

Appendix A

Data Protection Impact Assessment (DPIA) Screening Questions

The below screening questions should be used to inform whether a DPIA is necessary. This is not an exhaustive list therefore in the event of uncertainty, completion of a DPIA is recommended.

Title	Facebook Page for Bank Staff.
Brief description	Staff to join the Facebook page to provide updates on shift information

Screening completed by

Name	
Title	FWT/E Rostering Team leader
Department	FWT/E-Rostering Team
Email	
Review date	

Marking any of these questions is an indication that a DPIA is required:

Screening Questions		Tick
1	Will the project involve the collection of new identifiable or potentially identifiable information about individuals?	Y
2	Will the project compel individuals to provide information about themselves or involve the processing of personal data not obtained directly from the individual? i.e. where they will have little awareness or choice or it is impossible or would involve disproportionate effort to inform the individuals that the processing is taking place.	N
3	Will identifiable information about individuals be shared with other organisations or people who have not previously had routine access to the information?	N
4	Are you using information about individuals for a purpose it is not currently used for or in a new way? i.e. using data collected to provide care for an evaluation of service development; data matching from multiple sources.	N
5	Where information about individuals is being used, would this be likely to raise privacy concerns or expectations? i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress.	N
6	Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	N
7	Will the project result in you making decisions in ways which can have a significant impact on individuals? i.e. will it affect the care a person receives.	N
8	Does the project involve you using new technology which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition, artificial intelligence or automated decision making.	Y
9.	Is a service being transferred to a new supplier (re-contracted) and the end of an existing contract or the processing of identifiable/potentially identifiable data being moved to a new organisation (but with same staff and processes)	N
10.	Will the project involve systematic monitoring of a publicly accessible area on a large scale? i.e. use of CCTV.	N
11.	Will the project involve the targeting of children or other vulnerable individuals i.e. for marketing purposes, profiling or other automated decision making?	N

Please retain a copy of this questionnaire within your project/system documentation.

Section A: New/Change of System/Project General Details

Name of system/project/process:	Facebook Closed Group for Bank Staff	
Objective:	To have an alternative way to communicate with staff about bank shift availability. The closed group will only accept joining requests from active bank staff.	
Background: <small>Why is the new system / change in system required? Is there an approved business case?</small>	Proactive approach to bank staff – providing more ways to communicate with them. Staff are currently notified of available shifts via email from the FWT.	
Benefits:	Able to communicate at all times. Makes the bank staff feel inclusive within the Trust.	
Constraints:		
Relationships: <small>(for example, with other Trust's, organisations)</small>	None	
Quality expectations:		
Expected "go-live" date.	July 2019	
Cross reference to other projects:	None	
Project Manager:	Name:	
	Title:	
	Department:	
	Telephone:	
	Email	
Information Asset Owner: <small>(All systems/assets must have an Information Asset Owner (IAO).</small>	Name:	
	Title:	H R Business Partner
	Department:	Workforce and OD
	Telephone:	
	Email	
Information Asset Administrator: <small>(It is necessary that there is a deputy in place for when the IAO is absent from the workplace for whatever reason)</small>	Name:	
	Title:	FWT/E-Rostering Team Leader
	Department:	FWT
	Telephone:	
	Email	
Customers and stakeholders:		

Section B Data Protection Impact Assessment Key Questions

Question	Response
Data Items	
<p>1. Will the system/project/process (will now be referred to thereafter as 'asset') contain Personal Confidential Data or Sensitive Data?</p> <p style="color: blue; font-size: small;">If answered 'No' you do not need to complete any further information as DPIA is not required.</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If yes, who will this data relate to:</p> <p><input type="checkbox"/> Patient</p> <p><input checked="" type="checkbox"/> Staff</p> <p><input type="checkbox"/> Other (specify)</p>
<p>2. Please state purpose for the collection of the data:</p> <p style="color: blue; font-size: small;">for example, patient treatment, health administration, research, audit, staff administration</p>	<p>The data will not be collated, it is what is visible on Facebook and this is set by the individual's privacy settings. The FWT team will not be accessing profiles, it is only to be used as an Information/communication tool</p>
<p>3. Please tick the data items that are held in the system</p> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 20px;"> <div style="text-align: center;"> <p>Personal</p> </div> <div style="width: 80%;"> <p><input checked="" type="checkbox"/> Name <input type="checkbox"/> Address</p> <p><input type="checkbox"/> Post Code <input type="checkbox"/> Date of Birth</p> <p><input type="checkbox"/> GP <input type="checkbox"/> Consultant</p> <p><input type="checkbox"/> Next of Kin <input type="checkbox"/> Hospital (District) No.</p> <p><input type="checkbox"/> Sex <input type="checkbox"/> NHS Number</p> <p><input type="checkbox"/> National Insurance No. <input type="checkbox"/> Online identifier (e.g. IP address)</p> </div> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 20px;"> <div style="text-align: center;"> <p>Special Category</p> </div> <div style="width: 80%;"> <p><input type="checkbox"/> Health data <input type="checkbox"/> Sex life and sexual orientation</p> <p><input type="checkbox"/> Political opinions <input type="checkbox"/> Religion</p> <p><input type="checkbox"/> Biometric data <input type="checkbox"/> Racial or ethnic Origin</p> <p><input type="checkbox"/> Genetic data <input type="checkbox"/> Trade Union membership</p> </div> </div> <p style="margin-top: 20px;">Other (please state here):</p>	
<p>4. Will the asset collect new personal data items which have not been collected before?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>If yes, please give details:</p>
<p>5. What checks have been made regarding the adequacy,</p>	<p>As the Facebook group is a closed group we need to identify that the individual works for the Trust and is a member of bank. We</p>

<p>relevance and necessity for the collection of personal and/or sensitive data for this asset?</p>	<p>wished to ask 3 questions to give them access to the Bank Facebook page:</p> <p>What is your employee number OR</p> <p>Work email address</p> <p>(What Units have you worked on) – Not essential to verify, so suggest removal of this.</p> <p>These questions will be asked as part of the joining request. Facebook has the capability of asking questions at the point of making the joining request. The staff member will provide the information via the Facebook joining request and it will be sent to the FWT on the Facebook notification.</p> <p>This information will not be retained by the FWT. The information will be received via the joining request, verified by the FWT against Allocate (Health Roster) and the group joining request will be accepted or declined appropriately.</p> <p>AMENDMENT approved by IG Group 09/04/20 – The staff member is asked to provide EITHER employee number OR work email address in order to verify their identity in order to minimise the personal data shared through Facebook.</p>
<p>6. How will the information be kept up to date and checked for accuracy and completeness?</p>	<p>The individual staff member updates their own profile. The Trust Facebook group for bank staff will be updated by the FWT but does not contain personal data</p>
<p>Data processing</p>	
<p>7. Will a third party be processing the data?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>The three questions to verify a person’s identity will shared via Facebook.</p>
<p>8. Is the third party contract/supplier of the system on the Register of Fee Payers with the Information Commissioner? What is their registration number?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Data Protection Act Registration Number: ZA265194</p>
<p>9. Has the third party supplier completed a Data Security and Protection Toolkit?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>If yes, please give assessment status:</p>
<p>10. Does the third party/supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>The staff member when becoming a Facebook member will have agreed to the Facebook T&C’s. This is between the individual and Facebook.</p> <p>Is the contract based on or utilise the NHS Standard Contract?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>

<p>11. Will other third parties (not already identified) have access to the data? (include any external organisations)</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>If so, for what purpose? Please list organisations and by what means of transfer</p>
<p>12. Who provides the information for the asset?</p>	<p><input type="checkbox"/> Patient <input checked="" type="checkbox"/> Staff</p> <p><input type="checkbox"/> Others – Please specify e.g. Interfaces from PAS</p>
<p>Confidentiality</p>	
<p>13. Please outline how individuals will be informed and kept informed about how their data will be processed. (A copy of the privacy notice/leaflet must be provided)</p>	<p>Minimal personal data will be used. The staff member can leave the Facebook group at any time.</p> <p>No posts can be added from an individual on Facebook unless authorised by FWT. Where a staff member attempts to make a post within the closed group, a notification is sent to the FWT with the option to accept the post or decline the post.</p>
<p>14. Does the asset involve new or changed data collection policies that may be unclear or intrusive?</p> <p>Are all data items clearly defined?</p> <p>Is there a wide range of special category data being included?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>15. Are you relying on individuals (patients/staff) to provide consent for the processing of personal identifiable or sensitive data?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Where consent <i>is</i> being sought:</p> <p>Is the consent explicit?</p> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Where explicit consent is <i>not</i> being sought:</p> <p>a. Will identifiable data only be handled within the patient’s direct care team (in accordance with the Common law duty of confidence)</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>b. Which legal basis/justification is in place to permit this processing (in accordance with Data Protection Act/General Data Protection Regulation)?</p> <p>Article 6</p> <p><input type="checkbox"/> Performance of contract</p> <p><input type="checkbox"/> Legal obligation</p> <p><input type="checkbox"/> Vital interests</p>

	<input type="checkbox"/> Public task <input type="checkbox"/> Legitimate interests (Public bodies cannot rely on this basis for the performance of their tasks as a public authority) Article 9 if special category of data is processed. <input type="checkbox"/> Employment, social security and social protection law <input type="checkbox"/> Vital interests <input type="checkbox"/> Non for profit body <input type="checkbox"/> Data made public by the data subject <input type="checkbox"/> Exercise/defend legal claims <input type="checkbox"/> Substantial public interest <input type="checkbox"/> Provision of health or social care <input type="checkbox"/> Public health <input type="checkbox"/> Archiving/research/statistical
16. If yes, how will that consent be obtained? Please state: Please include a copy of any consent forms	When the staff member sends a request to join the group. New Bank staff are informed that there is a closed Facebook group that is available to staff to join. Emails to Bank Staff make reference to the Facebook group to raise awareness. The FWT have found that word of mouth between bank staff have increased the number of staff requesting to join the closed Facebook group. The FWT may look to inform staff of the closed Facebook group through the strap lines at the bottom of FWT email's.
17. Will the consent cover all the proposed processing and sharing/disclosures	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
18. How will consent and non consent be recorded and respected?	The staff member will be required to request to join the closed group. Only active bank staff members will be accepted into the group. If the staff member does not consent to joining the group, they will not make a request to join the group.
19. What arrangements are in place to process subject access requests?	Personal Data will not be retained by the FWT. Personal data will be shared by the staff member to verify their identity and then deleted by the FWT.
20. Is automated decision making used? If yes, how do you notify the individual? Please also outline what arrangements are available to the enable the individual access and to extract data (in a standard file format) Please detail any profiling that may take place through automated processing.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
21. What procedures are in place	If a joining request is received from a person who is not on the

<p>for the rectifying/blocking of data by individual request or court order?</p>	<p>Active Bank, the joining request will not be accepted. The FWT have a procedure to follow when staff leave the bank. This “termination process” will be updated to include a step to direct the FWT to remove leavers from the closed Facebook group.</p> <p>The staff member can remove themselves from the closed group at any point.</p>
<p>Engagement</p>	
<p>22. Has stakeholder engagement taken place?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>If yes, how have any issues identified by stakeholders been considered?</p> <p>If no, please outline any plans in the near future to seek stakeholder feedback.</p> <p>Staff are informed of the Facebook group by email and word of mouth. Feedback on the group can be provided to the FWT email address.</p>
<p>Data Sharing</p>	
<p>23. Does the project involve any new information sharing between stakeholder organisations?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>If yes, please describe:</p> <p>Please provide a data flow diagram showing how identifiable information would flow.</p>
<p>Data Linkage</p>	
<p>24. Does the asset involve new linkage of personal data with data in other collections, or is there significant changes in data linkages?</p> <p>The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously).</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>If yes, please provide a data flow diagram showing how identifiable information would flow.</p>
<p>Information Security</p>	
<p>25. Who will have access to the data within the system/project?</p>	<p>The FWT Team will have access: Team leader, FWT Co-Ordinators</p>

Please refer to roles/job titles.	
26. How will access to the system be provided?	Access is provided via IT
27. Is there a useable audit trail in place for the asset. For example, to identify who has accessed a record?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
28. Where will the information be kept/stored/accessed?	<input type="checkbox"/> On paper <input type="checkbox"/> On a database saved on a network folder/drive <input checked="" type="checkbox"/> Website <input type="checkbox"/> On a dedicated system saved to the network <input type="checkbox"/> Other – please state below: Facebook – the closed group will be available via the Trust Facebook page. Facebook do acknowledge in their Privacy Policy that they do collect data from the content that is shared on their platform. Therefore, the content of the request to join the Bank Staff closed Facebook group, is considered a message on their platform, the content of which would be retained by Facebook.
29. Where is this information located? Please detail the countries where the servers are located.	Facebook have servers within the US, EEA and other Countries. The Privacy Policy for Facebook advises that it will rely on adequacy decisions for data transfers to certain countries.
30. Please state by which method the information will be transported	<input type="checkbox"/> Fax <input type="checkbox"/> Email <input type="checkbox"/> Via NHS Mail <input checked="" type="checkbox"/> Website <input type="checkbox"/> Via courier <input type="checkbox"/> By hand <input type="checkbox"/> Via post – internal <input type="checkbox"/> Via telephone <input type="checkbox"/> Via post - external <input type="checkbox"/> Other – please state below:
31. Does the asset involve new privacy-enhancing technologies? Encryption; 2 factor authentication, pseudonymisation	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, please give details:
32. Is there a documented System Level Security Policy (SLSP) or process for this project? A SLSP is required for new systems	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Not applicable If yes, please provide a copy.

<p>33. Is there a Security Management Policy and Access Policy in place? Please state policy titles.</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>34. Are there procedures in place to recover data (both electronic /paper) which may be damaged through:</p> <ul style="list-style-type: none"> • Human error • Computer virus • Network failure • Theft • Fire • Flood • Other disaster <p>Please provide policy titles.</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>35. What training and instructions are necessary to ensure that staff know how to operate a new system securely?</p>	<p>IT has provided access to Facebook for the FWT. The Trust Communications Team manages the Trust Facebook Page and has created the closed group for use by the FWT. Staff in the FWT can be guided by the Trust Communications Team.</p>
<p>Privacy and Electronic Communications Regulations</p>	
<p>36. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>If yes, what communications will be sent?</p> <p>Will consent be sought prior to this?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If no, please explain why consent is not being sought first:</p>
<p>37. Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003 (see appendix for definition)</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Records Management</p>	
<p>38. What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management Code of Practice for Health and</p>	<p>No retention required as the FWT will not retain any data provided on the request to join the closed group.</p>

Social Care 2016) and list the retention period for the identifiable project datasets	
39. How will the data be destroyed when it is no longer required?	Not relevant – data will not be stored, please see question 38.
Business Continuity	
40. Is there a contingency plan / backup policy, or business continuity plan in place to manage the effect of an unforeseen event? Please provide a copy.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No The closed Facebook group is an additional means of communicating with bank staff about the availability of bank shifts and any changes within the Active Bank.
Open Data	
41. Will identifiable/potentially identifiable data from the project/system be released as Open Data (placed in to the public domain)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No The joining request will not be in the public domain, it will be transferred from Facebook to FWT to administer the request.
Data Processing Outside of the EEA	
42. Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If yes, where? Facebook have servers within the US, EEA and other Countries. The Privacy Policy for Facebook advises that it will rely on adequacy decisions for data transfers to certain countries.
43. What is the data to be transferred to the non EEA country?	On the joining request, the FWT are requesting staff provide – Employee number, Bases previously worked and work email address.
44. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable The Privacy Policy for Facebook advises that it will rely on adequacy decisions for data transfers to certain countries outside of the EEA and US.
NHS Number Verification Status Organisations should risk assess their own and new systems and processes, and implement appropriate solutions. It is recommendation to ensure all NHS Numbers are verified to support safer patient identification practices. If the answer to any of the below questions is Yes then the system is an applicable system and the NHS Number standard applies	
45. Does the system act as a master index to send patient identifiable data and NHS	No

Numbers to other systems?	
46. Will the system be used to produce hard-copy outputs containing patient identifiable data (this includes patient facing information such as appointment letters)	No
47. Does the system need to transfer information between organisations	No
48. Will the NHS Number ever be required to be stored against patient identifiable data in the system (e.g. for audit purposes)	No
<p>Clinical Safety</p> <p>The organisation must be compliant with the mandated information standards (ISB 0129 and ISB 0160). Appropriate mechanisms should be in place to ensure patient safety during the whole life cycle of a Healthcare IT system which is led by a suitably qualified experienced clinician. The standards are to be followed for all implementations, updates, upgrades, and decommissioning of systems. The standards apply to any Healthcare IT system developed, deployed or used in the trust including those not implemented by IT programmes.</p>	
49. Is the implementation a First of Type or Early Adopter	No
50. Has the supplier safety documentation been reviewed	No
51. Does the implementation have a Clinical Risk Management Plan?	No
52. How will compliance with Data Set Change Notice (DSCN) 18/2009 Patient Safety Risk Management System – Deployment and Use of Health Software be managed.	

Risk Assessment: Detail any risks identified in the DPIA process?

Risk	Measures to reduce/eliminate the risk	Result: Is the risk eliminated, reduced or accepted	Measure approved: Yes/No
Acceptance of Non-Staff Member to join the closed Facebook group.	To ask the questions detailed in question 5 of the DPIA.	The questions asked will allow the applicant to be verified against the Allocate system which holds staff details of the active bank staff. However, the Privacy Policy for Facebook does acknowledge that the company will collect data shared via its platform.	Part – Suggested to ask for only Employee Number or Work Email address to minimise the personal data that we are asking the staff member to share.
Delay in removal of bank staff who are no longer on the Active bank.	Updated FWT “Termination process” to ensure that staff review members of the closed Facebook group as staff leave the Active bank.	Ensure that leavers are removed from the closed Facebook Group in a timely manner.	Yes.

Evaluation

53. Is the DPIA approved? If not, please state the reasons why and the action plan put in place to ensure the DPIA can be approved	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
--	---

Form completed by:

Name	
Title	FWT and E-Rostering Team Leader
Signature	
Date	11.02.2020

Information Governance Team Review

Name	
Title	Information Governance Support Officer
Signature	
Date	11.03.2020

Information Governance Group Approval

Date of IG Group approval	09.04.2020
Any data to be redacted	
Date of publication	16.04.2020

Appendix B – Glossary

Item	Definition
Anonymity	<p>Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.</p>
Authentication Requirements	<p>An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.</p>
Automated Decision Making	<p>Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned.</p>
Data Protection Act 2018	<p>This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The fundamental principles of DPA 2018 specify that personal data must be:</p> <ul style="list-style-type: none"> • processed lawfully, fairly and transparently. • Collected for specified, explicit purposes (purpose limitation) adequate, relevant and limited to what is necessary (data minimisation). • accurate and where necessary kept up to date (accuracy). • Kept in an identifiable form for no longer than is necessary (storage limitation). • Processed in a manner that ensure appropriate security (integrity and

	<p>confidentiality)</p> <p>The Act also requires organisations to be able demonstrate compliance with the principles (accountability).</p>
Direct Marketing	<p>This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing.</p> <p>Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you.</p> <p>Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.</p>
European Economic Area (EEA)	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients casenotes) or in writing, to a particular use of disclosure of information.
General Data Protection Regulation (EU) 2016/679 Principles of Lawful Processing of Personal Identifiable Information	<p>The GDPR requires that data controllers ensure personal data shall be:</p> <ol style="list-style-type: none"> a) processed lawfully, fairly and in a transparent manner in relation to individuals b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

	<p>e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals</p> <p>f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures</p>
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and

	agreements, business continuity plans, software and hardware.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Personal Data	<p>Any information relating to an identifiable natural person (data subject), identified either directly or indirectly by:</p> <p>Name, identification number, location data, online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p>
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Pseudonymity	This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Records Management Code of Practice for health and social care records 2016	<p>Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. This also includes public health functions in Local Authorities and Adult Social Care where their is joint care provided within the NHS.</p> <p>It is based on current legal requirements and professional best practice. The code of practice contains an appendix with retention schedules for a care records, business and corporate records.</p>
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or

	<p>because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.</p>
<p>Senior Information Risk Owner (SIRO)</p>	<p>This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board</p>
<p>Special Category Data</p>	<p>This means personal data revealing:</p> <ul style="list-style-type: none"> A. Concerning health, sex life or sexual orientation B. Racial or ethnic origin C. Political opinions D. Religious or philosophical beliefs E. Trade union membership F. Genetic data G. Biometric data H. Data concerning health I. Data concerning sex life or sexual orientation.