Yeovil District Hospital NHS
NHS Foundation Trust

DATA PROTECTION POLICY

Version Number	6.1	Version Date	May 2018
Policy Owner	Chief Information Officer		
Author	Trust Data Protection Officer		
First approval or date last reviewed	July 2013, March 2017		
Staff/Groups Consulted	Information Governance Steering Group		
Approved by	Information Governance Steering Group		
Next Review Due	May 2021		
Policy Audited	Yes		
Equality Impact Assessment Completed		Yes	

Table of Contents

	Section	Page
1.	Rationale	5
2.	Aim	5
3.	Definitions	6
4.	Roles and Responsibilities	7
5.	Data Protection	10
6.	Data Protection Principles	11
7.	Lawful Basis for Processing Personal Data	13
8.	Individual Rights	15
9.	Right of Access – Subject Access Requests	15
10.	Disclosure to Others	15
11.	Exemptions	16
12.	Transfer of Personal Data	16
13.	Human Resources	16
14.	Breaches	16
15.	Year on Year Improvement Plan and Assessment	17
16.	Training	17
17.	Implementation, Monitoring and Evaluation	18
18.	References and Associated Documentation	18
Appendix 1 – Equality Impact Assessment Form		19

DATA PROTECTION POLICY

1. RATIONALE

1.1 The Trust needs to collect and use certain types of information about people with whom it deals in order to operate including 'personal data' as defined by the General Data Protection Regulations and Data Protection Act 2018 (Data Protection Legislation). These include patients, current, past and prospective employees, suppliers and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information of this kind to comply with the requirements of public authorities for business data, for example.

1.2 This personal information must be dealt with properly however it is held whether:

- manually stored paper data, e.g. health records, personnel records etc
- computer referenced paper data e.g. health records, personnel records etc
- computerised data held in computer applications and databases
- tapes and other data from CCTV systems
- data held offsite in archive storage
- data held on CD, disks, computer disks, memory sticks etc

1.3 The Trust regards the lawful and correct treatment of personal information very important to providing services and to maintaining confidence. The Trust ensures that personal information is processed lawfully and correctly. To this end, the Trust fully endorses and adheres to the principles of data protection, as defined in the Data Protection Legislation.

1.4 This policy covers all aspects of processing relating to personal information within the Trust and is not solely patient related. It includes information held by all areas such as:

- Healthcare including:
  - Acute, Community & Intermediate Care
  - Mental Health
  - Learning Disabilities
  - Primary Care
  - Safeguarding Children
- Human Resources – including Disclosure Barring Service checks on staff
- Payroll and Finance
- Procurement
- Estates
- Occupational Health

1.5 This policy includes the Trust's policy document as required by Paragraph 38 of Schedule 1 Part 4 of the Data Protection Act 2018 in relation to processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of that Schedule.

2. AIM

2.1 This policy aims to help Trust staff understand their legal obligations to protect personal information. It details how the Trust meets its legal obligation and NHS requirements concerning confidentiality and information security standards as laid down in the Data Protection Legislation.

2.2 This Policy applies to all Trust employees (including temporary and agency staff), Independent Contractors, Non-Executive Directors and volunteers. This policy also applies to staff employed by subsidiary companies of the YDH Group.

2.3 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.

2.4 Data processors appointed by the Trust will be required to comply with the principles in this policy.

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

- Openness
- Compliance
- Security
- Quality assurance

3. DEFINITIONS

Personal Data

3.1 Personal data is 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.

Special Category Personal Data

3.2 Certain types of data are regarded as special category personal data. The Data Protection Legislation stipulates that special measures must be taken in the process and protection of this type of data as it is more sensitive and could create more significant risks to a person's fundamental rights and freedoms . Types of special category personal data include:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life or
- sexual orientation

Data Subject

3.3 The identified or identifiable living individual to whom personal data relates.

Data Controller

3.4 Data Controllers are 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.

Data Processor

3.5 A data processor is 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.

Data Security and Protection Toolkit (DSPT)

3.6 The DSP Toolkit is a comprehensive and rigorous set of standards describing how information is to be managed in an NHS setting. The organisation self-assesses compliance against these, uploading the necessary evidence to the DSP Toolkit portal provided by NHS Digital.

Breach Notification

3.7 Under the GDPR, breach notification to National Regulatory Body (which in the UK is the ICO) is mandatory for all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". **This must be done within 72 hours of first having become aware of the breach.** Data processors will also be required to notify data controllers "without undue delay" after first becoming aware of a data breach.

Information Commissioner's Office (ICO)

3.8 The UK's independent supervisory authority which upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Information Asset/Information Asset Owner

3.9 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.

Information Governance (IG)

3.10 Information governance (IG) is the set of multi-disciplinary structures, policies, procedures, processes and controls implemented within the Trust to manage information, supporting the organisation's immediate and future regulatory, legal, risk and operational requirements.

4. ROLES AND RESPONSIBILITIES

Trust Board of Directors

4.1 The YDH Trust Board is the data controller for the purposes of the General Data Protection Regulations 2016 and the Data Protection Act 2018.

4.2 The Board is responsible for ensuring that information within the Trust is processed according to statutory requirements and arrangements are in place for the management of Data Protection.

4.3 Responsibility for compliance with the standards set out in the DSPT rests with every officer of the Trust, including executive directors, clinical chairs, divisional directors, heads of profession, senior managers, etc.

Senior Information Risk Officer (SIRO)
Nominated SIRO at YDH – Tim Newman, Chief Finance and Commercial Officer

4.4 The Senior Information Risk Owner (SIRO) is an executive director who takes overall ownership of the organisation's information risk 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.

4.5 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.

4.6 The SIRO implements and leads the IG risk assessment and management processes within the organisation and advises the Board on the effectiveness of information risk management across the organisation.

Data Protection Officer
Appointed Data Protection Officer at YDH – Samantha Hann, Trust Risk Manager and Data Protection Officer

4.7 The Trust, as a public authority, will appoint a Data Protection Officer in order to comply with the requirement within under the General Data Protection Regulations.

4.8 The Data Protection Officer will:

- Inform and advise the Trust and its employees who carry out processing of their obligations pursuant to the Data Protection Legislation
- monitor compliance with the Data Protection Legislation 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 ICO
- Act as the contact point for the ICO 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 SIRO 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 Annual Governance Statement
- Be responsible for providing specialist Information Governance advice
- Ensure the DSPT is submitted accurately and on time
- Ensure that the Trust fulfils Individual rights under Data Protection Legislation including Data Subject Access Requests

4.9 The Data Protection Officer has responsibility for maintaining awareness of confidentiality and security issues for all staff.

4.10 The DPO & Information Governance Manager are jointly responsible for reporting any Data Protection breaches to the Information Governance Steering Group and if necessary informing the ICO.

Caldicott Guardian
Nominated Caldicott Guardian at YDH – Tim Scull, Medical Director

4.11 The Caldicott Guardian has responsibility for reflecting patients' interests regarding the use of patient identifiable information and overseeing disclosures of patient information including extraordinary disclosures (those which are not routine) in accordance with the 'NHS Confidentiality Code of Practice' (November 2003).

4.12 The Caldicott 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 Caldicott 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 IG requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

Information Governance Manager
Appointed Information Governance Manager at YDH – Karen Carter, Medical Records & Information Governance Manager

4.13 The Information Governance Manager is responsible for providing support and delivering the appropriate education to all individuals to ensure they are clear about their responsibilities when handling information and how to report any breaches of confidentiality.

4.14 The DPO & Information Governance Manager are jointly responsible for reporting any Data Protection breaches to the Information Governance Steering Group and if necessary informing the Information Commissioners Officer.

Clinical Governance Department

4.15 The Clinical Governance Department monitors any breaches of confidentiality reported through the Trust Incident Reporting System (Ulysses Safeguard). The Trust Risk Manager is responsible for adding any risks to the Risk Register ready for review by the Information Governance Steering Group.

IT Operations Manager
Appointed IT Operations Manager at YDH – Jim Mills, IT Operations Manager

4.16 The IT Operations Manager is 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.

Information Governance Steering Group (IGSG)

4.17 The IGSG reviews any breaches of the Data Protection Legislation as logged on the Trust's Incident Reporting System (Ulysses Safeguard).

4.18 The IGSG is responsible for raising awareness of any incidents to the SIRO for escalating to the Board of Directors and Chief Executive.

4.19 The IGSG will maintain the IG Risk Register.

4.20 The IGSG will 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

4.21 The IGSG will ensure that formal evidence of compliance across information governance disciplines is provided.

Information Asset Owners

4.22 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 lawful basis for holding and processing the data.

All Staff

4.23 All staff must:

- Understand their legal obligation to keep personal information confidential, to ensure they do not breach the data protection principles and uphold individual's rights
- Participate in induction, mandatory and awareness training sessions
- Be aware of the Trust's nominated Information Governance Manager, Data Protection Officer and Caldicott Guardian
- Challenge and verify where necessary the identity of any person who is making a request for confidential information and determine the validity of the reason for requiring that information
- Report actual or suspected breaches of confidentiality to their line manager
- Ensure data is recorded accurately and in a legible manner

5. DATA PROTECTION

5.1 The Data Protection Legislation is about ensuring that personal data about an individual is processed fairly and lawfully in order to protect the rights of an individual.

5.2 Whether held in electronic or paper form, personal data, within the Trust is taken to include:

- All patient information, including health records
- All staff information
- Any other personal data held on suppliers, contractors etc.

5.3 All staff employed by the Trust are affected by the Data Protection Legislation:

- They have rights as employees about whom data is held and
- They have obligations as healthcare professional who collect data about patients

6. DATA PROTECTION PRINCIPLES

6.1 The Trust and its staff (including temporary and agency) will at all times comply with the data protection principles set out in Article 5(1) of the GDPR. These principles specify (in summary) that personal data must be:

- (Principle A **'Lawfulness, Fairness and Transparency'**) processed lawfully, fairly and in a transparent manner in relation to the data subject
- (Principle B - **'Purpose Limitation'**) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- (Principle C - **'Data Minimisation'**) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- (Principle D - **'Accuracy'**) accurate and, where necessary, kept up to date
- (Principle E - **'Storage Limitation'**) 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 F - **'Integrity and Confidentiality'**) 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

6.2 Article 5(2) of the GDPR adds an addition principle that "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**')."

6.3 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 Data Protection Legislation 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 A)
- 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 A)
- The Trust will identify the legal basis for processing the personal data it holds. IAOs shall be responsible for ensuring that this is done for the assets for which they are responsible and associated data flows (Principle A)
- 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 C)
- 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 Data Protection Legislation provides 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 (Principles A, B, C & F)

- 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 E)
- 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 (Principles A & C)
- 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 F)
- Appropriate safe haven and faxing procedures will be maintained for the transmission of personal data (Principle F)
- 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 those handling subject access requests will receive additional support and training (Principle F)
- 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 C & D)
- 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 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 and Investigation Management Policy (Principle F)
- 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 F)
- It complies with the NHS Information Security Management standards including cyber security
- The Trust will appoint a Data Protection Officer as set out in section 4 of this policy

7. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

7.1 Article 5(1)(a) GDPR requires that all personal data is processed lawfully, fairly and in a transparent manner. Processing is only lawful if there is a lawful basis under Article 6 GDPR. To comply with the accountability principle in Article 5(2) GDPR, the Trust must demonstrate that a lawful basis applies and under the individual's right to be informed under Articles 13 and 14, the Trust is required to provide individuals with information about the lawful basis for processing by including these in the Trust's privacy notice. If no lawful basis applies to the processing, the processing will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully.

7.2 The lawful basis for processing personal data are set out in Article 6(1) of the GDPR. At least one of these must apply whenever personal data is processed:

- **(a) Consent:** the individual has given clear consent to process their personal data for a specific purpose
- **(b) Contract:** the processing is necessary for a contract held with the individual, or because they have asked for specific steps to be taken before entering into a contract
- **(c) Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations)
- **(d) Vital interests:** the processing is necessary to protect someone's life
- **(e) Public task:** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law
- **(f) Legitimate interests:** the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply for public authorities i.e. the Trust, for processing data to perform official tasks)

7.3 The lawful basis for processing special category personal data are set out in Article 9(2) of the GDPR. At least one of these must apply whenever personal data is processed:

- **(a) Explicit Consent:** the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- **(b) Obligations under employment, social security or social protection law:** 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) Vital Interests:** 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) Charity or not for profit bodies:** 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) Manifestly made public:** processing relates to personal data which are manifestly made public by the data subject
- **(f) Legal Claims:** processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- **(g) Substantial public interest:** processing is necessary for reasons of substantial public interest
- **(h) Provision of health and social care:** 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 Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3
- **(i) Public health:** 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) Historical, statistical or scientific purposes:** processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

7.4 The lawful basis for processing can affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent			✘ but right to withdraw consent
Contract			✘
Legal obligation	✘	✘	✘
Vital interests		✘	✘
Public task	✘	✘	
Legitimate interests		✘	

8. INDIVIDUAL RIGHTS

8.1 The Trust will maintain appropriate procedures and guidance for both staff and those interacting with the Trust (please refer to the Standard Operating Procedure for the Management of Individual Rights under the Data Protection Legislation) to ensure that individuals are given and can exercise their rights under GDPR including:

- The **right to be informed** about the processing of their personal data under Articles 13 and 14 of GDPR in the form of a privacy notices on the Trust's 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 data portability** under Article 20
- The **right to object** to processing under Article 21 GDPR and **right to limit automated individual decision making** under Article 22

9. RIGHT OF ACCESS – SUBJECT ACCESS REQUESTS

9.1 All data subjects, or someone acting on their behalf, can request to view their personal data held by the Trust.

9.2 All applications regarding patient personal data must be made in writing to the Health Records Manager as outlined in the Trust's Health Records Management Policy.

9.3 Under GDPR, all data controllers and data processors have one month to respond to a subject access request and can no longer charge a fee to respond to a request in most circumstances.

9.4 Further detail in relation to individual rights and timeframes are included within Appendix 1.

10. DISCLOSURES TO OTHERS

Statutory Requests

10.1 All statutory requests from courts or Coroner's offices etc will be complied with by the Clinical Governance Team. If appropriate the patient may be informed that the data has been disclosed unless this would prejudice criminal investigations.

Medico-Legal Requests

10.2 All requests from Solicitors and healthcare providers will only be complied with if the Trust is in receipt of written consent of the patient or their representative. These requests will be managed by the Clinical Governance department.

Police

10.3 All requests from the police for personal data will be viewed on a case by case basis via the Clinical Governance department who will decide if the information can be disclosed.

10.4 All requests must be in writing using the documentation provided by the Police authority.

10.5 The lawful basis for disclosure (without the patient's consent) to the police are under Article 6(1)(c) and would include:

- Prevention of Terrorism Act 1989 and Terrorism Act 2000 - it is a statutory duty to inform the police about information gained (including personal information) about terrorist activity

- The Road Traffic Act 1988 - it is a statutory duty to inform the police, when asked, the name and address (not clinical information) of drivers who are allegedly guilty of an offence

- Court order - where the courts have made an order the information must be disclosed unless the Trust decides to challenge the order of the court

11. EXEMPTIONS

11.1 Exemptions under the Data Protection Legislation are included within Article 23 of GDPR and Schedules 2-4 of Data Protection Act 2018. There are specific reasons why access to personal data may be denied including:

- Where the data released may cause serious harm to the physical or mental condition of the patient, or any other person
- Where access would disclose information relating to or provided by a third party. (where consent had not been received by the third party to release their data) N.B. this does not include information recorded by Trust employees as part of their normal duties

12. TRANSFER OF PERSONAL DATA

12.1 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.

13. HUMAN RESOURCES

13.1 Staff Contracts of Employment are monitored by the Trust's Human Resources Department. All contracts of employment include a data protection and general confidentiality clause. Agency and contract staff are subject to the same rules.

13.2 Any member of staff current, past or potential (applicants) who wish to have a copy of their information under the subject access provision of the Data Protection Legislation have the right to access information held on them and applications should be made to the HR Team.

14. BREACHES

14.1 The Data Protection Legislation introduces a duty on data controllers and data processors to report certain types of personal data breaches which meet the criteria of the DSPT IG Incident Matrix to the relevant supervisory authority. There is a requirement this must be completed by the data controller within 72 hours of becoming aware of the breach. Data Processors are required under Article 33(2) to inform the data controller without undue delay as soon as they become aware of a breach.

14.2 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, data controllers must also inform those individuals without undue delay.

14.3 All data controllers and data processors should have robust breach detection, investigation and internal reporting procedures in place to facilitate decision-making about whether or not the incident needs to be notified to the relevant supervisory authority and the affected individuals.

14.4 All staff have a duty to report any breaches to their Manager, Data Protection Officer and Information Governance Manager under the Trust's Incident Reporting and Investigation Management Policy and Trust Risk Management Strategy. This will be reported through the Trust Incident Reporting System and if a theme or risk is identified, recorded on the Risk Register.

14.5 Where a breach has occurred, disciplinary action may be taken and working practices and procedure will be reviewed.

14.6 Serious breaches, or serious untoward incidents, will be addressed by the Trust Data Protection Officer and Information Governance Manager, by raising a Serious Untoward Incident Form on the DSPT and by informing the ICO.

14.7 Under the Data Protection Legislation data controllers and data processors are required to keep a record of any personal data breaches, regardless of whether the breach has reached the threshold to notify the relevant supervisory authority. This information is held on the individual incident report within the Trust's Incident Reporting System.

14.8 Failing to notify a breach when required to do so can result in a significant fine for the data controller and/or data processor by the ICO. The fine can be combined with the ICO's other corrective powers under Article 58 GDPR.

15. YEAR ON YEAR IMPROVEMENT PLAN AND ASSESSMENT

15.1 Confidentiality and Data Protection Assurance form part of the DSPT.

15.2 An assessment of compliance with requirements will be undertaken each year.

15.3 Annual reports and proposed action/development plans will be presented to the IGSG for approval of submission to the DSPT.

16. TRAINING

16.1 To ensure the successful implementation and maintenance of data protection, staff will attend IG training as part of the Trust's Induction and Mandatory Training Programme. Any additional or specialised training will be identified at staff appraisal or identified through IG/data protection incidents.

16.2 All training provided will be recorded on the individuals Electronic Staff Record (ESR) and centrally by the Academy Team.

16.3 Agency and contract staff are subject to the same rules as substantive members of staff.

17. IMPLEMENTATION, MONITORING AND EVALUATION

17.1 Data Protection compliance will be monitored through:

- The Information Governance Steering Group
- The Data Security and Protection Toolkit
- Incident Reports
- Audits
- External Reports
- The number of reportable information governance and data protection incidents
- Compliance with time limits for individual rights

18. REFERENCES AND ASSOCIATED DOCUMENTATION

- General Data Protection Regulations
- Data Protection Act 2018
- Trust Information Governance Policy
- Trust Information Security Policy
- Trust Health Records Management Policy
- Standard Operating Procedure for the Management of Individual Rights under the Data Protection Legislation
- Trust Incident Reporting and Management of Investigation Policy
- Trust Risk Management Strategy
- Trust Disciplinary Policy contained within Trust HR Manual
- Trust Freedom of Information Act 2000 Policy
- NHS Confidentiality Code of Practice' (November 2003)
- NHS Digital Data Security and Information Governance Guidance

EQUALITY IMPACT ASSESSMENT TOOL

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

		Yes/No	Comments
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 including lesbian, gay and bisexual people	No	
	• Age	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	N/A	
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so can the impact be avoided?	N/A	
6.	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7.	Can we reduce the impact by taking different action?	N/A	

If you have identified a potential discriminatory impact of this procedural document, please refer it to Yeovil Academy, together with any suggestions as to the action required to avoid/reduce this impact.

Name: Samantha Hann, Trust Data Protection Officer Date: 25 May 2018