information Governance agenda. GDPR incidents/breaches will be reported and investigated. Data Protection audits will be carried out on a regular basis |
| Other relevant policies/documents & references: | Information Security Policy  Incident Reporting & Management Policy  Health Records Policy  DH - Confidentiality Code of Conduct |
| Additional Information: |  |