Data Protection Compliance Policy

***Previous known as IG02 Confidentiality & Data Protection Policy, IG15 Data Encryption Policy, IG01 IG Policy, IG16 Risk Policy, IG13 Information Security Policy, Data Protection Impact Assessment Procedure**

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	The purpose of this policy is to ensure all Solent Staff, Contractors and other third parties are aware of their responsibilities, with regards to ensure the Trust's compliance with Data Protection Legislation
Document Type	[x] Policy
Reference Number	Solent NHST/Policy/ IG23 Previous policies: IG02, IG15, IG01, IG16, IG13
Version	V1
Name of Approving Committees/Groups	Information Security Group ICT Group Policy Steering Group Assurance Committee
Operational Date	May 2019
Document Review Date	May 2022
Document Sponsor (Job Title)	Chief Operating Officer and Senior Information Risk Owner
Document Manager (Job Title)	Data Protection Officer and Head of Information Governance & Security
Document developed in consultation with	Information Governance Team Information Security Group ICT Group
Intranet Location	Policies and Procedures – Solent
Website Location	Policies and Procedures – Publication Scheme
Keywords (for website/intranet uploading)	Data Protection, General Data Protection Regulations, DPA, GDPR, Information Security, Cyber Security, Impact Assessment

Amendments Summary:

Please fill the table below:

Amend No	Issued	Page	Subject	Action Date

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes
1	02/01/2019	Sadie Bell, DPO	-	This policy has been produced by amalgamating similar policies and has been updated to reflect current Data Protection Legislation. Previous policies are; Confidentiality & Data Protection Policy Data Encryption Policy IG Policy IG Risk Policy Information Security Policy Data Protection Impact Assessment Procedure

SUMMARY OF POLICY

Data Protection Legislation: This policy outlines how the Trust will ensure that it confirms to, implements and enforces its legal obligations, as outlined by Data Protection Legislation, such as the General Data Protection Regulations 2016 and Data Protection Act 2018.

The policy clearly breakdowns the 6 Data Protection Principles, to which all staff must comply with;

- Personal data shall be processed fairly, lawfully and transparently
- Personal data shall be processed for limited purpose (purpose limitation)
- Personal data processed shall be adequate, relevant and necessary (data minimisation)
- Personal data processed shall be accurate
- Personal data processed shall only be stored for minimum period of time (storage limitation)
- Personal data processed shall be kept secure (integrity and confidentiality)

In addition the policy clearly breakdowns the 8 Data Subject Rights, informing staff that they must be aware of and adhere to these rights and ensure that they know when and how to provide Data Subject's with these rights. The Trust should display these rights on it's public website (within its Privacy Notice) and upon request. Staff should ensure that they know where Data Subject Rights are published and can provide a copy upon request. The Data Subject Rights are as outlined below;

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

It also identifies the Trust's commitment to Privacy by Design, which means that the requirements of GDPR are embedded seamlessly into culture and practice, with minimal impact to services, by utilising the Information Governance Team and allowing for compliance to become business as usual. The Data Protection Officer and there team should be used as the Practices primary contact for all queries, issues and risks around Data Protection and consultant as a matter of routine when wanting to process data in a new way, taking on a new contractor, working in partnership with another provider, etc… By allowing the Information Governance Team to become the primary contact, this will allow the Data Protection Officer to become aware of, input into, advise on and complete certain actives, where practice changes, innovation, integration etc… is taking place, implementing GDPR compliance.

The policy clearly outlines what staff can and can not do with the personally identifiable data the Trust holds and that if they use any of this data without a legal basis, that this will constitute a Data Breach, which will be reportable to the Information Commissioners Office.

Caldicott Principles: The policy outlines how other health and social care requirements work alongside Data Protection Legislation and in particular how the 6 Caldicott Principles should be implemented;

- Justify the purpose(s)
- Don't use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need-to-know basis
- Everyone with access to patient-identifiable information should be aware of their responsibilities
- Understand and comply with the law

Data Security and Protection Toolkit: This section of the policy outlines how the Trust, through the Information Governance Team will undertake the Trust's annual Data Security and Protection Toolkit and ensure full compliance with the requirements outlined in the Toolkit.

Information Security Requirements: All of the Trust's Information systems are secure and confidential and are operated in accordance within NHS guidance, ISO/IEC 27002 Code of Practice for Information Security Management, Caldicott Guidance and relevant legislation such as the Data Protection Act (2018) and that the Trust ensures that the data it is in precession of confirms to the standards of confidentiality, integrity and availability of information are maintained.

- **General Principles:** All access to confidential and/or sensitive information (whether in hard copy or on computers) located within Trust property must be restricted through the use of the same precautions that are taken for other valuable assets of the Trust. Such restrictions include perimeter security, making sure that security doors are closed properly, blinds drawn, and that any door entry codes are changed regularly, ideally when a member of staff leaves the team / area or it is suspected that someone else knows the code.
- **Information Assets:** Information Asset Owners will be responsible for keeping an up-to-date Information Asset Register for their service. This Register should include all paper and electronic Information Assets.
- **Information Classification:** Classifications will be implemented and adhered to *Personally identifiable, Organisationally sensitive, Public information*
- **Clear Screen Policy:** When moving away from your desk, you must ensure you lock your computer, by holding *'Ctrl' + 'Alt' down and pressing the 'Delete'* key. Then select *'Lock Computer'.*
- **Clear Desk Policy:** Any confidential information must be placed out of sight, in locked cabinets when not in use. This includes any portable computers that may contain confidential information.
- **Information Security:** Security Standards for Electronic Records should observe the aforementioned guidance whilst also ensuring adherence to The Computer Misuse Act 1990. This section also covers the following to ensure Trust Information Security;
    - Transferring PID
    - New Information Systems
    - Management of Manual Records
    - Electronic Records Security; Physical Security
    - Equipment Security:
    - System Ownership
    - Passwords
    - Storage
    - Information Backup
    - Transferring Data Externally
    - Disposal of Equipment and Media
    - Business Continuity
    - Personal Use
    - Local and Wide Area Networks
    - Network Drives
    - User Access to Network, Computers and Applications
    - Web Services (Internet & Email)
    - Internet
    - Email
    - Wifi
    - Social Media
    - Security of Third Party Access to NHS Networks
    - Use and Installation Software
    - Cyber Security
    - Data Encryption

Information Governance Risk Management: This section of the policy outlines how Information Governances will be reported and processed through the Trust's Risk Management / Incident processes, as per any other incident. However in addition it will also outline how the Trust's Data Protection Officer will enforce and comply with the Trust's additional legal requirements under Data Protection Legislation, to report all Serious Incidents to the Information Commissioner's Officer, within 72hrs of being informed of a Data Breach, meeting the criteria of a "serious breach".

Data Protection Impact Assessments: It is a legal requirement of Data Protection Legislation that a Data Protection Impact Assessment (DPIA) / Privacy Impact Assessment (PIA) is undertaken, where any of the following are applicable and are linked to the use of Personally Identifiable Data. The purpose of these assessments is to ensure, compliance with legal requirements, to ensure that there is a legal basis for what is proposed and that any risks to privacy are addressed at the development stage.

Services / Staff are responsible for ensuring that the Information Governance Team are notified of any new uses or changes to the use of Personally Identifiable Data, who will then in turn complete the relevant documentation. The policy outlines the process that will be followed to ensure that the Trust meets its legal obligations with regards to these assessments.

Responsibilities and Training: All staff are responsible for understanding their obligations under Data Protection Legislation and how to adhered to these. This is further enforced and awareness raised through the mandatory requirement that all staff are to receive annual Information Governance Training.

Table of Contents

Data Protection Compliance Policy

1. INTRODUCTION & PURPOSE

1.1. Solent NHS Trust has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by NHS Digital, the Information Commissioners Officer, other advisory groups to the NHS and guidance issued by professional bodies

1.2. This policy is to outline how Solent NHS Trust will ensure that it complies with all requirements of Data Protection Law, both European Law and Local Law, as well as other guidance issued by professional bodies and/or authorities and other legislation.

1.3. It should be noted that European Law affects the data of European citizens and not just applicable to countries who are part of the European Union and therefore is applicable and enforceable to any organisation that processes the data of European citizens.

1.4. This policy outlines how the Trust will ensure that is complies with (but not limited to) the following;

- General Data Protection Regulations 2016
- Data Protection Act 2018
- Access to Health Records Act 1990
- Caldicott Reports and Requirements
- Common Law Duty of Confidentiality
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Mental Capacity Act 2005
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- ISO/IEC 27002 Code of Practice for Information Security Management
- NHS Guidelines:
  - NHS Code of Practice – Confidentiality
  - NHS information Security Management Code of Practice
  - Employee Code of Practice
  - NHS and Health & Social Care Records Management Code of Practice
  - No Secrets: 'Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse'
  - Data Security & Protection Toolkit Requirements

This policy has been written in line with the above.

2. SCOPE & DEFINITIONS

2.1. This policy applies to locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), bank staff, volunteers (including Associate Hospital Managers), Non-Executive Directors, governors and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights

Policy. It also applies to external contractors, Agency workers, and other workers who are assigned to Solent NHS Trust.

2.2. Solent NHS Trust is committed to the principles of Equality and Diversity and will strive to eliminate unlawful discrimination in all its forms. We will strive towards demonstrating fairness and Equal Opportunities for users of services, carers, the wider community and our staff.

2.3. Glossary

DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
GDPR	General Data Protection Regulations
IAC	Information Asset Custodian
IAO	Information Asset Owner
PIA	Privacy Impact Assessment
PID	Personally Identifiable Data
SIRO	Senior Information Risk Owner

2.4. Definitions

- **Business Critical Information**: Where the loss of data would have a significant impact on the performance, reputation and operational effectiveness of the organisation. This may include but is not limited to Financial, personal, major projects.
- **Data:** Information which-
  - is being processed by means of equipment operating automatically in response to instructions given for that purpose.
  - is recorded with the intention that it should be processed by means of such equipment,
  - is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system or,
  - does not fall within above paragraph but forms part of an accessible record
- **Data Controller:** A person that collects personal data and who determines the purpose for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation (e.g. Solent NHS Trust) and the processing may be carried out, alone, jointly or in common with other persons.
  - **Alone** – Sole Data Controller
  - **Joint** – two or more Data Controllers who act together to decide the purpose and manner of any data processing.
  - **In common** – two or more Data Controllers who share a pool of personal data that they process independently of each other.
- **Data Processor:** Someone other than the Data Controller, who processes personal data on their behalf. Anyone responsible for the disposal of confidential waste is also included in this definition
- **Data Subject:** This is the living individual who is the subject of the personal information
- **Encryption:** A process of scrambling data unless authorisation is given to the user to view it.
- **Mobile Data Devices**: This includes any mobile device that can store data. This will include laptops, Smartphones, palm tops (or personal digital assistants), USB memory sticks, CD/DVD, iPads, etc...

- **Personal Identifiable Data (PID):** Means data which relates to an individual who can be identified from that data. This is not just name and address but also things like (not extensive);
  - Date of Birth (when used with other identifiers)
  - National Insurance number
  - Credit card number
  - Passport number
  - DNA
  - Post code
- **Patient:** Throughout this document the term "patient" is used. This term includes those who are also known as "Service Users", "Clients" and "People".
- **Privacy Notice:** A public notice telling data subjects what information a Data Controller is processing and the purpose / intended use of the data
- **Processing:** Processing means obtaining, recording or holding the data or carrying out any operation or set of operations
- **Relevant Filing System:** A structured set of information that can reference individuals either directly or indirectly.
- **Special Category Data** Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.
- **Third Party** Any person other that the Data Subject, Data Controller or Data Processor

3. DATA PROTECTION LEGISLATION

3.1. Data Protection Act 2018 / General Data Protection Regulations 2016

The Trust will ensure that it and its staff are aware of and comply with the Six principles outlined in Data Protection legislation.

3.1.1. Legislation applies to all PID held in manual files, computer databases, videos and other automated media, about living individuals. It dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff may result in disciplinary action.

3.1.2. Legislation requires Solent NHS Trust to register as a Data Controller with the Information Commissioners Officer; identifying the purposes for holding the data, how it is used and to whom it may be disclosed. Failure to register, an incorrect registration or an outdated registration, is a criminal offence. This may lead to prosecution of the organisation. The Trust's Data Protection Officer is responsible for maintaining the notification to the Information Commissioners Office. All applications/databases required under law to be registered for data protection purposes will be registered under Solent NHS Trusts global registration with the Information Commissioner and does not need to be done individually

The Data Protection Principles, that Solent NHS Trust, all employers must adhered to are;

3.1.3. Personal data shall be processed fairly, lawfully and transparently

- You must identify valid grounds under GDPR (known as a 'lawful basis') for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.

- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data (privacy notice).

To identify a lawful basis for processing please contact the Information Governance Team

3.1.4. Personal data shall be processed for limited purpose (purpose limitation)

- You must be clear about what your purposes for processing are from the start.
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

3.1.5. Personal data processed shall be adequate, relevant and necessary (data minimisation)

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

3.1.6. Personal data processed shall be accurate

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

3.1.7. Personal data processed shall only be stored for minimum period of time (storage limitation)

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements, (Records Management Policy).
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

3.1.8. Personal data processed shall be kept secure (integrity and confidentiality)

You must ensure that you have appropriate security measures in place to protect the personal data you hold. Refer to the Information Security section of this policy for further information

3.1.9. Accountability Principle

The accountability principle requires organisations to take responsibility for what they do with personal data and how they comply with the other principles.

Data controllers must have appropriate measures and records in place to be able to demonstrate your compliance.

3.1.10. Data Protection by Design / Default

GDPR identifies greater compliance requirements and the implementation of Privacy by Design reduces the administrative burden of this. Privacy by Design means that the requirements of GDPR are embedded seamlessly into culture and practice, with minimal impact to services, by utilising the Information Governance Team and allowing for compliance to become business as usual. The Data Protection Officer and there team should be used as the Practices primary contact for all queries, issues and risks around Data Protection and consultant as a matter of routine when wanting to process data in a new way, taking on a new contractor, working in partnership with another provider, etc… By allowing the Information Governance Team to become the primary contact, this will allow the Data Protection Officer to become aware of, input into, advise on and complete certain actives, where practice changes, innovation, integration etc… is taking place, implementing GDPR compliance.

3.1.11. Exemptions to the DPA 2018 and GDPR 2016

In certain circumstances personal information may be disclosed and guidance is detailed below. However it is vital in each case, that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. Where reasonable practically this should be done in conjunction with the Information Governance Team.

3.1.11.1. Disclosing information against the subject's wishes

The responsibility of whether or not information should be withheld or disclosed without the subject's consent lies with the senior manager or senior clinician involved at the time and should be done in consultation with the Trust's Data Protection Officer and where applicable Caldicott Guardian and SIRO.

Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Child abuse and vulnerable adults
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is considered to be an immediate/imminent serious threat to the healthcare professional or other staff
- Where there is considered to be an immediate/imminent serious threat to the community
- In other exceptional circumstances, based on professional consideration and consultation.
- Court Order and/or other legal requirement
  - Births and deaths - National Health Service Act 1977
  - Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
  - Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974
  - Terminations - Abortion Regulations 1991, duty to inform
  - Offenders thought to be mentally disordered – Mental Health Act 1983

- Child abuse – Children's Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

Solent NHS Trust will support any member of staff who, using careful consideration, professional judgement and has sought guidance from the Trust's Data Protection Officer and can satisfactorily justify any decision to disclose or withhold information against a patient's wishes.

3.1.12. Data Subjects Rights

The Trust and its staff must ensure it is aware of and adheres to the Data Subject Rights, as outlined by Data Protection Legislation. The Trust should display these rights on it's public website (within its Privacy Notice) and upon request. Staff should ensure that they know where Data Subject Rights are published and can provide a copy upon request. The Data Subject Rights are as outlined below;

- **The right to be informed:** Individuals should be informed of how their data will be used. This applies to both patient and staff data.
- **The right of access:** Individuals have the right to access their personal data, which is referred to as a Subject Access Request. All requests of this nature should be submitted to the Information Governance Team.
- **The right to rectification:** Personal data can be rectified if it is inaccurate or incomplete
- **The right to erasure:** This is often referred to as the "right to be forgotten". This right only applies in certain circumstances
    - the basis for lawful processing is consent and the this has been withdrawn and there is no other legal ground for processing
    - the individuals whose data is being processed objects and there are no overriding legitimate grounds
    - the personal data has been collected in relation to information society services
    - the personal data is no longer necessary for the purposes for which it was collected for
- **The right to restrict processing:** Individuals have the right to require organisations to restrict processing where:
    - accuracy is contested by the individual
    - processing is unlawful and the subject opposes erasure
    - the organisation no longer needs the data, but the subject requires it to be kept for legal claims
    - the individual has objected, pending verification of legitimate grounds.
- **The right to data portability:** Individuals have the right to receive personal data about them in a 'commonly used and machine readable format'. This right is only available where the processing is based on consent and the processing is automated.
- **The right to object:** Individuals have the right to object to:
    - processing based on legitimate interests or the performance of a task in the public interest / exercise of official authority (including profiling);
    - direct marketing (including profiling); and
    - processing for purposes of scientific/historical research and statistics.
- **Rights in relation to automated decision making and profiling**

3.2. Patient Confidentiality (Common Law Duty of Confidentiality)

3.2.1. Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

3.2.2. On admission or on first contact with the service for a particular matter, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, or those they specifically do not give permission to receive information.

3.2.3. In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

3.2.4. In the event a person lacks capacity to consent to information being shared staff should check if a person is authorised by a Lasting Power of Attorney (welfare) or been appointed by the court of protection to make that decision. The document must be seen. This person can consent on their behalf but must act in the person's best interest. If they have not then no one can consent on behalf of that person. A professional in the care team must assess if it is in the best interest of the person to share the information. The person's wishes and feeling, although not determinative, should be the starting point in this assessment. For further information see the Deprivation of Liberty and Mental Capacity Act policy.

3.2.5. In all cases, the wishes expressed must be appropriately documented in the patient's Health Records.

3.3. Breaches of Confidentiality

3.3.1. All Staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner.

3.3.2. All staff have a confidentiality clause in their contract of employment. Solent NHS Trust has an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.

3.3.3. Confidential information must not be disclosed to unauthorised parties without prior authorisation by a senior manager. Staff must not process any personal information in contravention of Data Protection legislation.

3.3.4. Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.

3.3.5. It is a breach of confidentiality and Data Protection Legislation to access, obtain or use personally identifiable data, without a justifiable reason to do so.

3.3.6. It is a breach of Data Protection Legislation and other Acts of law e.g. Computer Misuse Act 1990, for staff to unlawfully access, obtain or destroy their own personal data (both personal and medical information), without obtaining the data through lawful processes, as Solent NHS Trust is the Data Controller of this data.

3.4. Data Quality

3.4.1. Data quality is the ability to supply accurate, timely and complete data, which can be translated into information, whenever and wherever, is required. Data quality is vital to effective decision making at all levels of the organisation.

3.4.2. Poor quality data can create clinical risk, cause inconvenience to service users and staff, compromise effective decision making and impact on the Trust's ability to monitor standards of care and secure income for its services.

3.4.3. All staff should be aware of the importance of good data quality and their own responsibility for achieving it. Staff should receive appropriate training in relation to data quality aspects of their work.

3.4.4. Supplying accurate data is a complicated task for a number of reasons:

- There are many ways for the data to be inaccurate; data entry errors and missing data, etc.
- Data can be corrupted during translation depending on who is translating it, how and with what tools/processes.
- Data must relate to the correct time period and be available when required.
- Data must be in a form that is collectable and which can subsequently be analysed.

3.4.5. The following principals are used in assessment of data quality:

- Accuracy: Is the data correct and is it valid?
- Accessibility: Can the data be readily and legally collected?
- Comprehensiveness: Is the relevant data collected and are any data omissions (where intentional or otherwise known) documented.
- Consistency: Are clear and accurate data definitions implemented and adhered to? Do the data definitions define what level of detail is collected?
- Validity: Is the data up-to-date?

3.4.6. All staff will conform to legal and statutory requirements and recognised good practice, aim to be significantly above average on in-house data quality indicators, and will strive towards 100% accuracy across all information systems.

3.4.7. All staff should be aware of the importance of good data quality and their own contribution to achieving it, and should receive appropriate training in relation to data quality aspects of their work.

3.4.8. Staff with responsibility for data assurance will put in place mechanisms to ensure there is feedback to individual users on data quality issues. Wherever possible data should be corrected at source.

3.4.9. For further information, please refer to the Trust's Data Quality Policy

3.5. Pseudonymisation

3.5.1. The overall aim of pseudonymisation is to enable the legal, safe and secure use of patient data for secondary (non-direct care) purposes by the NHS (and other organisations involved in the commissioning and provision of NHS-commissioned care) and to enable NHS businesses to no longer use identifiable data in its non-direct care related work wherever possible.

3.5.2. Data usage types are identified as Primary Uses, where data is used for a purpose of directly contributing to the safe care of a patient, and Secondary Uses, where data is used for any other purpose than Primary Use. This could be for performance management, commissioning or contract monitoring.

3.5.3. **Secondary Uses (Non-Healthcare Medical Purposes):** A secondary use of data is any use which is not covered in the definition of a primary use. In essence it relates to the use of patient identifiable information which does not directly contribute to the safe care of the individual concerned. Examples of secondary use of patient data include performance management, commissioning and contract monitoring.

3.5.4. **De-identifying Data:** The process of using one or more techniques that transform data to make it less likely that individuals can be identified. The goal of de-identifying data is to render it "effectively anonymised". De-identification techniques include stripping out person identifiers, pseudonymisation, aggregation and derivation. Section 9 details how these processes should be used in practise.

3.5.5. **Effectively Anonymised Data:** Data is "effectively anonymised" when the recipient is unable to infer the identity of individuals from the data without the application of effort or resource where it would be unreasonable to anticipate in the circumstances that apply. Effectively anonymised data would almost certainly neither be considered "personal data" nor "sensitive personal data" under Data Protection Legislation, nor "confidential patient information" under the NHS Code of Confidentiality 2006.

3.5.6. **Stripping Out Person Identifiers:** This is the process of removing person identifiers from data. This may be partial (where only some identifiers are removed) or complete.

3.5.7. **Pseudonymisation:** The process of replacing person identifiers in a dataset with other values (pseudonyms) from which the identities of individuals cannot be intrinsically inferred. Examples of this process are replacing an NHS number with another random number, replacing a name with a code or replacing an address with a location code. Pseudonyms themselves should not contain any information that could identify the individual to which they relate (e.g. should not be made up of characters from the date of birth, etc.). The correct application of this process will produce the same pseudonym for a patient across different data sets and time so that patient data can still be linked.

3.5.8. **Aggregation:** This is the process of pooling data such that category totals are displayed rather than individual values. Care must be taken so that when small datasets are used an individual's identity cannot be inferred because they are the only person in a category. Most reports for contract and performance purposes provide aggregated data.

3.5.9. **Secondary Purpose Exemptions:** In the following circumstances, identifiable data can be used for secondary purposes:

- The patient's consent
- Legal requirements, such as the Mental Health census
- Regulations relating to specific organisations and their function, such as the Care Quality Commission, Audit Commission and Health Protection Agency.
- Regulations under Section 251 relating to health functions, such as Cancer Registries, communicable diseases and other Public Health functions.
- Approval by the Secretary of State for specific or class approval under Section 251, such as research projects.

3.5.10. The person(s) responsible for providing data extracts for secondary uses purposes, is to ensure that a process in place to adhered to requirements of Pseudonymisation.

3.5.11. For further information, please refer to the Trust's Pseudonymisation Policy

4. CALDICOTT PRINCIPLES / REQUIREMENTS

4.1. The Caldicott Principles have been developed for health and social organisations to work alongside Data Protection Legislation and support the sharing of PID for care related purposes.

4.2. There are 6 Caldicott Principles which are;

- **Justify the purpose(s):** Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
- **Don't use patient-identifiable information unless it is absolutely necessary:** Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
- **Use the minimum necessary patient-identifiable information:** Where the use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
- **Access to patient-identifiable information should be on a strict need-to-know basis:** Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
- **Everyone with access to patient-identifiable information should be aware of their responsibilities:** The organisation must ensure that those handling patient-identifiable information, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **Understand and comply with the law:** Every use of patient-identifiable information must be lawful. The Caldicott Guardian is responsible for ensuring that the organisation complies with legal requirements.

4.3. The duty to share information can be as important as the duty to protect patient confidentiality: Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

5. DATA SECURITY AND PROTECTION TOOLKIT (DSPT) COMPLIANCE

5.1. The DSPT is an online self-assessment tool, mandated by NHS Digital, which enables Health and Social Care organisations to measure their performance against Data Security and Information Governance legislation. The DSPT was developed following the National Data Guardian's (NDG) review which was instated in July 2016 and is information security focused.

5.2. It incorporates the ten Data Security Standards, which were a result of the National Data Guardian (Caldicott) review and therefore the focus of the Toolkit:

5.2.1. **Leadership Obligation 1 – People:** Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

- All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
- All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
- All staff complete appropriate annual data security training and pass a mandatory test.

5.2.2. **Leadership Obligation 2 – Process:** Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses

- Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
- Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
- Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
- A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

5.2.3. **Leadership Obligation 3 – Technology:** Ensure technology is secure and up to date

- No unsupported operating systems, software or internet browsers are used within the IT estate.
- A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
- IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.

5.2.4. The Data Security and Protection Toolkit features ***forty assertions*** that have been identified for Mental Health Trust's, Community Trust's and General Practitioner's to provide evidence of compliancy against. Within the forty assertions there are ***thirty-two mandatory assertions*****,** which if not met, the Trust will be deemed as non-compliant with the whole toolkit.

5.3. Solent NHS Trust has tasked the Information Governance Team with ensuring compliance of these assertions and completed the annual Toolkit Submission and required baseline submissions.

6. INFORMATION SECURITY REQUIREMENTS

6.1. Standards for ensuring information security

6.1.1. All of the Trust's Information systems are secure and confidential and are operated in accordance within NHS guidance, ISO/IEC 27002 Code of Practice for Information Security Management, Caldicott Guidance and relevant legislation such as the Data Protection Act (2018).

6.1.2. Confidentiality, integrity and availability of information are maintained.

6.1.3. This section describes the policy and principles for ensuring all PID / Sensitive Data held by the Trust, in both electronic & paper format are held, stored, shared and destroyed securely. In many cases the day to day local procedures and practices will exceed these standards.

6.1.4. General Principles: All access to confidential and/or sensitive information (whether in hard copy or on computers) located within Trust property must be restricted through the use of the same precautions that are taken for other valuable assets of the Trust. Such restrictions include perimeter security, making sure that security doors are closed properly, blinds drawn, and that any door entry codes are changed regularly, ideally when a member of staff leaves the team / area or it is suspected that someone else knows the code.

6.1.5. Information Assets: Information Asset Owners will be responsible for keeping an up-to-date Information Asset Register for their service. This Register should include all paper and electronic Information Assets.

ICT will also be responsible for keeping an up-to-date Asset Register of all electronic devices e.g. laptops, desktops, iPads, Blackberries, Mobile Phones, etc….

6.1.6. Information Classification

Personally identifiable – Structured filing systems (electronic or paper) containing identifiable information are, subject to the terms of Data Protection legislation and afforded a degree of legal protection in their handling.

Organisationally sensitive – This classification includes any information relating to activity that does not identify an individual, but may cause operational difficulties if the information became unavailable or was disclosed in the wrong environment. This classification should not in any way be seen as a level of secrecy from the public. It is envisaged it will only be used for documentation that if disclosed would be prejudicial to developments (such as draft service development plans).

Public information – Information that does not contain data on individuals nor has any degree of service sensitivity will be considered in the public domain. In line with developments of the 'Freedom of Information Act' – this information will be actively contained within publication schemes and made freely available. It is envisaged the majority of documentation that is afforded 'organisationally sensitive' status will at appropriate time be made publicly available.

Responsibility for definition of an information asset into these categories remains with the originator or owner. By default any information identifying an individual falls into the 'Personal Identifiable' category.

6.1.7. Clear Screen Policy: When moving away from your desk, you must ensure you lock your computer, by holding *'Ctrl' + 'Alt' down and pressing the 'Delete'* key. Then select *'Lock Computer'.* You may be working on a confidential piece of work and by locking your screen, it

ensures that no one else will be able to read or access any other files on your computer in your absence.

6.1.8. **Clear Desk Policy:** Any confidential information must be placed out of sight, in locked cabinets when not in use. This includes any portable computers that may contain confidential information.

When moving away from your desk ensure you do not leave person identifiable / sensitive information available for others to view, put it in a drawer or cover it up.

All other Trust assets including phones, keys, USBs, documents and other valuables must be stored in a locked drawer, cupboard or room.
Whiteboards should be erased after use.

6.1.9. **Transferring PID**

Staff must adhere to this policy when sending or receiving personal identifiable, sensitive or confidential information whether this is by:

- Email
- Post (internal, external or private courier)
- Transfers by hand or in person
- Telephone voice calls
- Text messages
- Removable media e.g. encrypted USB memory sticks, CDs, external hard drives, backup tapes etc
- Portable devices e.g. Smartphones, Laptops, PDA's, etc.

See Appendix B: Guidance for Sharing Personal Information.

Portable devices and PID should never be left in a car overnight. If taken home or out of working hours, then this must be taken in doors and placed in a secure / restricted location and returned to base as soon as possible.

6.1.10. **New Information Systems:** All new critical information systems must have a System Level Security Policy (SLSP) produced and approved by the IAO.

All software used on the Trust's network must be strictly controlled and approved. Measures such as user rights to load software are controlled to ensure users do not compromise information systems. Software changes must be subject to formal change control and test procedures.

Unauthorised software should be reported to the Trust's Information Security Manager for investigation.

6.1.11. **Identification Badges:** Staff must carry and wear identification badges and where practical should challenge individuals not wearing identification in areas they know are not for public access. In such areas visitors should be met at reception points and accompanied at all times. Unaccompanied visitors should be taken to the Trust employee they are visiting. Where staff are Agency and contractors must be issued with temporary badges that clearly advise the start and termination date of their contract and/or day visitor badges/passes.

6.1.12. **Home Working:** Staff that use Trust computers at home for work must ensure that they safeguard corporate equipment. This includes maintaining the physical security of the

computer and any confidential information, held on the machine. e.g. computers holding confidential information must be encrypted.

Staff, are also responsible for ensuring that they do not allow the system to be accessed by any unauthorised individuals.

Staff must connect through the relevant VPN approved remote access methods.

6.2. Paper Records Security

6.2.1. **Management of Manual Records:** Storing, archiving and disposing of manual records will be dealt with in accordance with the Health & Social Care DH Records Management Code of Practice (which Solent NHS Trust has adopted) and the Trusts Records Management Policy.

6.3. Electronic Records Security

6.3.1. **Physical Security:** Computers that hold confidential information should be located in rooms that have lockable doors or if not possible should be secured to the desktop. In the case of laptops these must be encrypted and stored securely out of sight overnight. Staff on termination of employment or contract must surrender door keys and all Trust equipment.

All computer assets including hardware and software must be recorded on an asset register that details the specification, user and location of the asset. The IT service desk must regularly update the asset register. Each machine will be security marked and its serial number recorded.

Non-portable IT equipment must not be moved without notifying the Service desk in advance

Computers (whether supplied by the Trust or a non-Trust computer) must not be connected to any network, including the Internet, without the permission of the IT service desk.

The Information Asset Owner (IAO) should be aware all computer equipment removed/used off-site. When removed from Solent NHS Trust premises the user must take all reasonable care whilst in their possession. In particular, equipment must not be left visible in unattended cars, in cars overnight or on open display; this also applies if used at home and consequently vulnerable to theft. Equipment used at home should be stored securely and out of sight when not in use.

Any theft, suspected theft, actual or suspected misuse must be reported to the Information Governance Team and the IT Helpdesk management.

Employees should make every effort to minimise the risk that fire, flood and accidents do by causing damage machines.

Equipment must be sited to minimise the risk of accidental damage. Common hazards include drinks cups, food and overstraining of leads when a machine is moved.

Excessive paper should not be stored on or near computer equipment due to the risk of fire; computers generate a lot of heat in use and need adequate ventilation.

Any suspected damage, which may not be visible externally (for example after dropping a computer), must be reported to the IT service desk for checking before continued use.

6.3.2. **Equipment Security:** To avoid interruption to business activity, IM&T equipment will be protected against loss or damage. Environmental controls will be installed to protect central/key equipment.

The Trust also requires the protection of associated network cabling and wiring from the threats of access, removal, fire, water, electrical surges and power-cuts.

All critical processing equipment, including file servers, will be covered by third party maintenance agreements.

All such third parties will be required to sign confidentiality agreements –this should be included in all Service Level Agreements/contracts.

6.4. Information Security

Security Standards for Electronic Records should observe the aforementioned guidance whilst also ensuring adherence to The Computer Misuse Act 1990. The relevance of the Act when used in application to electronic records is that it creates three offences of unlawfully gaining access to computer programmes.

The offences are:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or cause commission of further offences; and
- Unauthorised modification of computer material.

Access is defined in the Act as;

- Altering or erasing the computer program or data;
- Copying or moving the program or data;
- Using the program or data; or
- Outputting the program or data from the computer in which it is held (whether by having it displayed or in any other manner).

Unlawful access is committed if the individual intentionally gains access; knowing they are not entitled to do so; and is aware they do not have consent to gain access, even if they have access to the record / system.

The 'further offence' applies if unauthorised access is carried out with intent to commit or cause an offence.

The 'Modification' offence applies where an individual does any act causing unlawful modification of computer material and does so in the knowledge that such modification is unlawful, and with the intent to:

- Impair the operation of any computer;
- Prevent or hinder access to any program or data held in any computer; or
- Impair the operation of any such program or the reliability of any such data.

The above also applies to paper based information, which is covered under other Data Protection legislations.

6.5. System Ownership

Each system will have a specified Information Asset Owner (IAO) who with the Information Asset custodian (IAC) or equivalent must ensure compliance with the Information Security

section of this Policy, ensuring the appropriate use of equipment, support and maintenance. Each critical system must have a documented system level security policy (SLSP) which will maintain security accreditation and support IG assurance reporting to the SIRO.

6.6. Passwords

Passwords are required when accessing a Trust account to protect the Trust, CGI and confidential patient information.

Password Guidance; Passwords have a valuable role in protecting systems from unauthorised access and are most effective when they:

- carry no meaning
- are not names or have other connections to the user
- are changed regularly and are not related to previous passwords
- are a minimum of 8 characters
- are a mixture of letters (upper / lower case), numbers and symbols
- are kept secret
- are not 'VISITOR', 'GUEST' or similar
- are not shared

Passwords used within the Trust systems must be a minimum of 8 characters; they must be changed at least every 90 days and accounts disabled when a user no longer requires access to the system. A default password will be assigned when accounts are set-up. The user will then be prompted to change the password on first use.

Only the person to whom it is issued should use that password. Employees must never divulge a password.

Only in exceptional circumstances and not without agreement of the Information Asset Owner will ICT change a password to grant temporary access, after-which, a new password will be generated before further access to the system.

This policy will ensure proper auditing of accesses made can be maintained and security of original user account is not compromised.

6.7. Information Storage

The Information Security section of this Policy prohibits the storage of PID outside of the network as this is considered an unacceptable risk and obligations under the DPA require that personal information remains secure at all times. This information is to be stored on the network servers with restricted access. This will maintain confidentiality, availability and integrity of that information and reduce impact of breaches in physical security. Similarly for manual patient records they must not be removed from Trust premises unless a risk assessment has been carried out and can be justified under the SIRO Guidelines & Caldicott Principles. The justification must be approved and documented by the line manager/Information Asset Owner.

Desktop computers and portable devices must not be used to store or transfer confidential information unless they are encrypted to an approved standard and comply with the SIRO Guidelines & Caldicott Principles.

Any bulk extracts or transfers of confidential or sensitive data must be authorised by the responsible Director or the Information Asset Owner for the work area and approved by the SIRO.

No information must be held that breaches Data Protection Legislation or formal notification and guidance issued by NHS Digital. All personal identifiable information must also be used in accordance with the SIRO Guidelines & Caldicott Principles.

All staff must comply with Data Protection legislation and must not be allowed to access information until line managers are satisfied that they understand and agree these responsibilities. This should be included in all contracts of employment.

Information that is no longer required should be disposed or archived securely and in line with the Records Management Policy. Paper records containing personal information must be disposed of securely. Anything containing personal and/or confidential information that does not require archiving must be shredded after use. Any confidential information must be placed out of sight, preferably in locked cabinets when not in use.

Databases holding personal identifiable health information should have a defined security and system management policy for the records and documentation. This documentation must include a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection Notification.

6.8. Information Backup – Network Backup

The Trust requires it's ICT / System Providers to ensure information is backed up in accordance with the written back-up procedures to provide at least one month's information retention. Such information will be stored off-site, as required, to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.

All back-ups will be maintained securely and will be erased when no longer required. These backups are kept for the purposes of recovery from computer system failure, not as a mechanism for meeting any requirements for records storage. Archival of electronic files for longer-term storage is possible and requirements should be discussed with your manager and IT support team in the first instance.

If information is copied between systems within the network, employees should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the first.

6.9. Transferring Data Externally

Transferring data outside of Trust computing environments must be avoided unless supported by a valid business reason. Regardless, users must be aware of the requirements for copying, transmitting, and storing information, outlined in Appendix B when considering how data may be transferred outside of the Trust.

6.10. Disposal of Equipment and Media

Computer assets (includes removable computer media, such as tapes and disks) must be disposed by the Trusts ICT provider CGI Ltd.

All data storage devices will be purged of sensitive data before disposal. Where this is not possible, due to quantities involved the equipment or media will be destroyed by a technical

waste service provider. The Information Governance Team should be contacted for further details.

Copies of destruction certificates for all assets that are decommissioned on behalf of the Trust must be made available to the Data Protection Officer and Head of Information Governance and Security.

The asset register must be updated by the IAO or the organisation with delegated responsibility for secure disposal.

Printed matter should be confidentially destroyed using the shredders and confidential waste bins provided by approved contractors. Where large quantities of confidential waste need to be disposed of (such as during relocation of staff) the Information Governance Team can help to securely facilitate this.

6.11. Business Continuity

All designated critical systems must have a written business continuity plan (BCP) these will be drawn from the IT providers BCP and approved by the Trust; Local BCP will be the Trust responsibility

This is required to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

The Trust policy and scope for activating disaster recovery of computer hardware and software contingency is set out in the separate disaster recovery plan agreement held by the Trust IT lead and ICT Services.

6.12. Personal Use

The following use of Trust resources is considered acceptable use:

- Conduct research within the bounds of appropriate and ethical professional behaviour.
- Upgrade professional development skills (training, e-learning, professional body certification, and maintenance).
- Collaborate with work-related professional contacts and participate in discussion groups on subjects of professional interest.
- Conduct internal and client work-related business with email and Internet, using common sense and ensuring proper email content when sending and receiving work-related emails.
- Use emails and Internet browsing in a manner that does not interfere with other business activities, disrupt services, or incur additional costs to the Trust or CGI.

The following use of Trust resources is considered unacceptable use:

- Use Trust assets for private or personal gain.
- Make misrepresentative or fraudulent statements or claims when using Trust assets.
- Access, view, create, promote, or distribute any material that:
    - Is illegal, as defined by the laws of the jurisdiction within which it is accessed, viewed, created, or distributed;
    - Defames, libels, or promotes hatred or discrimination against any gender, ethnicity, race, religion, nationality, or social group;
    - Libels, abuses, embarrasses, or harasses other users, management, clients, or partners;
    - Adversely impacts Trust relationships with clients and/or the Trust's reputation;
    - Adversely impacts CGI's relationships with other clients and/or CGI's reputation, investor confidence, or stock trading value;

- Contains any of the following: pornography, chain mail, racial or hate propaganda websites, unauthorized mass mailings, spam, malicious code, malware, or hacker/cracker tools.
- Modify ICT assets, or change the standard configuration of Trust systems or assets;
- Download or install third party software without proper authorization and review of licensing;
- Bypass or reduce any Trust, CGI, partner, or supplier security mechanisms;
- Conduct or use any form of intrusion, invasive techniques, network monitoring or scanning outside the scope of regular authorized duties.
- Cause security breaches, congestion, or disruption to Trust assets and/or network systems or sites.

Connecting to the Trust network

- Do not install an unauthorized wireless connection in Trust or other CGI-managed facilities.
- When working remotely (at home, in an airport, in a hotel, etc.), users must use a secure Trust-authorized remote connection to connect to Trust networks and services.
- Users' computers must not be connected to the Trust wired network and a non-Trust managed wireless network simultaneously. WIFI should be disabled when not in use.
- To ensure that computer operating systems, anti-virus and other software remain up-to-date, all users working externally who do not visit a Trust site regularly must connect to the Trust network at least once a month through a Trust-authorized remote access solution.

Authorised devices

- Only Trust-approved smartphones/tablet/ computers that meet the necessary handheld standards can connect to the Trust network and/or email system.

Personal emails

- It is prohibited to send any emails containing Trust information to or from a personal email account.

6.13. Local and Wide Area Networks

Through connection to the Trusts network it is possible to receive and forward information to other users of the network and other networks using, for example, electronic mail. Should employees receive, identify how to, or gain access to unauthorised information on any networks then this event must be reported to the Trust's Information Security Manager.

A security log must be maintained of all access to the Trusts network by external organisations. The IT service desk will hold this log. Only computers approved by the Trust may be connected to the network, and in line with the Trust's policy on connection.

All computer files, transferred from other networks (including public access networks such as the 'Internet') and removable media must be checked for viruses before use within the organisation. Files stored on the network will be checked daily.

Equipment should not be used until advised by the installation technician that the system is ready for use.

Employees must inform the IT service desk if a virus attack is detected or suspected.

6.14. Network Drives

Any drive/folder identified as a restricted drive, should have a nominated 'Gatekeeper'. The Gatekeeper will be the only person who can authorise access to the drive/folder and will be responsible for ensure that only authorised people have access and that this authorisation is kept up-to-date e.g. when staff leave a service their permission is removed.

6.15. User Access to Network, Computers and Applications

Only Solent NHS Trust staff or authorised support agents are authorised to access Trust computers and the information held on them or National Systems such as Care Records System (if issued with a Smartcard). Unauthorised access may contravene the Computer Misuse Act (1990), Data Protection legislation and other legislation leaving *the user* open to prosecution.

Services managers must provide formal authorisation of user access request to the network, computers and applications following the system level security policies for critical systems

No individual will be given access to a live system unless properly trained and made aware of his or her security responsibilities.

User access to the network will be protected by allocated user accounts and passwords and must use a strong authentication for remote access to the network. Employees must be granted access only to those areas that they require to perform their duties.

The Human Resources department will provide a leavers list each month via the Electronic Staff Records System (ESR) to advise the Registration Authority information governance staff who will in turn inform the relevant service desks of staff changes affecting computer access (for example job function changes / leaving department or organisation) so that access may be amended or deleted, from effective dates. The RA Manager will also be informed of any leavers to ensure the necessary Smartcard revoking procedures are implemented.

A remote access form can be completed online by manager of a staff member and sent to the IT service desk to allow remote access for staff to be set up,.

Evidence will be required from IT providers on user access to networks, applications and computers as defined in the Trust System Level Security Policies (SLSP).

6.16. Web Services (Internet & Email)

Staff should be aware that all email and web use may be monitored by the Trust and its agents. The policy contains details of this.

Internet

The Trust regards the Internet as a tool for managing and delivering services and as a useful mechanism for the open exchange of ideas and non-confidential sources of information between its employees, other members of the NHS and the public. The Internet can also be a wasteful resource in terms of the amount of time that it could consume if not used wisely or appropriately.

The following excessive and/or inappropriate use of the internet is not acceptable:

- Participate in non-work related chat-rooms, social networking, web conferencing or similar services unless you are authorised to do so on behalf of the Trust.

Use file sharing services (including instant messaging, social networking and cloud services) for the sharing of information, music, videos, pictures or software.

- Use on-line (cloud) storage (e.g. Dropbox, Google Documents, and Sky Drive) to store, edit or transmit Sensitive Information, unless approved by the Trust's Data Protection Officer.
- Use the Internet for accessing or playing games.
- Use the Internet to obtain unauthorised access to other organisation's IT facilities or data or information which is personal or private to another individual or organization
- Create, download, upload or transmit material that may be construed as disruptive or a hindrance to the work of others
- Breach copyright or licensing laws when distributing or using material obtained via the Internet
- Use the Internet to commit the Trust to purchasing or acquiring goods or services without proper authorisation.
- Set up web-sites relating to the Trust or its services without prior and appropriate authorisation of the Trust.

Email

E-mail is identical to any other form of the Solent NHS Trust business correspondence and can be legally binding or challenged. The Freedom of Information Act and Data Protection legislation states that emails are releasable under the Acts.

The sending of emails containing sensitive personal data to external web mail addresses should be avoided; web mail needs to be appropriately encrypted to be secure.

All e-mails to be sent externally (to non-Trust individuals) must, at a minimum, contain the following notice (or similar) which is automatically implemented by the Trust's ICT Provider, not staff action is required:
Proprietary/confidential information belonging to Solent NHS Trust may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason that this message may have been addressed to you in error, you may not use or copy or deliver this message to anyone else. In such case, you should destroy this message and are asked to notify the sender by reply email.

Auto-forwarding from a Trust email account to any external email account is forbidden, unless otherwise approved by a senior manager.

NHSMail has been mandated as the only permitted methods of emailing PID **externally** to NHS Organisations. Solent NHS Trust has adopted NHSMail as its secure external email system; both the sender and receiver must have NHSMail accounts or similar Government approved encrypted mail systems. NHSmail is only encrypted and secure when sent from an NHS mail account to another NHSmail account or approved encrypted email services, which are similarly secure for transfer of PID. Examples can be found in Appendix B.

Staff can obtain an NHSMail account through Solent NHS Trust's ICT provider.

If sending PID via email to any other account where there is no NHSmail account or other secure network, always use a Trust approved encryption source. Where there is a business need, the Trust can sponsor third party organisations to have an NHSmail account.

The sender must always confirm the NHSmail address of the recipient (i.e. DO NOT assume it is firstname.lastname@nhs.net, always use the directory on the NHSmail website to check.

The receipt facility must always be used for transfers of PID.

Whatever route the email takes, the subject line of the email must never contain PID.

Email addresses ending in @solent.nhs.uk have been assessed as secure for internal use only (@solent.nhs.uk to @solent.nhs.uk), the same guidelines as above apply for the use and transmission of PID within emails.

NHSmail to Solent email addresses are not secure transfers of data.

6.17. Wifi

Any person may use the wireless Internet connection provided from Solent NHS Trust (The Trust) premises providing they have obtained a WiFi User ID and password from the Trust. The service is provided free of charge in accordance with these terms and conditions.

6.18. Social Media

Social media is now the most popular way of communicating and sharing information and advice. Employees should refer to the Trust's Social Media Policy for further information.

6.19. Security of Third Party Access to NHS Networks

Written agreement must be received from all external contractors and non-NHS parties that they agree to treat all information confidentially and that information will not be disclosed to unauthorised individuals. Such contractors should also sign a declaration that they understand the relevant legislation should they need to access sensitive information stored on a computer system.

6.20. Use and Installation Software

Under no circumstances should software, other than that approved and authorised, be loaded onto Solent NHS Trust computers. Employees must not bring or download software onto Solent NHS Trust premises without first getting permission from the IT service desk.

All changes to and installation of software programs may only be undertaken under the direction of the IT service desk.

'Games' Software, except for the purpose of authorised training is not permitted for use on Solent NHS Trust equipment and must not be installed or used on the premises.

Authorised training software includes "games" shipped as part of MS Windows.

Installing and/or purchasing software requires proper validation of licensing agreements and prior written approval from Trust ICT management.

Only Trust-licensed software may be installed on Trust computers.

When installing upgrades, shareware, freeware, or trial software, users must validate the cost and obtain written approval from the Trust ICT management in advance. License agreements must be carefully read and understood prior to accepting and proceeding with installation. Installing or distributing pirated software is unauthorized, including using or purchasing a single user license and loading it on multiple Trust computers.

6.21. Cyber Security

- Suspicious emails
  Suspicious e-mails should not be opened, and should be reported to the CGI Service Desk (0845 605 1334 or email: solentnhsicthelp.uk@cgi.com) immediately.

- Antivirus protection and encryption
  Trust computers must have active anti-virus and PC firewall protection that is regularly updated.
  Trust laptop computers must possess full disc encryption.

- Computer Viruses
  Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses.
  Virus threats are a day-to-day threat however the type, strain, and number of incidents may well increase due to the increased web activity.

  This can cause serious disruption to both the user and the IT Support Teams.

  All Solent NHS Trust computers must run anti-virus software and it is each user's responsibility to check that the anti-virus software is current on their computer. Compliance with this is monitored through the Information Security Group.

  This will ensure that any infected computer media put on Trust computers would be identified and assure that computer media sent to the outside world would be free of viruses.

  Staff must contact the IT service desk if a virus incident is suspected.

- Cyber Security – Trust Security Management Plan
  The Trust Security Management Plan provides a definitive high-level overview of the Information Security Management System developed and operated for Solent NHS Trust (the "Trust") by CGI. The 10 steps to Cyber Security are embedded within the plan. Refer to plan for further information.

- Virus and Malware Controls
  Virus detection and prevention best practice are adhered to and described in CGI's shared service security rules. Corporate awareness activities surrounding anti-virus policy ensure that all staff are kept informed of best practice and their responsibilities. Further mitigation controls includes antivirus software, firewalls and the use of mandatory password-protected screensavers.

Software distribution is protected by Anti-virus software and CGI use content filtering to prevent installation of unauthorised mobile code, and compliance to the Anti-Virus policy is ensured through both daily and weekly monitoring of the installed Anti-Virus systems. McAfee Email Gateway is employed for inappropriate e-mail content and attachment blocking on CGI's corporate networks.

6.22. Data Encryption

The Trust will ensure that an appropriate software encryption package has been implemented.

Situations may arise which require Personal Identifiable Data to be transferred within the NHS, or shared with authorised third parties, on removable media such as writable CD/DVD, memory sticks, or through the use of internet services such as email. The following provides guidance on the proper handling of this data to ensure confidentiality.

6.22.1. **Areas of Risk / Encryption Strategy**

The listing below identifies the risks the Trust may be subjected to and the strategies that will be adopted in order to comply with national mandatory requirements:

- **Emailing personal identifiable/business critical information:** NHSMail has been mandated as the one of the permitted method of emailing personal identifiable data (PID) externally for NHS Organisations. Solent NHS Trust has adopted NHSMail as its secure external email system; both the sender and receiver must have NHSMail accounts or similar Government approved encrypted mail systems.

  Staff can obtain an NHSMail account through Solent NHS Trust's ICT provider.

- **Laptops** are the most common form of mobile device holding mobile data. A laptop that does not have any form of encryption can allow unauthorised access to the data contained on it, and, so, must be protected.

  All Trust laptops must be encrypted with BitLocker full disk encryption with AES encryption algorithm and a 256-bit key is used.

  Laptops are encrypted by Solent NHS Trust's ICT provider, prior to being distributed to staff.

- **USB memory sticks and USB connected hard drives or similar**; these drives have the potential to store large quantities of data and therefore will need to be fully encrypted using hardware / device encryption and a justified case made for their use.

  All laptops and desktops are equipped with Port Lockdown. This means that if an individual wishes to download something onto a portable devise, they will be asked to encrypt the devise with BitLocker full disk encryption with AES encryption algorithm and a 256-bit key

- **Desktop PCs** should be risk assessed and those identified at risk must be encrypted with full disk encryption. It is Trust policy that data should not be stored on the local hard drive so it would only be desktops which have a valid business reason to store data locally and are in vulnerable locations that would require encrypting.

All Trust desktops must be encrypted with BitLocker full disk encryption with AES encryption algorithm and a 256-bit key is used.

Desktops are encrypted by Solent NHS Trust's ICT provider, prior to being distributed to staff.

- **Other mobile devices** including PDA's, smart phones, CD, iPhones, iPad, DVD's, etc… The loss of any of these devices containing sensitive data would compromise the Trust's information security if there was not robust encryption in place. It is the user's responsibility to make sure that these devices are encrypted and used within the scope of this policy.

  Smartphones: Solent NHS Trust's ICT provides Airwatch on all Solent NHS Trust devices, which enables remote wipe, should a device become lost.

  CD & DVD's: Only if there is an approved business reason to put PID onto CD or DVD should this media of data transfer be used.

  Other removable devices: These may be added on an ongoing basis if it is deemed that there is a potential need for data to be downloaded to these. However, these will be fully encrypted in line with this policy. All authorisations for reading and writing to any other mobile devices must be granted by the user's manager. In cases involving high volumes of data, a Risk Assessment may be required.

  All mobile devices classified within the scope of this policy must be encrypted to the national standard to prevent the possible loss of any Trust data.

  Only Trust owned authorised mobile devices may be used.

Departments using such devices will remain responsible for the safekeeping and recovery in the event of staff leaving the organisation as with any other piece of Trust equipment

6.22.2. **Guidance**

- The minimum encryption standard for transferring sensitive data across the N3 (**N3** is the national broadband network for the National Health Service (NHS), connecting all NHS locations and 1.3 million employees across England) Wide Area Network is 112 bit **Triple DES** is the common name for the **Triple Data Encryption Algorithm**.

- This standard is available when using applications such as **Pretty Good Privacy** (**PGP**) which is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communicationor WinZIP (used to compress large files) version 9 or later. With these products the data can be put into a Self Decrypting Archive (SDA), as the software that created the archive does not need to be installed on the recipient's computer.

- The passphrase for the archive must be of an appropriate length and complexity, that is to say, a **minimum** of **25 characters** which comprise alphanumeric, upper case characters, and punctuation.

- The information must of course be encrypted and be in the form of:
  - A 'Self Decrypting Archive' (SDA) attached to an email, providing the passphrase is forwarded to the recipient by alternate means separately from the SDA, such that the SDA and passphrase cannot be associated.
  - An SDA on CD, DVD or other removable media containing the data is delivered to or collected by a representative from the organisations involved. An email (or other communication entirely separate from the SDA) providing the passphrase is sent to the recipient.

- If the SDA is sent by non-electronic means, check that the removable media has been safely received by the recipient.

7. INFORMATION GOVERNANCE RISK MANAGEMENT

7.1. Solent NHS Trust will be vigilant in the protection of all personal data whose release or loss could cause harm or distress to individuals.

7.2. Solent NHS Trust will identify, risk assess and manage appropriately data they or any third party contractor hold whose release or loss could cause harm or distress to individuals. It will handle all such information as if it were at least "PROTECTED – PERSONAL DATA" while it is held, processed or stored within this organisation or that of its partners, applying the measures outlined within this policy.

7.3. Information Governance Risk assessments will be undertaken for all Solent NHS Trust Clinical and Corporate critical information systems and critical information assets. Information Governance Risk /Data Protection Impact Assessments will occur at the following times:

- Quarterly for the review of information risk , and annual reports to the SIRO from the IAO's are undertaken to support the SIRO's written advice on the Statement of Internal Control to the Chief Executive – strategy for delivery (IAO's annual report)
- At the inception of new systems, applications, facilities, changes to process etc. that may impact the assurance of Solent NHS Trust Information or Information Systems Data Privacy Impact Assessments (DPIA's) will be completed. These DPIA's will be brought with supporting documentation to the Information Communication Technology Group for consideration and review.
- Ideally DPIA's should be completed before enhancements, upgrades, and conversions associated with critical systems or applications.
- When NHS policy or legislation requires risk determination
- When the Solent NHS Trust organisation Management team / Board requires it

7.4. Information Governance incident reporting will follow the same processes embedded within the organisations overall risk management approach and suite of Policies.

7.5. All IG incidents will be reviewed and scored in accordance with NHS Digital's; "Guide to the Notification of Data Security and Protection Incidents" https://www.DSPToolkit.nhs.uk/Help/Attachment/148

7.6. Depending on the outcome of the review, an incident will either be identified as a local incident, a High Risk Incident or a Serious Incident. The IG incident level will determine the type of incident investigation that should take place and who should be involved and/or

notified. Solent NHS Trust's Executive Team is also briefed on a weekly basis of the status of High Risk Incidents and Serious Incidents.

Local Investigation.
The following will be involved in the incident investigation;
- Reporter
- IG Team
- Governance Lead/ Professional Standards Lead
- Information Asset Custodian (if required)

The following will be informed of the incidents after the investigation;
- Information Asset Owner (Monthly incident reports)
- Senior Information Risk Owner (Annual Report)

High Risk Incident (HRI) Investigation
The following will be involved in the incident investigation;
- Reporter
- IG Team
- Governance Lead/ Professional Standards Lead
- Information Asset Custodian (if required)
- Information Asset Owner

The following will be informed of the incident and advise may be sought from;
- Caldicott Guardian
- SIRO

Serious Incidents (SI)
The following will be involved in the incident investigation;
- Reporter
- IG Team
- Governance Lead/ Professional Standards Lead
- Information Asset Custodian (if required)
- Information Asset Owner
- Associate Director
- Caldicott Guardian
- SIRO

The following will be informed of the incident and advise may be sought from;
- CEO

The incident will be reported, using the DSPT Online Toolkit and consequently the following will be notified of the incident and a formal report will need to be shared with;
- The Information Commissioners Office
- NHS Digital
- Commissioners

7.7. High Risk Incident – formal and informal investigations

All IG incidents within Solent NHS Trust meeting the High Risk category in accordance with NHS Digital's guidance for scoring IG incidents are to be measured against a checklist to determine if a formal or informal investigation will be carried out. It has been agreed that;

- Formal investigations of High Risk or Serious IG incidents will be presented individually to

SI panel.

- Informal investigations of High Risk IG incidents will be collated and presented by the IG team within one report to SI panel

It may be agreed and determined at the incident review meeting that no additional learning will be identified as a result of a formal investigation, due to a number of factors, e.g. the incident was the result of an unintentional human error, the incident was a result of failure to follow process, this is an isolated event specific to a service and all actions were taken immediately, etc….. Under these circumstances no formal investigation report will be required to be undertaken by services. The IG team will monitor these incidents within a consolidated report to SI panel to highlight incidents ensuring awareness of data breaches and allow preventative work to be undertaken within the Trust.

7.8. Serious Incident – Notification: As soon as Solent NHS Trust becomes aware that a personal data breach has occurred, the Information Governance Team will notify the personal data breach to the ICO without undue delay and, where feasible, not later than 72 hours of the Trust having become aware of it, unless able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of Data Subjects. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Solent NHS Trust are required to report IG incidents via the DSPT (notifying the ICO) within 72 hours once notified of an incident (within this time are view meeting must take place to determine if the category meets a level 2 or above)

Solent NHS Trust's should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the Data Subject in order to allow him or her to take the necessary precautions. Solent NHS Trust's Duty of Candour procedures should be followed when notifying individuals of personal data breaches.

7.9. Human Resources – Disciplinary Process: If an IG breach should lead to a member of staff being investigated through the Disciplinary Process, the Data Protection Officer / Head of Information Governance and Security (or appointed delegate) should be consulted with as a professional advisor as necessary during the investigation process. The Data Protection Officer / Head of Information Governance and Security will consult with the Senior Information Risk Owner (SIRO) and/or Caldicott Guardian, as accountable officers for IG Breaches. The SIRO and Caldicott Guardian must always be notified of the outcome summary of the disciplinary e.g. no action, verbal warning, official warning, retraining, etc… so that the Information Commissioners Office can be advised, as this is a requirement of their investigation process.

7.10. Transparency about Information Risk: Solent NHS Trust promotes transparency about its information governance risks, incidents and lessons learned and publishes information setting out how it handles information and a summary material on Information Risk issues in the Trusts Annual Governance Statement, within its Annual Report.

7.11. Lessons learnt: Any teams/ services where Information Governance incidents occur will receive advice and where required bespoke Information Governance Training to avoid repetition. These lessons will then be cascaded within Information Governance communications to all staff to enable Trust wide learning.

8. DATA PROTECTION IMPACT ASSESSMENTS

8.1. It is now a legal requirement that a Data Protection Impact Assessment (DPIA) / Privacy Impact Assessment (PIA) is undertaken, where any of the following are applicable and are linked to the use of Personally Identifiable Data (this is not an exhausted list)

- ☐ New project involving the use of Personally Identifiable Data
- ☐ New system / technology
- ☐ Collection of new information about Data Subjects
- ☐ Transfer of Service – involving transfer of data
- ☐ Information Sharing – not under a contract
- ☐ Data Sharing – under a contract
- ☐ Using Data Subjects information for something other than the purpose it was collected for
- ☐ Processing data in a way that would likely to raise privacy concerns or expectations
- ☐ Processing data in a way that would require contacting Data Subjects in ways they may find intrusive
- ☐ Any other reason a PIA would need to be undertaken (where personally identifiable data is affected)

8.2. The purpose of these assessments is to ensure, compliance with legal requirements, to ensure that there is a legal basis for what is proposed and that any risks to privacy are addressed at the development stage.

8.3. The aim of this procedure is to ensure that all new, changes or renewal of projects, processes, contracts, that uses of effects PID are done so in a structured way, legal basis are identified and all risks are mitigated.

8.4. This process will ensure that the Trust complies with GDPR 2016;

- Principle 1 – *"Lawfulness, fairness and transparency"*
- Principle 2 – *"Purpose limitation"*

8.5. Process for completion

8.5.1. A DPIA / PIA must be completed for all scenarios, identified in section 8.1 of this policy and for any other situation where personally identifiable data is affected)

8.5.2. A DPIA / PIA must be undertaken at the start of projects, processes, contracts, that uses of effects Personally Identifiable Data or as soon as it becomes evident that one needs to be undertaken. This can be for anything new, changes or renewal (if not previously undertaken).

8.5.3. These should be carried out by the Data Controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with law.

8.5.4. At the point a DPIA / PIA is identified as being required, the project lead or service manager, should contact the Information Governance Team immediately (0300 123 3919 or

InformationGovernanceTeam@Solent.nhs.uk). At this point a relevant member of the Information Governance Team (normally the Data Protection Officer or Assistant Data Protection Officer) will arrange to meet with all key / relevant parties to under the DPIA / PIA immediately, ensuring that all questions are completed correctly and any unforeseen queries are addressed.

8.5.5. It is important to inform the Information Governance Team at the earliest opportunity, this prevents a situation where the Information Governance Team is asked to approve a new process at the last minute which may result in potential delays because appropriate areas have not been considered.

8.6. Approval Process

8.6.1. Once a DPIA / PIA has completed the following approval process will be followed;

8.6.2. The Trust's Data Protection Officer will review the DPIA / PIA and assess if they are happy to approve the assessment or make recommendations to the Trust if not fully supported; ensuring all risks have been assessed and mitigations put in place

8.6.3. DPIA / PIA's will then be required to be supported by the relevant Information Asset Owner (IAO).

8.6.4. Once the above has taken place, the next approval is dependent on the reason the DPIA / PIA was required;

- Service Line Governance Groups
  - Transfer of Service – involving transfer of data
  - Information Sharing – not under a contract

- ICT Committee
  - New project involving the use of Personally Identifiable Data
  - New system / technology
  - Collection of new information about Data Subjects
  - Using Data Subjects information for something other than the purpose it was collected for
  - Processing data in a way that would likely to raise privacy concerns or expectations
  - Processing data in a way that would require contacting Data Subjects in ways they may find intrusive
  - Any other reason a PIA would need to be undertaken (where personally identifiable data is affected)

- Commercial Group, Finance & Commercial Group or Finance Committee (depending on contract value).
  - Data Sharing – under a contract

8.6.5. The final stage of the approval process is for the Senior Information Risk Owner and Caldicott Guardian to advise if they are happy to approve the DPIA / PIA

8.6.6. **Please Note:** After each approval the DPIA / PIA is to be returned to the Information Governance Team, with the appropriate approval / comments (all comments are to be noted on the DPIA / PIA). The Information Governance Team will manage the approval process

8.6.7. Once fully approved, the relevant project lead / senior manager and IAO will be advised.

8.6.8. The Information Governance Team will keep a central list of all DPIA's / PIA's that have been approved and will periodically publish these on the Trust's public Intranet page, as part of having "Greater transparency about processing", as required under Data Protection legislation.

8.6.9. Solent NHS Trust will undertake and publish DPIA's as part of its information governance risk management programme for all new projects, systems and research proposals.

8.7. Information Commissioners Approval Process

8.7.1. From the 25th May 2018, if the outcome of an assessment is deemed high risk, then the DPIA / PIA should be presented to the Information Commissioners Officer (ICO) for sign off and the ICO will respond within 8 – 14 weeks.

8.7.2. The above, must be factored into any project's timescales.

9. ROLES & RESPONSIBILITIES

9.1. The Chief Executive (Accountable Officer)

The Chief Executive has overall responsibility for Data Protection and Confidentiality within the Organisation. An accountable officer is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Chief Executive has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

The Chief Executive duties are to ensure:

- staff are aware of the need to comply with Data Protection legislation, in particular with the rights of patients wishing to access personal information and or their health records.
- staff are aware of requirements of the common law duty of confidence as set out in Confidentiality: NHS Code of Practice.
- arrangements with third parties who process personal data on behalf of the Trust are subject to a written contract which stipulates appropriate security and confidentiality.
- Local Research Ethics Committees and researchers are aware of the Data Protection Act and how it applies to the use of data for research purposes.

9.2. Senior Information Risk Owner (SIRO) – Chief Operating Officer, Southampton & County-wide

The SIRO has overall ownership of organisational information risk and acts as champion for information risk on the Board; providing written advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk.

The SIRO will ensure that they are familiar with information risks and the approach taken within Solent NHS Trust, to ensure the organisation can provide the necessary mitigation and support to the Board and in so doing to the Accountable Officer.

The SIRO will with assistance from the other directors nominate Information Asset Owners (IAO's) at an appropriate senior level to be ascribed to Information Assets.

9.3. Caldicott Guardian – Medical Director

The Caldicott Guardian is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of patient-identifiable information across the Trust and supporting agencies. To assist with the volume and diversity of this task the Caldicott Guardian is supported by the Information Governance Team, Information Asset Owners and Information Asset Custodians.

9.4. Data Protection Officer (DPO) – Head of Information Governance and Information Security

The Data Protection Officer is part of the Information Governance Team. The Data Protection Officer has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance throughout the Trust with Data Protection Legislation.

The DPO has these tasks:

- To promote awareness of the Act and Procedures contained in this policy
- To be responsible for compliance with the Act and the six data protection principles.
- To ensure Trust compliance of Notification requirements with the Information Commissioner's Office
- To monitor changes to working practices, and where any such changes are found to come within the remit of the Act, to take appropriate action
- Liaise with the Information Commissioner's Office
- Be the first point of contact within the organisation for data protection and Caldicott issues
- Advise and update the Trust in relation to directives/guidance from the
- Information Commissioner and the Department of Health
- Via the Information Governance Framework – ensure that the Caldicott Guardian and Senior Information Risk Owner (SIRO) are informed of relevant issues and decisions are recorded
- Developing and enforcing detailed procedures to maintain security.
- Ensuring compliance with relevant legislation.
- Monitoring for actual or potential information security breaches.
- Ensuring that the Trust's personnel are aware of their responsibilities and accountability for information security
- Provide effective training for all staff in the requirements of Data Protection legislation and the Caldicott principles
- To liaise closely with the Information Asset Custodians and the Information Asset Owners.
- Carry out Data Protection and Caldicott compliance checks in departments, as required
- To help maintain the organisations Data Protection inventory by recording all service/local changes to the systems (both computerised and manual) inventory.
- Oversee applications for Subject Access and maintain appropriate files.

9.5. Information Asset Owners (IAO)

The Information Asset Owner (IAO) is a senior member of staff who is the owner for one or more identified information assets of the organisation.

There are several IAOs within the organisation, whose departmental roles may differ. IAOs will work closely with other IAOs of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. IAOs will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

IAO's will take appropriate actions to:

- Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Ensure that information risk assessments are performed quarterly on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency
- Ensure that Information Governance security accreditation is maintained by undertaking at least yearly reviews of the system level security policy for critical systems owned
- IAO's shall submit the risk assessment results and associated mitigation plans to the IG team for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks
- IAO's shall complete an overarching annual report to the SIRO
- IAO's shall be responsible for developing a Business Continuity Plan for their assets which shall be reviewed on an annual basis

9.6. Information Asset Custodians (IAC)

Information Asset Custodians, identified within each department of the organisation, are responsible for ensuring that the Data Protection and Caldicott principles are fully observed and complied with by staff within their department. They are required to ensure that all data flows and processing of data complies with all current Data Protection policies, working closely with Information Governance Team as appropriate.

Their tasks are to:

- Promote Data Protection & Caldicott Principles on an on-going basis, including posters, articles and local briefings
- Promote local induction and ensure that all new starters, before they access any information system, are given instruction on the Data Protection Act and Caldicott, as part of their first day/week induction programme.
- Ensure that all staff are aware of the Information Asset Custodian for their area and the contact details for the Information Governance Team
- Ensure that all staff know the procedure for reporting security incidents
- Ensure applications for access to systems within the department are processed following the agreed procedures and with appropriate authorisation
- Have systems in place to enable the above to be managed effectively within the service.
- Maintain close liaison with the Information Governance Team regarding any changes within the department

9.7. IG Team

Senior IG Officers and Senior Records Officers will be required to obtain and maintain expert and specialist knowledge of Information Governance, Data Protection and Information Security requirements. They will, alongside the DPO, be required to implement and support staff within the Trust to ensure compliance is maintained at all times and where issues or risks arise identify solutions to resolve / minimise the risk / impact.

9.8. ICT Provider

Solent NHS Trust's ICT provider will be responsible for:

- The implementation of encryption on all Trust Laptop's and approved mobile data devices, including the facility for content encryption and the training in its use;
- The support and maintenance of this system via the ICT helpdesk function;
- Managing changes to the configuration of the service.

9.9. All Staff and other individuals covered by this policy

Everyone has a role to play in the effective management of information governance and data protection. All staff will participate in the mandated annual Information Governance training in compliance with the training needs assessment matrix and actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate mitigating actions under advisement of the Information governance team.

Everyone is responsible to ensuring that they abide by legal obligations and report non-compliance immediately.

10. TRAINING

10.1. All Trust staff will be made aware of their responsibilities regards Data Protection, through their annual Information Governance Training.

10.2. It is the responsibility of the Information Governance Team to produce the training tool

10.3. Compliance with this training requirement will be monitored by the Learning & Development Team in conjunction with the Information Governance Team via a reporting mechanism learning and development training tool.

11. EQUALITY IMPACT ASSESSMENT AND MENTAL CAPACITY

11.1. A thorough and systematic assessment of this policy has been undertaken in accordance with the Trust's Policy on Equality and Human Rights.

11.2. The assessment found that the implementation of and compliance with this policy has no impact on any Trust employee on the grounds of age, disability, gender, race, faith, or sexual orientation. See Appendix A

12. SUCCESS CRITERIA / MONITORING EFFECTIVENESS

12.1. Data Security & Protection Toolkit:

The monitoring of this policy and its effectiveness and maintenance will be audited annually using the DSPT or sooner if new legislation, codes of practice or national standards are introduced. The DSPT it is a self assessment audit undertaken by the Information Governance Team. In addition to this the DSPT is audited annually by the Trust's Internal Auditors.

The owner/author of the policy is responsible for undertaking this audit and ensuring the policy's effectiveness. This will be monitored through the ICT Group to ensure effectiveness.

The implementation of this policy will be audited annually by the Information Governance Team who will also perform spot check audits to assess compliance.

Service Managers and Information Asset Custodians will work with the Information Governance Team to develop local action plans and monitor their completion. Service

Managers and Information Asset Custodians will elevate risks identified through the Risk Register system.

The Information Governance Team will on a weekly basis review and monitor all Information Governance incidents and were required conduct full investigations.

The Toolkit is reported to the Trust's Board every four months and the SIRO and the DPO sign off the final submission of the Toolkit.

12.2. Audits:

The Trust reserves the right to monitor the activity of individuals in relation to the use of PID/business critical information on all Trust equipment both static and mobile.

Spot checks will be conducted by the Information Governance Team as a result of one or more of the following;

- Service has been highlighted as a concern by a member of the public or a member of staff within the organisation
- Service has reported Serious Incident
- Service has reported a high number of IG incidents
- Review as a result of concerns raised, following a previous spot-check audit. This will be conducted within three months of the original audit to review changes in practice.
- Selected at random

Reports following each spot check are required to be signed off by services IAO, the SIRO and Caldicott Guardian.

12.3. Non-Compliance:

Failure by any employee of Solent NHS Trust to adhere to the policy and its guidelines will be viewed as a serious matter and may result in disciplinary action.

Where employees believe that it is not possible to uphold the policy and associated guidelines they must bring this to the attention of the Data Protection Officer and Head of Information Governance & Security

13. REVIEW

13.1. This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

Appendix A: Equality Impact Assessment

Step 1 – Scoping; identify the policies aims	**Answer**		
1. What are the main aims and objectives of the document?	To outline the process for complying with Data Protection Legislation		
2. Who will be affected by it?	All staff and third parties working with Solent NHS Trust		
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	DSPT compliance Compliance with legal requirements		
4. What information do you already have on the equality impact of this document?	None		
5. Are there demographic changes or trends locally to be considered?	None		
6. What other information do you need?	N/A		
Step 2 - Assessing the Impact; consider the data and research	**Yes**	**No**	**Answer** (Evidence)
1. Could the document unlawfully discriminate against any group?		X	
2. Can any group benefit or be excluded?		X	
3. Can any group be denied fair & equal access to or treatment as a result of this document?		X	
4. Can this actively promote good relations with and between different groups?		X	
5. Have you carried out any consultation internally/externally with relevant individual groups?	X		Current Policy Steering Group members consulted and wider groups represented by PSG members..
6. Have you used a variety of different methods of consultation/involvement	X		Via email and face to face meetings
Mental Capacity Act implications			
7. Will this document require a decision to be made by or about a service user? (Refer to the Mental Capacity Act document for further information)		X	
External considerations			
8. What external factors have been considered in the development of this policy?	X		Data Protection Legislation
9. Are there any external implications in relation to this policy?	X		Non-compliance with Data Protection Laws – fines
10. Which external groups may be affected positively or adversely as a consequence of this policy being implemented?		X	N/A

Appendix B: Guidance for sharing personal information

Transferring PID Leaflet:
http://intranet.solent.nhs.uk/TeamCentre/InformationGovernance/TeamDocument/Forms/Guidance%20%20leaflets.aspx

Appendix C: Staff Checklist

This checklist is intended to be a helpful Information Security aide-memoir for employees. It is not intended to be a comprehensive summary of user responsibilities and does not reduce or alter the standards or principles outlined in this policy.

Employees should:

- Contact the Information Governance Team if you are aware that you are not meeting the standards and principles of this policy.
- Be aware of the potential risks that surround the data and systems you use. For example, is the information secure from accidental disclosure? Is it appropriate to those who need to know? Can amendments and additions be traced to the person making changes? Consider the security measures that you currently use in relation to these risks.
- Not store personally identifiable information outside of the network as this is considered an unacceptable risk. Under Data Protection legislation the Trust is obliged to ensure that personal information remains secure at all times
- Store all sensitive information on central file servers and not on personal computers or local devices if the facility is available
- Inform your manager should a legitimate need arise for local storage or transfer of confidential information so that a risk assessment is undertaken by the Information Asset Owner / Custodian and the justification approved under the Caldicott principles and agreed by your line manager. This agreement must be documented and submitted to the Data Protection Officer and Head of Information Governance and Security for consideration of risks
- Ensure any bulk extracts of confidential or sensitive data are authorised by the responsible Director for the work area.
- Ensure that whatever standalone device is used to store PID (desktop computer, portable device or removable media), then these must be installed with encryption prior to use
- Safeguard portable IT equipment. Do not leave them visible and unprotected in public places. Portable hardware must be installed with encryption where available otherwise password protection. Please contact the IT service desk.
- Dispose of any confidential data, on printouts or computer media, securely
- Follow the Clear Screen Policy;
  When moving away from your desk, you must ensure you lock your PC, by holding *'Ctrl' + 'Alt' down and pressing the 'Delete'* key. Then select *'Lock Computer'.* You may be working on a confidential piece of work and by locking your screen, it ensures that no-one else will be able to read or access any other files on your PC in your absence.
- Follow the Clear Desk Policy
  Any confidential information must be placed out of sight, in locked cabinets when not in use. This includes any portable computers that may contain confidential information. When moving away from your desk ensure you do not leave person identifiable / sensitive information available for others to view, put it in a drawer or cover it up.
- Use email professionally. As if writing on the Solent NHS Trust own letterhead
- Use NHSmail if you are sending or receiving PID or sensitive or confidential information externally.
- Be aware of other Solent NHS Trust related policies
- Wear your staff identification badge at all times
- Ensure they have read and understood the guidance for sharing personal information contained in Appendix A. Any queries should be directed to your Manager or the Corporate Services Team.

Employees should not:

- Move any non-portable IT equipment without prior Local management approval
- Use e-mail for clinical or confidential information (unless approved secure email route) – refer to secure email grid above.
- Share passwords or use someone else's credentials
- Hold personal data on your own system without understanding the Data Protection Act and Principles and confirming that there is sufficient physical security in place (e.g. lockable doors, approved encryption)
- Copy personal data from one system to another without confirming that the recipient system has the same or greater security protection
- Use or try to use IT networks which you have not been authorised to use
- Install or make copies of ANY software. ICT Services should be consulted. Copying software must be done with the authority of the copyright holder.

Appendix D: Card Payments

1. The Trust handles cardholder information daily. Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

2. The Trust commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

3. Employees handling cardholder data should ensure:
   - Handle Company and cardholder information in a manner that fits with their sensitivity and classification;
   - The Trust reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
   - Do not disclose personnel information unless authorised;
   - Protect cardholder information;

4. All cardholder data stored and handled by the Trust and its employees must be securely protected against unauthorised use at all times. Any card data that is no longer required for business reasons must be discarded in a secure and irrecoverable manner.

5. If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.

6. PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

7. It is strictly prohibited to store:
   - The contents of the payment card magnetic stripe (track data) on any media whatsoever.
   - The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
   - The PIN or the encrypted PIN Block under any circumstance.

8. All Access to cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.
   - Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
   - Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
   - No other employees should have access to this confidential data unless they have a genuine business need.
   - If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix C.
   - The Company will have a process in place to monitor the PCI DSS compliance status of the Service provider.

9. All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.
   - Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.

- If there is a business justification to send cardholder data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10.Credit Card (PCI) Security Incident Response Plan

- If a breach of information security policy was to occur, the Trust's IG Risk Policy is to be followed
- In response to a systems compromise, The Trust's Data Protection Officer and the Information Communication Technology Team will:
  - Ensure compromised system/s is isolated on/from the network.
  - Gather, review and analyse the logs and related information from various central and local safeguards and security controls
  - Conduct appropriate forensic analysis of compromised system.
  - Contact internal and external departments and entities as appropriate.
  - Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
  - Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.
- The credit card companies have individually specific requirements that must be addressed in reporting suspected or confirmed breaches of cardholder data. See below for these requirements.
  - **VISA Steps:** If the data security compromise involves credit card account numbers, implement the following procedure:
    - Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
    - Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
    - Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
  - **MasterCard Steps:**
    - Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team.
    - Provide a detailed written statement of fact about the account compromised (including the contributing circumstances)
    - Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
    - Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
    - Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
    - Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
    - Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of

MasterCard.

- **Discover Card Steps**
  - Within 24 hours of an account compromise event, notify Discover Fraud Prevention
  - Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
  - Prepare a list of all known compromised account numbers
  - Obtain additional specific requirements from Discover Card
- **American Express Steps**
  - Within 24 hours of an account compromise event, notify American Express Merchant Services
  - Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
  - Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express