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**

1 Introduction

As a Prerequisite for complying with legislation and NHS Digital standards, this document sets out the hospital's policy to be followed in relation to data protection. 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). Information must be collected and used fairly, stored safely and not disclosed to any unauthorised person. The General Data Protection Regulations (GDPR) and the Data protection Act are the two pieces of law which underpin and govern how we handle, store and process personal data. They apply to both manual and electronically held data.

We are the guardians of personal and sensitive information, and we must ensure it is kept safe and handled correctly to ensure trust and confidence in our organisation, and the wider NHS, is maintained.

The overall objective of this policy is to ensure that there is a hospital-wide approach to the management and implementation of data protection procedures, which is communicated to and available to all staff.

2. 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 (DPIA) completed and approved.
- If a new process involving the use of person-identifiable information is introduced, the Information Governance Team must be informed in order to check its compliance with the Data Protection Act 2018. The Information Governance Team must be advised of the existence of any Information Asset, which is any system, database or process that uses personally identifiable data.

- The Data Security & Protection Toolkit is a National Audit of NHS trusts conducted annually. WSFT must record evidence and demonstrate compliance with GDPR to pass this audit.
- Only authorised staff should have access to person-identifiable information for legitimate work purposes. Access for personal purposes is a disciplinary offence which may be investigated by Human Resources.
- All confidentiality breaches must be reported via Radar and notified to the IG team as soon as possible and as a must within 72 hours.
- The Information Governance Team will answer all queries on Data Protection and confidentiality issues in the first instance.
- All staff will ensure any person identifiable data they process as part of their role, including patients and employee data, will be in accordance with the General Data Protection Regulations (GDPR) which came into effect on 25 May 2018, and is now known as the Data Protection Act (DPA) 2018.
- The Trust's computer systems processing patient identifiable data are auditable.
- Staff are to ensure any contracts with third parties involving the processing of person identifiable data comply with the Data Protection Act 2018 Contracts Protocol.
- Whilst the Data Protection Act and GDPR only apply to living patients, the duty of confidentiality exists after a patient has died and staff will observe the principles of good practice set out in this document when handling Deceased patient records and there will be no distinction to when they were in life.
- Records and documents containing personal data will only be destroyed in accordance with the Trust policy on the Retention and Destruction of records

2.1 **Background information**

The General Data Protection Regulation came into force on 25 May 2018. It unified the rights of EU member states and forms part of the Data Protection Act 2018. It replaces the Data Protection Act 1998.

The Data Protection Act 2018 is the UK's implementation of the GDPR and therefore this law still applies now that the UK has left the EU. Under the Data Protection (Charges and Information) Regulations 2018, the Trust is obliged by law to register all processing activities with the Information Commissioner's Office on an annual basis and failure to comply with this requirement is a criminal offence.

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.

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.

3 What is Personal Data?

The GDPR defines personal data as any information that can identify a living individual either directly or indirectly, this could be name, but also includes hospital numbers, NHS Numbers and employee numbers as the identification numbers if entered onto a system can lead to a person being identified.

GDPR extends the definition of personal data to biometric and genetic data such as fingerprint and retinal scanners. Internet Protocol (IP) addresses is unique to an individual's browsing history therefore this also falls under the scope of GDPR.

To process Personal Data, organisations must have a lawful basis, as defined in Article 6 of GDPR.

3.1 Processing of personal data

This can go ahead if one of the following terms is met:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.2 Consent

Under Data Protection legislation, you only need consent if you cannot find another appropriate legal basis. You must consider if it is reasonable and proportionate to use someone's data without consent, and have an appropriate legal basis to do so.

Where you cannot find another legal basis, the Trust may require explicit patient consent. For example, to sign a patient up to a mailing list we need their consent (opt in) Consent should be freely given, which means giving individuals genuine ongoing choice and control over how the Trust uses their data

Under Article 21, individuals have the right to object to their data being processed by the Trust. This is not an absolute right, however if an individual withdraws consent from receiving marketing emails i.e. from the Trust charity, this must be complied with. Further details regarding this right can be found in the Right to Object SOP.

Consent should be recorded, either using a written consent form, or clearly noting and storing if verbal consent is given.

Under UK GDPR, consent forms with pre-ticked opt-in boxes are banned. Consent should be separate from any other terms and conditions and should not be a pre-requisite to obtaining a service.

A consent form should include:

- The name of the Trust
- The name of any third party data controllers who will rely on the consent
- Why the Trust requires the data
- What the Trust will do with the data
- Confirmation that individuals can withdraw their consent at any time
- A link to the Trust's Privacy Notices

Individuals must actively opt-in for their consent to be valid. Completed consent forms should be stored in a secure shared drive or locked filing cabinet. Consent forms should be regularly reviewed for validity, approximately every two years, if the sharing/processing of data is on an ongoing basis.

4. What is Special Category Data?

GDPR defines any personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and
the processing of genetic data, biometric data of a living individual as Special Category Data. If an organisation wishes to use special category data, it must have a lawful basis under Article 6 and also Article 9 of the GDPR.

4.1 Processing of special category data

If sensitive information eg health records is being processed you must also agree a legal basis under Article 9 Processing of special category data i.e. health data can go ahead if an Article 6 condition above is met ***and*** a condition under Article 9 is met:

- (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 and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- (c) processing is necessary to protect the vital interests of the data subject 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, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

5. Responsibilities

All staff working on behalf of the West Suffolk NHS Foundation Trust are responsible for adhering to the GDPR and for maintaining patient and staff confidentiality.

A breach of confidentiality, whether directly or indirectly, is a disciplinary offence that could result in dismissal and/or prosecution under the GDPR.

It is a legal responsibility of organisations to ensure that transfers of personal information for which they are responsible are secure at all stages.

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.
Following the national Caldicott Committee's Report on the Review of Patient-Identifiable Information published in December 1997, every NHS Trust has a duty to appoint a Caldicott Guardian.

The Caldicott principles are concerned with the use and protection of patient-identifiable information.

All Trusts must abide by the principles for all patient-identifiable information flows:

Principle 1 – Justify the purpose(s) for using confidential information.
Principle 2 – Only use it when absolutely necessary.
Principle 3 – Use the minimum personal data required.
Principle 4 – Access should be on a strict need-to-know basis.
Principle 5 – Everyone must understand his or her responsibilities.
Principle 6 – Understand and comply with the law.
Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality.
Principle 8- Inform patients and service users about how their confidential information is used.

Data Protection Officer
The 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) each Division will nominate an individual who liaises with the IG Team regarding their data flow activities on a regular basis.

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's compliance with the General Data Protection Regulations (GDPR) ensures that it treats personal data in a confidential manner. A principle aim of the GDPR is to promote openness in the processing of personal data and therefore the Trust must ensure that Data Subjects know the reason their information is collected, its uses within the organisation and to whom, and the circumstances when, it may be disclosed.

The GDPR can only be applied to records relating to living individuals. However, a duty of confidence is still owed to the deceased and their families so this policy includes information on the Access to Health Records Act 1990 and the Common Law Duty of Confidence to provide guidance on this type of data.

6.1 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 restrict processing
- Right to be informed
- Right to erasure
- Right to have information rectified
- Rights in relation to automated decision taking
- Right to data portability
- Right to object
  These rights are not absolute and will be each be dealt with on a case by case basis. Approval where necessary will be sought from the Caldicott Guardian and or the DPO

6.2 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 Information Governance team via the email info.gov@wsh.nhs.uk or telephone 01284 713454for data protection advice when unsure.

7 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
  - Patient Safety team as part of the Patient Safety Incident Review Framework (PSIRF)

- **Employees must never access their own medical record – copies of records need to be applied for from the Medico Legal Team whose email address is accesshealthrecords@wsh.nhs.uk.**

- **Employees must not access records of people they know (whether a relative or not) without a legitimate (see above) reason for doing so.**

7.2 Access to Personal Data

There are procedures in place to ensure that appropriate access to care records systems is provided to those members of staff who require access as part of their role.

If staff change role, they must ensure they inform IT to remove any legacy access that is no longer required in their new role.
All clinical records should be kept secure. There should be a barrier (eg locked filing cabinets, passwords on computer systems, locked office doors) between clinical records and unauthorised access.

All departments holding confidential files should have a locked filing cabinet for these records and access to the filing cabinet should be limited to authorised personnel.

Staff must **never** access their own medical record or information treated in confidence – copies of records need to be applied for from the Access to Health Records Team, or HR for Personnel files Staff must also **not** access records of people they know (whether a relative or not) without a legitimate clinical reason for doing so.

7.3 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. A deputy should be appointed for times of absence and messages dealt with promptly and removed from the answering machine.
- 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 dialed the right number before leaving a message.
- Care must be taken when divulging patient information to a family member or carer. Do not assume you have consent. Always check with the patient before disclosing information about their care. Wards are encouraged to have a password policy in place that family members/carers/friends must confirm before information about the patient can be disclosed. The password can be recorded in the patient's medical record

When confirming details such as address, please ensure that you ask the patient to tell you the address and do not read out the information and simply ask them to confirm if correct. The patient should tell you their details. This helps prevent giving out information to unauthorised persons or bogus callers.

7.4 Email

Under Section 250 of the health and Social Care Act 2012, the Secure Email Standard (Information Standards Notice DCB1596) was released.

This required organisations in health, public and social care to have secure accredited email systems in place

The Trust appears on the NHS Digital List of Accredited Organisations and refreshes its conformance with the standard on an annual basis

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.

- **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.**

Email encryption

WSFT email addresses (@wsh.nhs.uk) are DCB1596 accredited. All internal email is therefore encrypted and secure.

For external email please check the DCB1596 register to see if the recipient is also accredited and secure eg @nhs.net, @pnn.police.uk, @gov.uk. If the address is not accredited, please use the Zivver functionality as described below.

To send an email to a non secure email address eg @gmail.com please use the Zivver functionality embedded into MS Outlook. Toggle Zivver on to ensure end to end encryption.

For NHS organisations that do not use nhs.net email, it is the responsibility of the Trust staff member to seek assurance from the recipient that their email is secure to receive confidential personal data. For a list of accredited organisations, please see the link below:
The secure email standard - NHS Digital

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.

Use of Photographs or Videos on Social Media

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, nor of Trust holdings or logos. The only exceptions to this are by the written agreement of the Head of Communications, for example in health education campaigns.

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/Filming

Photography or filming is not permitted in any public areas throughout the Trust (eg ED waiting room). Approved Trust staff can take photographs for media purposes with the appropriate consent.

Recording within other areas (eg wards or clinical treatment areas) by a patient on their mobile device can only be carried out with the consent of the person being recorded. The use of a device in a clinical/ward area is a privilege that can be withdrawn if this guidance is not followed.

Where patients do not comply with this guidance, then they must be asked to cease using their device. In situations where the patient lacks capacity to understand the implications of the guidance and the impact on others, then ward staff should liaise with the patient's carers/family to seek their support or for them to remove the device.

We have a duty to protect our patients in ward/treatment areas whose confidentiality is being or is likely to be breached.

All incidents where a patient or visitor has photographed or recorded another patient/service user must be reported using Radar to provide a record of the incident and an audit trail. This must include details of the actions taken as a result of the incident.

The recording of any information which does not relate specifically to the patient themselves:

- Is strictly prohibited – to protect against any breach of privacy/confidentiality
- Constitutes a significant breach of the Trust's expected 'behaviour standards' of any patient or visitor to the Trust.
- May result in delay or withdrawal of any treatment if staff are not willing to care for the patient
- Could result in the recording device being seized and retained as evidence of an offence if other patients are including in any filming.
- Could result in involvement of the police.
- May lead to criminal charges if the recording is subsequently disclosed to unauthorised parties without appropriate consent from all the parties it features. This includes any kind of publication on the internet.

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 Blue waste bins/ Cross shredded.**

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. Community staff are authorised to take data between sites, however care must be taken to keep the data secure.
- Install unauthorised software or download software or data from the internet.

7.10 Mobile Devices

- Staff must not store person identifiable data on mobile devices unless they are Trust issued or rebuilt/ configured to meet Trust security standards
- Mobile devices must be pin protected
- Mobile applications containing PID must be password protected

7.11 Text Messages

Key considerations when using text messages are:

- When consent is sought for appointment reminder services, service 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.
- Text messages should not be used to convey sensitive information and the use of text messages for the transfer of personal data should be kept to a minimum.
- Is the mobile phone number correct?
- Is the mobile phone receiving the text message being used by the intended recipient of the message?
- Has the message been received, and what provision is there to audit message receipt?
- Messages are stored in mobile phone internal storage and/or removable storage (e.g. SD card) and may be synchronised to Cloud services.- as mobile phones are easy to misplace or may get stolen, there is a danger of a breach of confidentiality occurring that the patient / service user may find distressing or damaging.

WhatsApp should **Never** be used to send confidential patient information.

7. 12 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.

7.13 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.

7.14 Loss of Data

Any loss of personal information should be reported to your manager, the Information Governance Team and also reported via Radar immediately. All incidents recorded on Radar must include any appropriate actions taken in order to document common causes for incidents i.e. human error.

Serious breaches as determined under the national NHSE guidance, are reported to the Information Commissioner's Office within 72 hours once the organisation has become aware of it.

7.15 Security and Confidentiality Breaches

Security and Confidentiality 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.

A data breach is where there is breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All breaches of confidentiality will be investigated. The Information Governance Team will provide investigating officers with advice on suspected breaches of confidentiality. The Data & Security Administrator, the Information Governance Manager, and the Trust's Head of IT Security and Compliance may share details of confidentiality breaches to ensure appropriate action is taken. All breach reports should have lessons learned in the Radar record.

The severity of the breach is determined by an assessment to the risk to the 'rights and freedoms' of the data subject. For example, a severe data breach is if sensitive personal data is accidentally disclosed to a member of the public, who then contacts the press about the breach. The Information Governance team will give advice on the severity of a breach and the level of investigation required.

In accordance with the Trust's Disciplinary & Procedures Policy, action may be taken against members of staff who are negligent or commit a deliberate breach of the Data Protection Act.

Where an information governance breach meets externally reportable criteria as set out in the NHS Digital 'Notification of Data Security and Protection Incidents' guidance, the Data Protection Officer or a designated deputy will report these onto the Data Security &

Protection Toolkit within 72 hours of the organisation becoming aware of it. Reporting onto the Data Security & Protection Toolkit automatically notifies the Information Commissioner's Office. The Information Governance team will need to report data breaches even if the full information is not available, as further information can be appended at a later date.

In order to report a data breach to the ICO, the IG team will require:

- A full description of the breach
- How many data subjects the breach affects
- What type of person it affects (i.e. vulnerable adults or children)
- What level of data was breached
- Has the breach been reported in the press
- Has the data left the UK
- Have regulatory bodies or the police been notified
- Have data subjects been informed of the breach
- Is there a high level risk to the rights and freedoms of the data subject

If the Trust fails to report a reportable breach to the ICO within the 72 hour time frame, the Trust could face regulatory action including monetary fines.

7.16 Duty of Candour

The data subject should be notified of the data breach under Duty of Candour if it is determined that there is a high risk to their rights and freedoms, and/or if the breach is not contained, i.e. we are unable to retrieve or destroy the breached data.

The Duty of Candour letter should include:

- the name and contact details of any data protection officer you have, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

7.17 Patients Right of Access to Medical Records

An individual who wishes to exercise his/her right of access their medical records are asked to formally request this information in writing to the Medico Legal Health Records Team who will provide an application form. Please refer to the Subject Access Request policy

7.18 Staff Right of Access to Personal Records

Employees wishing to access personal data should put their request in writing to the Information Governance Team. Please refer to the Subject Access Request policy

7.19 Disclosure outside the UK and EEA (European Economic Area)

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 Information Governance Manager.

7.20 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 2021.

7.21 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.

7.22 NHS National Data Opt Out

This national policy enables patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients log their choice centrally with NHS Digital and the Trust implements processes at an organistional level to ensure patient's choices are complied with.

West Suffolk is compliant with the National Data Opt Out and the Data Protection Officer is the Responsible Officer for the Trust's Standard Operating Procedure in relation to this requirement

7.23 General Security

- Paper must not be re-used for any purpose – all printed/written paper must be disposed of in the confidential waste.
- Do not allow unauthorised people into areas where confidential information is held unless they are supervised.
- Do not hold keypad lock/swipe card protected doors open for people following you in.
- Do not wedge open security doors and check that windows are closed/locked at the end of the day.
- Do not share door security codes with unauthorised people.
- Operate a clear desk policy. Do not leave confidential information out overnight.
- Wear your Trust identity badge so that other members of staff know who you are.
- Person identifiable information should be kept in locked rooms/drawers/filing cabinets.
- Take measures to prevent casual observation of person-identifiable or sensitive information e.g. remove case notes from unmanned reception areas. All person identifiable and/or sensitive records must be stored face down in public areas and not left unsupervised at any time.
- If a patient needs to attend more than one department within the hospital and his/her hospital information is required, then the patient data must be placed in a sealed envelope and an explanation should be given to the patient that it must only be opened by the receiving clinician.
- Ensure confidential conversations are held in an appropriate place.
- Gain patient consent before sharing personal information with relatives or friends.
- Store nursing notes in wards securely, away from patient areas. Minimal nursing notes can be stored in patient bays**. Visitors are not allowed to access a patient's notes** unless through the Access to Health Records Team
- Any medical notes should be checked by clinicians before patients see them, to check for any information that might cause the patient harm or distress to read.
- Forward any requests from patients for copies of their notes to the Access to Health Records team.
- Personal data or any other confidential data stored in a paper format is not to be taken off-site unless you are authorised to do so
- When taking Trust equipment and belongings off site, store them in the boot of the car and where possible do not leave them in your vehicle overnight
- If staff are taking paperwork off site to visit community patients, use a lockable storage box/bag to store the paperwork whilst in the community
- Handover documentation for staff should only contain the minimum data required and must not be taken off a ward/clinic and disposed into confidential waste when no longer required

7.24 Cyber Security

All staff (including bank and contractors) must remain vigilant when processing personal identifiable data electronically i.e. submitting online forms or emailing. If staff receive an

email from someone asking for confidential details or requesting payment and it is not expected or the sender is unknown to you, staff should follow the guidance below

- Do not click on links or open attachments
- Always question if you receive a request for payment outside the proper channels
- Do not use your NHS email address to subscribe to mailing lists unless work related
- Delete suspicious emails – do not reply
- Report suspicious activity to the Service Desk

7.25 NHS Counter Fraud Authority

This is concerned with dealing with requests for information from the NHS Counter Fraud Authority or Local Counter Fraud Specialist (LCFS) in the prevention, detection and investigation of potential or actual crime. The Trust must co-operate with the CFSMS under these circumstances and can do so without the data subject's consent.

7.26 Police

All requests from the police for personal data will be dealt with on a case-by-case basis via the IG Manager, Caldicott Guardian, (or other Director on call), who will decide if the information can be disclosed. To release information to the Police, or another enforcement agency, without the data subject's consent, the following grounds must be met:

- There must be an overriding public interest such as to safeguard an individual's safety or for the detection and prevention of a serious crime
- Another lawful basis to release information i.e. under the Road Traffic Act
- A court order

The most likely legal basis for disclosure (without the patient's consent) to the police are:

- Prevention of Terrorism Act (1989) & Terrorism Act (2000)
- The Road Traffic Act (1988)
- Court Order
- HM Government (2015) Prevent Strategy

Detailed guidance on how to mage requests from the police and other enforcement agencies can be found in the Police Information Sharing SOP

7.28 Data Protection Compliance and Confidentiality Audits

In accordance with Article 34 of the GDPR, Data Protection Impact Assessments (DPIAs) must be completed when a new project/system incorporating the processing of special category data on a large scale is planned to be implemented. The DPIA is to be completed prior to implementation/commencement and approved by the Information & Records Governance Group.

It is the responsibility of the Data Protection Officer to provide advice and recommendations in relation to DPIAs. Any risks associated with the processing of large

scale special category data that cannot be mitigated, are to be referred to the Information Commissioner's Office to approve processing of the data

The Information Governance Team will periodically carry out data protection and confidentiality compliance checks on existing processes and a report will be made to the appropriate department manager and the IRGG Group.

Staff are reminded that computer systems can audit their access and requests to audit an individual staff member's activity can be undertaken at any time

Such requests must be authorised by the Data Protection Officer or Caldicott Guardian

SECTION 8 – STAFF TRAINING AND SUPPORT

The Trust offers Mandatory Information Governance training to all staff irrespective of their experience or grade. It is a mandatory requirement for all Trust employees to completed this training yearly.
Information Governance training compliance must be above 90% for all areas.

SECTION 9 – Monitoring

The Information Governance Team will undertake the following:

- IG compliance in all Trust areas as evidenced by an annual Data Security & Protection Toolkit submission to NHS Digital.

- Completion of Data Privacy Impact Assessments for existing and new processes and systems.

- Review 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):	Information Governance Manager
Other contributors:	
Approvals and endorsements:	Information Governance Steering Group
Consultation:	
Issue no:	9
File name:	S:\Information Governance\Policies and Guidelines\Trust Policies\PP-110- Data Protection
Supercedes:	8
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:	