Weston Area Health NHS Trust

GOV24 Data Protection Policy
v 1.0

Date Approved:	April 2019
Date for Review:	April 2021
Directorate / Department responsible (author/owner):	Corporate, Information Governance, Head of Information Governance
Contact details:	01934 647002
Brief summary of contents	The Trust has legal and regulatory responsibilities to safeguard the information utilised by and entrusted to it, and to process it both fairly and lawfully. This policy describes the Trusts framework for the protection of information and how compliance is recorded and evidenced.
Search criteria:	Information, governance, data protection
Executive Director responsible for Policy:	Director of Finance
Date revised:	April 2019
This document replaces (exact title of previous version):	Not applicable
Title and date of committee/forum/group consulted during development :	Information Risk Management Group
Signature of Executive Director giving approval	
Intranet location:	Information Governance
Links to key external standards	NA
Related Documents:	Included
Training Need Identified?	Yes

Version Control Table

Date	V	Summary of changes	Author

Document Amendment Form – minor amendments

No.	Date	Page no	Amendment	Authorised by
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Ten or less minor amendments can be made before the document is revised.

Major changes must result in immediate review of the document

If printed, copied or otherwise transferred from the Trust intranet, procedural documents will be considered uncontrolled copies. Staff must always consult the most up to date version – located on the intranet.

Table of Contents

1. Introduction and purpose

The purpose of this Policy is to ensure the Trust's adherence to statutory and legal frameworks relating to personal data including:

· General Data Protection Regulation 2016 (GDPR);
· Data Protection Act 2018 (DPA);
· Human Rights Act 1998 (HRA);
· Freedom of Information Act 2000 (FOIA);
· Common law duty of confidentiality;
· Any other relevant legislation.

The policy also includes the Trust's policy document as required by Paragraph 34 of Schedule 1 Part 4 of the DPA in relation to processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of that Schedule.

The policy provides a robust framework to ensure a consistent approach to both compliance and best practice across the whole organisation, and supports the duties set out in the NHS Constitution and the guidance in the NHS Confidentiality Code of Practice. It applies to all Trust staff (including temporary and agency staff and volunteers). All staff must comply with this policy as a condition of their employment. A breach involving unwarranted disclosure of information may result in disciplinary action.

All staff are required to comply with the principles in this policy.

This policy supports the aims and standards set out in the Trust's Information Governance Policy, including:

· Openness;
· Compliance;
· Security;
· Quality Assurance;
· Pro-Active use of information.

2. Scope

This policy is applicable to all areas of the organisation and to all staff, including students and contractors. The information covered by this policy includes, but is not limited to:

- Patient information including personal information and information relating to carers and family.
- Staff information including personal information and information relating to employment, training, appraisal, etc.
- Financial information including accounting and financial reporting.
- Corporate information including statutory reports.

3. Explanation of terms

3.1. Personal Data

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2. Data Controller
Data Controller means the person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Trust is a data controller and this policy sets out how it will comply with its responsibilities as such.

3.3. Data Processor
Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller. Employees and others acting under the direct authority of the Trust are not regarded as data processors.

3.4. Information Asset/Information Asset Owner
An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively, or the hardware, software, system or environment in which that information is stored. Each information asset has an identified information asset owner.
An information asset owner (IAO) is a senior member of staff who is nominated as owner of one or more of the Trust's information assets. He or she will have direct responsibility for the risk management and security for the asset, and for its effective and efficient use.

4. Roles and Responsibilities

4.1. Trust Board of Directors

a/ The Trust Board is the Data Controller for the purposes of the General Data Protection Regulations 2016 and the Data Protection Act 2018 1998.

b/ The Board is responsible for ensuring that information within the Trust is processed according to statutory requirements.

c/ Responsibility for compliance with the standards set out in the Data Security and Protection Toolkit rests with every officer of the Trust, including Executive Directors, Lead Clinicians, Directorate Managers, Heads of Profession, Senior Managers, etc.

4.2. Executive Directors

a/ Providing evidence to the Trust Board of Directors that information is processed according to prevailing legislation and regulation.

b/ Responsibility for overseeing the status of all risk to the Trust, including information risks, rests with the Information Risk Management Group, Senior Leadership Team, Directorate Management Boards and Directorate Governance Groups.

4.3. Trust Secretariat

a/ The Trust has appointed a Data Protection Officer for the purposes of the General Data Protection Regulations.

b/ The Data Protection Officer will:

- Inform and advise the Trust and its employees who carry out processing of their obligations pursuant to the General Data Protection Regulations 2016 and the Data Protection Act 2018;

- Monitor compliance with the General Data Protection Regulations 2016 and the Data Protection Act 2018 and Trust policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;

- Provide advice where requested as regards data protection impact assessments and monitor performance against such assessments;

- Co-operate with the Office of the Information Commissioner;

- Act as the contact point for the Office of the Information Commissioner on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter;

- Report matters of compliance or risk direct to the Trust Board and Senior Information Risk Owner where it is considered appropriate to do so in addition to using the Trust's existing risk management processes and provide an annual data protection assurance statement to the Trust Board as part of the Statement of Internal Control / Annual Governance Statement.

c/ Responsibility for the provision of specialist Information Governance advice, prioritisation of actions, and submission of the Annual Return rests with the Trust Secretariat – specifically the Information Governance Manager. The Trust Secretariat/ Information Governance Manager will:

- Ensure that the appropriate management groups or monitoring and scrutiny committees are provided with appropriate evidence of quality assurance within the management of patient, staff and corporate records.

- Be responsible for the correct dissemination of statutory information within the Trust.

- Ensure the DSP Toolkit is submitted accurately and on time. Ensure that the Trust fulfils Data Subject Access Requests and Freedom of Information Requests.

4.4. Caldicott Guardian

a/ Ensuring patient confidentiality, information sharing, data privacy and use of patient data in research according to the Caldicott Principles and the precepts of this policy.

b/ This role is described by Connecting for Health as: "The Guardian plays a key role in ensuring that NHS organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework."

c/ The Medical Director for professional standards is the Trust's current Caldicott Guardian.

4.5. Senior Information Risk Owner (SIRO)

a/ The Data Security and Protection Toolkit describes the Senior Information Risk Owner (SIRO) as “an Executive Director who takes overall ownership of the organisation’s Information Governance Policy, acts as champion for information risk on the Board and provides written advice to the Accounting Officer (Chief Executive) on the content of the Trust’s Annual Governance Statement in regard to information risk.

b/ The SIRO must understand the strategic business goals of the organisation and how other business goals may be impacted by information risks, and how those risks may be managed.

c/ The SIRO implements and leads the Information Governance risk assessment and management processes within the organisation and advises the Board on the effectiveness of information risk management across the organisation.

d/ The Director of Finance is the current SIRO and is supported in specialist functions by the Information Risk Management Group (which he Chairs) and the Trust Risk Management Group.

4.6 Registration Authority Manager

a/ The key task of the Registration Authority (RA) is to verify the identity of Trust staff who need access to sensitive data, and to establish and provide only the degree of access they need to do their jobs.

b/ Manage the issuing service of Smartcards to staff.

c/ Ensure that all RA procedures are carried out in accordance with the national policy.

4.7. Head of Health Informatics

a/ Responsible for ensuring technological security of information including, but not exclusively, access control and identity management, virus protection, malware protection, anti-phishing measures, and physical security of electronic systems under the care of Information Management & Technology Department.

4.8. Information Risk Management Group

a/ Reviewing the work of the Information Risk Management Group, reporting DSP Toolkit status changes to the Senior Leadership Team.

b/ Approval of Information Governance procedural documents.

c/ Co-ordinate and lead activity in the following areas of Information Governance:

- Information Governance and Risk Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance (includes clinical record keeping)
- Corporate Information Assurance
- Secondary Use Assurance.

d/ Maintain an Information Governance Risk Register

e/ Provide formal evidence of compliance across Information Governance disciplines to support the annual Data Security and Protection Toolkit submission.

4.9 Directorate Boards

a/ Directorate Management Boards have responsibility for the stewardship and management of the information generated, processed or stored within their Directorate.

b/ Accept delegated responsibility for the identification and management of information management risk in accordance with the Trust Risk Management Strategy.

4.10 Information Asset Owners and Administrators

a/ Information Asset Owners (IAO) have a key role to play in ensuring compliance with this policy. In particular, they have responsibility for ensuring appropriate security is in place for their assets which hold personal data and that staff are adequately trained to use them. They have specific responsibility for managing the content of, access to, use and transfer of and disposal of the personal data within the information assets and that there is a legal basis for holding and processing the data.

4.11 IT and HR Trainers

a/ Administer the Information Governance and data security training and support annual training needs analysis

4.12. All Staff

a/ All staff must understand and carry out their responsibilities and duties towards the protection of information.

b/ All staff have personal responsibility for undertaking training suitable to the requirements of their individual roles.

5. Policy details

- The Trust and its staff (including temporary and agency) will at all times comply with the data protection principles set out in Article 5 of the GDPR. These principles specify (in summary) that personal data must be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject (Principle 1);
    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Principle 2);
    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle 3);
    4. accurate and, where necessary, kept up to date (Principle 4);
    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 (Principle 5);
    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 (Principle 6).

In particular, in compliance with the above principles, the Trust will maintain appropriate procedures and guidance for both staff and those interacting with the Trust to ensure that:

- Where processing is required to take place without consent, data subjects will be given clear explanations including confirmation of the legal basis unless GDPR or DPA provides an exemption and there is good and lawful reason to apply that exemption.
- Where processing is by consent the Trust will ensure that such consent is freely given, specific, informed and unambiguous and obtained via a statement or by a clear affirmative action and in the case of special category data such consent is explicit (Principle 1);
- All processing of personal data is lawful and in particular in compliance with any duty of confidentiality and the Caldicott Principles as set out in the Trust's Confidentiality Policy. The confidentiality policy has more information about actions the Trust has taken to implement the recommendations of the Caldicott reports (Principle 1);
- The Trust will identify the legal bases for processing the personal data it holds (see below). IAOs shall be responsible for ensuring that this is done for the assets for which they are responsible and associated data flows (Principle 1);
- All processing of personal data is kept to the minimum necessary for compliance with the Trust's work and purposes and access to any personal data is restricted to those who need it for their work (Principle 3);
- Personal data is not informally shared with or disclosed to any third party. Any such sharing or disclosure will be controlled and appropriately authorised, will only be done where it is lawful to do so and notified to data subjects (if consent has not been obtained) unless GDPR or DPA provide an exemption and there is good and lawful reason to apply that exemption. When sharing personal data the Trust will comply with the Information Commissioner's Data Sharing Code of Practice (Principles1, 2, 3 & 6);
- Personal data will be kept no longer than is necessary for the purposes for which it is held. The Trust will maintain policies for the management of health and corporate records which shall include retention schedules. These schedules will be based on the recommendations in the NHS Records Management Code of Practice and any reasons for departure from those recommendations will be documented. The policies will also provide for the secure destruction of personal data which has passed its retention date (Principle 5);
- Where possible without interfering with the Trust's necessary work, or that of any third party with whom data is shared or to whom data is disclosed, any personal data is anonymised or pseudonymised before being used, shared or disclosed. The Trust will comply with the Information Commissioner's Anonymisation Code of Practice and NHS Guidance (Principles1 & 3);
- Personal data is kept secure from unauthorised use, access, disclosure or accidental deletion at all times in accordance with the Trust's IT Security Policy (and associated guidance) or physical security guidelines. Personal data stored on paper or other physical media will be kept in a secure place, when not in use, where unauthorised people cannot see it and shredded or otherwise disposed of securely when no longer required (Principle 6);
- Appropriate safe procedures will be maintained for the transmission of personal data (Principle 6);
- All staff handling personal data understand that they are legally and contractually responsible for following good data protection practice and have appropriate training. This will include, as a minimum, induction training and an annual refresher. Specialist staff including those with information governance roles, information asset owners and administrators and those handling subject access requests will receive additional support and training (Principle 6);
- Unauthorised copies of personal data are not held or processed (Principle 3);
- Personal data held is regularly reviewed for adequacy and relevance and to ensure that it is up to date. Where no longer required personal data will be destroyed securely in accordance with retention schedules - see the Trust's Records Management Policy (Principles 3 & 4);

- Data subjects are given straightforward procedures to enable them to exercise their rights set out below. Subject access procedures will be made available on the Trust website. The Trust will comply with the statutory time limits for subject access and the recommended NHS time limits for subject access to patient records. The Trust will comply with the Information Commissioner's Subject Access Code of Practice and the NHS Care Records Guarantee. The Trust will where appropriate take into account the Information Commissioners Office (ICO) guidance on Access to
- Information in Complaints Files, and in relation to subject access requests by employees the ICO Employment Practices Code and Supplementary Guidance;
- Breaches or suspected breaches of data protection, confidentiality and/ or information security will be reported in accordance with the Trust Incident Reporting Policy (Principle 6);
- Registers of data sharing and data processing agreements with third parties are maintained. Data processing agreements will conform to the requirements of Articles 28 to 32 GDPR, be in writing, and impose equivalent responsibilities on any data processor to those set out in this policy;
- Data protection by design and by default is built into its processes, in particular in relation to commissioning new information assets, new methods of processing and the use of new technology. Data protection impact assessments will be carried out for high risk processing operations;
- Information assets will be owned and managed and risk assessments of those assets and associated information flows are undertaken and reviewed at appropriate intervals;
- Appropriate guidance is available to staff on the steps they must take to comply with this policy (Principle 7);
- It complies with the NHS Information Security Management standards including cyber security;
- It appoints a Data Protection Officer as set out in the Information Governance Policy.
- The Trust will maintain appropriate procedures and guidance for both staff and those interacting with the Trust to ensure that individuals are given and can exercise their rights under GDPR including:
    - The right to information about the processing of their personal data under Articles 13 and 14 of GDPR in the form of privacy notices on the Trust website and in contracts, information leaflets, and explanations in correspondence where appropriate;
    - The right of access to their personal data under Article 15 of GDPR;
    - The rights of rectification, erasure and to restrict processing under Articles 16-18 of GDPR;
    - The right to object to processing under Article 21 GDPR and to limit automated individual decision making under Article 22.
- The Trust will ensure that any transfer of personal data outside of the European Union is compliant with Articles 44-49 of GDPR. Such transfers will not be made without consultation with the Trust's Data Protection Officer and in the case of confidential patient data without the approval of the Caldicott Guardian. Approvals and consultation may relate to regular or individual transfers.

6 Dissemination

The policy will be available on the Trust intranet site in the policy library. A trust- wide email will be issued to all staff to inform them of the policy update.

7. Implementation

The document will be referred to at induction and in relevant training and development programmes.

8. Monitoring Compliance and Effectiveness

Table 1. Mandatory Elements of Monitoring Compliance.

Element to be monitored	Action plans from Toolkit submission
Lead	Information Governance Manager
Tool	Data Security and Protection Toolkit
Frequency	Quarterly
Reporting arrangements	Information Risk Management Committee
Acting on recommendations and Lead(s)	Directorates
Change in practice and lessons to be shared	Communications Strategy Staff training

9. Reference and bibliography

- General Data Protection Regulation 2016
- Data Protection Act 2018
- Data Security and Protection Toolkit

10. WAHT associated records

- Health Records Policy
- Social Media for Personal Use Policy and Procedure
- Data Quality Policy
- Incident Management Policy
- Serious Incident Policy
- Risk Management Policy
- Staff Conduct Policy
- Disciplinary Policy
- Registration Authority Policy

11. Staff compliance statement

All staff must comply with the Trust-wide procedural document and failure to do so may be considered a disciplinary matter leading to action being taken under the Trust's Disciplinary Procedure. Actions which constitute breach of confidence, fraud, misuse of NHS resources or illegal activity will be treated as serious misconduct and may result in dismissal from employment and may in addition lead to other legal action against the individual concerned.

12 Equality and Diversity statement

The Trust aims to design and implement services, policies and measures that meet the diverse needs of users of our services, population and workforce, ensuring that none are placed at a disadvantage over others.

Equality Impact Assessment Screening Tool

To be completed for any procedural document when submitted to the appropriate committee for approval.

		Yes/No	Rationale
1	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the policy/guidance likely to be negative?	No	
5	If so can the impact be avoided?	No	
6	What alternatives are there to achieving the policy/guidance without the impact?	No	
7	Can we reduce the impact by taking different action?	No	
8	Actions identified following screening process	None	
9	Screening identified a full impact assessment.	No	

If you have identified a potential discriminatory impact of this policy/procedure, please refer it the appropriate Director in the first instance, together with suggested actions required to avoid/reduce this impact. For advice in respect of answering the above questions, please contact the H.R Department. For advice on completion of this form please contact the Governance Team.