V10 Data Privacy Impact Assessment Procedure

Introduction

A Data Privacy Impact Assessment (DPIA) is “a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. DPIAs help identify privacy risks, foresee problems and bring forward solutions.”

It is a requirement of the Data Protection Act that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

The DPIA will help to ensure that potential problems are identified at an early stage, and by addressing them, will often be simpler and less costly.

Reasons for undertaking a DPIA include:

- To identify privacy risks to individuals.
- To identify privacy and Data Protection compliance liabilities for the Trust.
- To protect the reputation of the Trust.
- To instil public trust and confidence in your change or product.
- To avoid expensive, inadequate “bolt- on” solutions.
- To inform your communications strategy.
- To reduce the likelihood of regulatory action against the Trust

It is essential that all new information systems go through the Information, Communications and Technology (ICT) departments’ change control process and are subject to a Privacy Impact Assessment.

Information systems, that is systems that process person identifiable information, may include but are not limited to:

Computer systems, PC’s, Tablets, PDAs, Servers, Spreadsheets, Databases,
Analysers, Scanners, Imaging systems, Medical Equipment, Diagnostic equipment, Geo-Centric, RFID, Tagging, Tracking,
Paper based filing systems.

Any change to the way Person Identifiable Information is processed or used must be subject to a DPIA or a refresh of the DPIA.

You must log your intention to run an information system change to an existing information system via the ICT helpdesk via ict.servicedesk2@nhs.net

The ICT help desk will respond with a form for you to complete to ensure that as much information as possible can be gathered to allow your change to be evaluated by the Change Control Board.

You must include the completed DPIA when you submit the change control form failure to do so will result in your change being rejected by the board.

You should also include the information flow mapping for your change with the DPIA documentation.

A Data Flow Map is a graphical representation of the data flow.

This should include:

- Incoming and outgoing data.
- Organisations and/or people sending/receiving information.
- Storage for the 'Data at Rest' i.e. system, filing cabinet, encryption used.
- Methods of transfer.

Once the Change has been approved by the CCB the flow mapping information must be transferred into the flow mapping tool.

It is essential that you provide as much information about your proposal on the "Request for Change" form, If the Change Control Board require more information your change is likely to be delayed.

You may have a local change control process for approving day to day changes to your information system(s) but you will still need to conduct a DPIA according to this procedure and submit it to your change control board should an assessment have been found to be necessary.

Copies of DPIA's that have been reviewed locally in your department along with their outcomes must be submitted to the ICT Change Control Board via the ICT helpdesk as these will be required to evidence that the correct procedures have been followed and facilitate audit.

Any risks identified by completing the DPIA must be entered onto the change risk register and if required transferred onto the divisional risk register.

The General Data Protection Regulation (GDPR) requires the Trust to be able to demonstrate via documentation that it is obtaining and processing personal information lawfully.

You may be required to attend a Change Control Board meeting to explain your change should the board feel further information is required.

Scope

This procedure applies to all staff, contractors or volunteers working for the Trust involved in change management or changes to existing systems that involve the use of personal information.

Purpose

The purpose and aim of this procedure is to provide a clear and straightforward overview to guide staff through the DPIA process and should be used alongside existing change management and risk management methodologies or a simplified process in its own right and to ensure that privacy risks are minimised whilst allowing the aims of the change to be met where possible.

Definitions

Data Privacy Impact Assessment - Privacy impact assessments (DPIAs) are a tool which can help the Trust to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

Confidentiality - is the right of an individual to have personal, identifiable medical information kept private. Such information should be available only to those with a legitimate right of access.

Information security - relates to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Benefits of Conducting a DPIA

Carrying out a DPIA is considered best practice, will improve transparency and is essential to demonstrate under data protection legislation that the impact of a change has been appropriately considered.

DPIA's once signed off by the SIRO and DPO must be published on the Trust website.

A change which has included a DPIA at the very start of the change, and updated as the change progresses, should result in the change being less privacy intrusive and therefore less likely to affect individuals in a negative way.

Assessing the need for a DPIA

The core principles of conducting a DPIA can be applied to any change which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals and can be used for a number of situations such as:

- A new IT system this would include clinical systems for storing and accessing personal data. This could be a spreadsheet, simple database or full scale clinical system.

- A proposal to identify people in a particular group or demographic and initiate a course of action for example a mail shot.

- Using existing data for a new and unexpected (by the data subject) or more intrusive purpose.

- A new surveillance system (especially one which monitors members of the public or patients) for example WiFi tracking, CCTV or tagging

- A new database which consolidates information held by separate parts of the Trust.

- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

- A data sharing initiative/agreement where two or more organisations seek to share, pool or link sets of personal data.

As previously stated a DPIA should be completed at the beginning of a change so that the outcome is able to influence the change, this may include preventing the change from going ahead. The DPIA must be reviewed and updated as a change progresses.

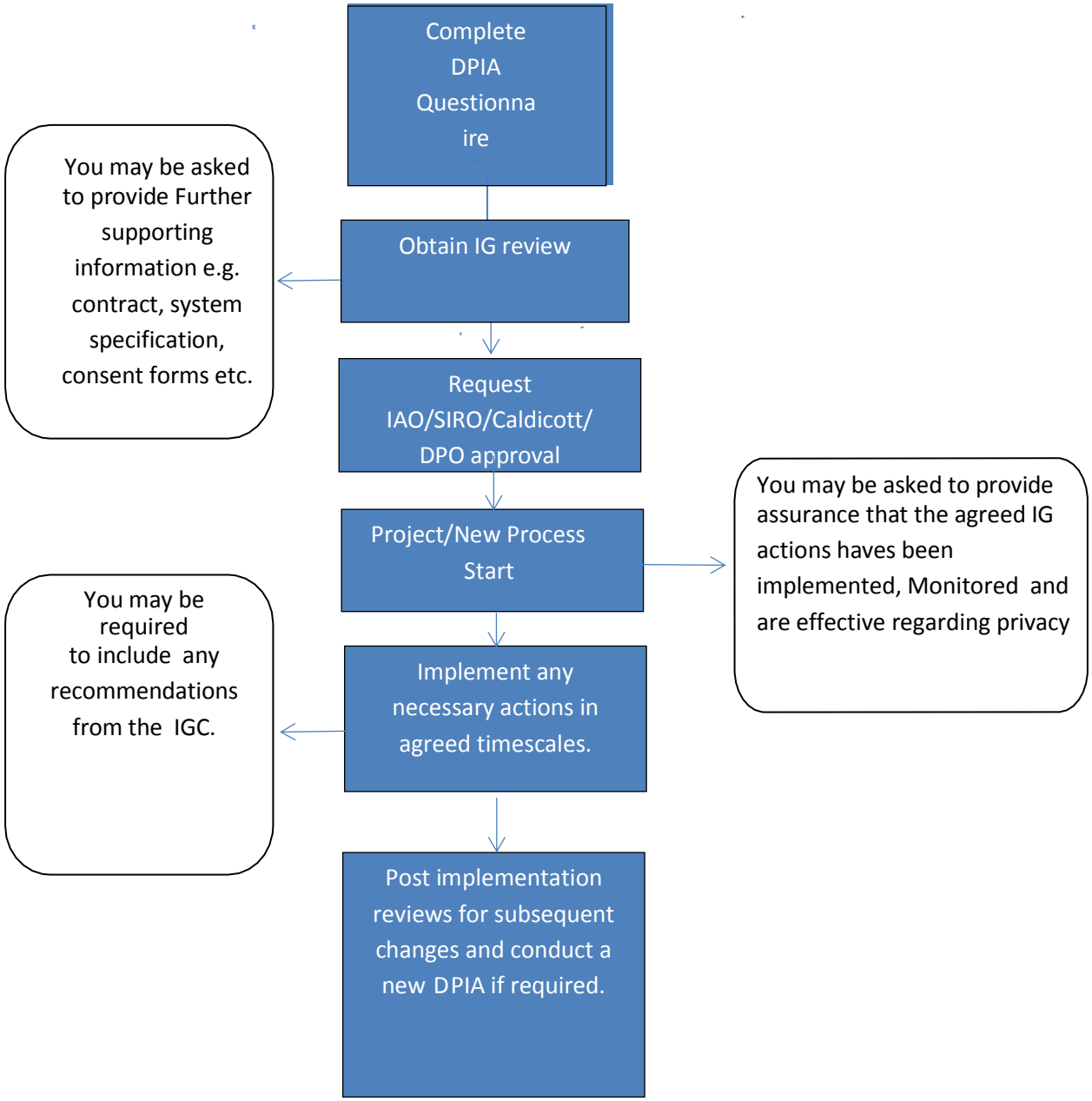
Responsibility for Conducting a DPIA

The person requesting or leading the change or change is expected to complete the DPIA using the guidance contained within this document to help focus on the privacy (including security) issues of the change or change.

The person completing the DPIA should not be afraid to involve others who may have appropriate skills although the DPIA is intended to be completed by non-experts.

When the completed DPIA is submitted to the ICT change and change board it will be reviewed by the appropriate people including the Information Governance Manager/DPO and the SIRO. The information governance manager can be consulted outside the process as required.

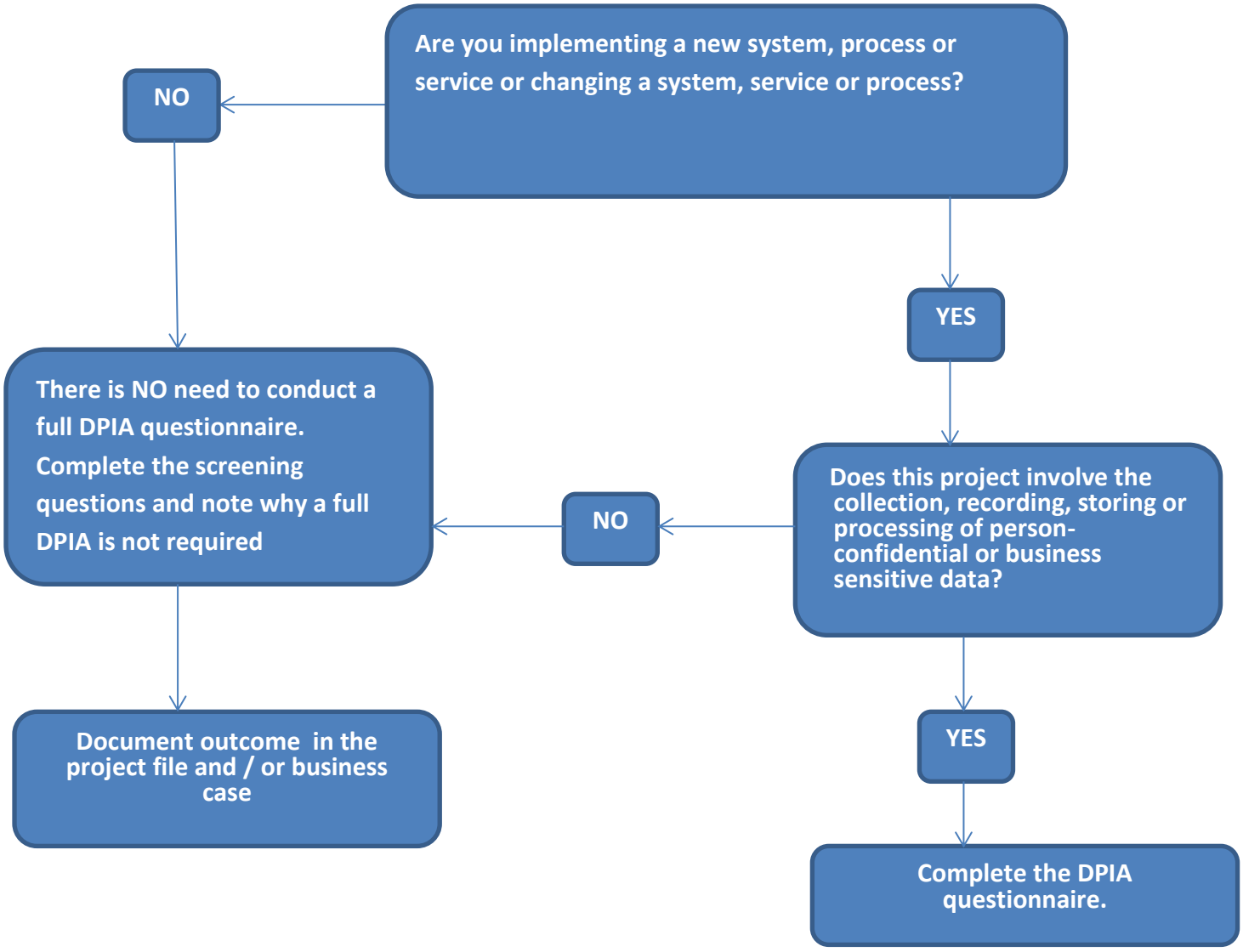
The DPIA Process


Complete DPIA Questionnaire
Obtain IG review
You may be asked to provide Further supporting information e.g. contract, system specification, consent forms etc.
Request IAO/SIRO/Caldicott/ DPO approval
Project/New Process Start
You may be asked to provide assurance that the agreed IG actions haves been implemented, Monitored and are effective regarding privacy
You may be required to include any recommendations from the IGC.
Implement any necessary actions in agreed timescales.
Post implementation reviews for subsequent changes and conduct a new DPIA if required.

Responsibility for the retention of documentation

Copies of the Change documentation must be appropriately retained by the relevant information asset owner (IAO).

Screening Questions – Do I need to complete a DPIA?



SECTION 2 - FULL DPIA

If a full DPIA is required complete the template below.

Please provide as much information as possible; the ICT Change Control Board is not able to carry out research on your behalf.

DPIA Cover sheet

ICT Help Desk Change Number		**N/A**
Project / Change Name		**Merton School children's Vision Screening by ESTH for London Borough of Merton**
Requester	**Name**	**<Redacted>**
	Title	**Joint Director of Planned Care**
	Email	**<Redacted>**
	'Phone	**<Redacted>**
Key Stake Holder (organisations) – Name		**<Redacted>**
	Title	Head of Contracts and School Organisation
	Email	**<Redacted>**
	'Phone	**<Redacted>**
This DPIA will be kept under review by Information Asset Owner	**Name**	**<Redacted> Joint Director of Planned Care**
	Email	**<Redacted>**

Full DPIA

Name of Organisations involved in the sharing of information	The London Borough of Merton, Education Team (CSF) will be sharing personal information with the Epsom and St Helier University Hospitals NHS Trust (ESTH).

Contract/Agreement: Describe type of contract.	London Borough of Merton (LBM), Education Team (CSF) has commissioned by way of contract ESTH to provide vision screening services in schools. A data sharing agreement will be put in place.
Background information on the project	The UK National Screening Committee recommends vision screening for 4 to 5 year old children. In October 2017, new guidance was published by Public Health England which states that Public Health within Local Authorities are responsible for ensuring that the vision screening of eligible children takes place as part of the healthy child programme. Please see the following link for more details: https://www.gov.uk/government/publications/child-vision-screening
Benefits of the project	Children with any issues identified as a result of the vision screening can be referred appropriately for early treatment and correcting at an early age.

Identify the conditions for each purpose to satisfy Article 6 and 9 of GDPR
How will these be met?

Purpose	GDPR Article 6	GDPR Article 9
'Processing is necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller'	**6(1)(e)**	
'…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'		**9(2)(h)**

In many cases the conditions would be
Art 6(1)(e) public function and Art 9(2)(h) health & Social Care

Lawfulness of the processing	Y/N
Processing is required by law	**N**
Processing is required to protect the vital interests of the person	**Y**
Is any processing going to be by a not for profit organisation, e.g. a Charity	**N**
Would any processing use data already in the public domain?	**N**
Could the data being processed be required for the defence of a legal claim?	**Y**
Would the data be made available publically, subject to ensuring no-one can be identified from the data?	**Y**
Is the processing for a medical purpose?	**Y**
Would the data be made available publically, for public health reasons?	**N**
Will any of the data being processed be made available for research purposes?	**Y**

Data Protection Review

Article 5 of the GDPR requires that personal data shall be:

Review compliance with the Data Protection Principles to ensure changes take account of these and follows a 'privacy by design' approach.

Principle	Compliance
(a) processed lawfully, fairly and in a transparent manner in relation to individuals;	LBM will provide fair processing information to parents and guardians. The data sharing agreement sets out how the personal information will be used.
(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;	The personal information will be processed for health care purposes. The data may be Anonymised or Pseudonymised for service planning and reporting purposes.
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	LBM will only share the information with ESTH required for ESTH to provide the service.
(d) accurate and, where necessary, kept up to date; every reasonable step must be	LBM will provide ESTH with accurate information based on their annual schools audit. ESTH will if it becomes aware of errors in the data

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;	provided by LBM inform LBM of the errors. An error or request to rectify may require ESTH to cease processing information in which case ESTH will inform LBM where the error is in the data provided by LBM.
(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;	The data provided by LBM to ESTH will be securely stored in ESTH's clinical records system in accordance with the Records Management Code of Practice for Health and Social Care 2016.
(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.	Access to ESTH computer systems requires a personal username and password. ESTH computer systems are regularly backed up, protected from Malware and protected by firewalls.
Article 5(2) requires that: "The controller shall be responsible for, and be able to demonstrate, compliance with the principles."	ESTH will have a data sharing agreement and contract in place with LBM which sets out how the personal data will be used in addition to this DPIA.

Consultation/Stakeholder Engagement

This section of the DPIA outlines:

- The key stakeholders;
- The areas of consultation;
- The method of consultation.

Stakeholder	Areas for consultation	Method of consultation	Outcome/Action
EG. Org Name	*EG: Operational matters relating to the joint care plan, consent issues, Fair Processing arrangement*	*E.G: Local internal meetings / Email*	*E.G: Data flows, NPIA, Information Sharing Agreement, consent model, privacy notice*
London Borough of Merton, Education Team (CSF)	Data sharing agreement / fair processing	Verbal discussion and email	DPIA, Data sharing agreement

Q	Category	Screening question	Yes/No
1.7	Data	Does the change involve new process, policy or significantly change the way in which personal and/or business sensitive data is handled?	No
1.8	Data	Does the change involve new or significantly changed handling of a considerable amount of personal and/or business sensitive data about each individual in a database?	N
1.9	Data	Does the change involve new or significantly change handling of personal data about a large number of individuals?	Y
1.10	Data	Does the change involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal and/or business sensitive data from multiple sources?	No
1.11	Data	Will the personal data be processed out of the U.K and / or EEA? Please give details	No

	N/A		
1.12	Exemptions and Exceptions	Does the change relate to data processing which is in any way exempt from legislative privacy protections? e.g. “251” exception	No
1.13	Exemptions and Exceptions	Does the change’s justification include significant contributions to public security and measures?	No
1.14	Exemptions and Exceptions	Does the change involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

2.1	**Is this a new or changed use of personal and/or business sensitive information that is already collected?**	New/Changed Changed in that ESTH will provide the screening service

2.2 What data will be collected?

Personal Confidential Data

Administration data

Forename	**X**	Surname	**X**	Date of Birth	**X**	Age	**X**	Gender	**X**
Address	**X**	Postcode	**X**	NHS No		Email Address			
Payroll number		Bio Metrics e.g. DNA, Finger prints				Tax, benefit, Pension			
Telephone Number		Hospital Number							
Bank, financial or credit card details		Mother’s maiden name				National Insurance number			
Health, adoption, employment, school, Social Services, housing records		Child Protection		Safeguarding Adults					
Another unique identifier (please specify)									

	Other data *(Please state):*	The Full name of parent/carer					
	Sensitive data						
	Racial or ethnic origin		Political opinion		Religious belief		
	Trade Union membership		Physical or mental health or condition				
	Sexual life		Commission or alleged commission of an offence				
	Proceedings for any offence committed or alleged						
	Will the dataset include clinical data? (please include)						
		No					
	Will the dataset include financial data?	No					
	Description of other data collected						
	NA						

	<u>Business sensitive data</u>			
	Financial			
	Local Contract conditions		(National contract conditions are in the Public domain)	
	Decisions impacting:	One or more business function		**Yes/No**
		Across the organisation		
	Description of other data collected			

2.3	**List of organisations involved in processing the data?** *If yes, list below*		Yes
			Yes
	Name	Data Controller (DC) or Data Processor (DP)?	Completed and compliant with the Data Protection and Security Toolkit
			Yes/No
	ESTH	DC	YES
	London Borough of Merton (LBM), Education Team (CSF)	DC	
	Comments on organisations involved in processing the data		
	NA		
2.4	**Has a data flow mapping exercise been undertaken?** *If yes, please provide a copy, if no, please undertake – see Note 4 for guidance*		Yes/No
			Yes
2.5	**Does the Work involve employing contractors external to the Organisation?** *If yes, provide a copy of the confidentiality agreement or contract?*		Yes / No
			No
	NA		

2.12	Is Mandatory Staff Training in place for the following?	Yes/No	Dates

2.6	**Describe in as much detail why this information is being collected/used?**		
	The information is being collected by LBM and shared with ESTH by LBM in order for ESTH to carry out children's vision screening for children living in the London Borough of Merton. Children will be able to benefit from this important screening. Children with any issues identified as a result of the vision screening can be referred appropriately for early treatment and correcting at an early age		
2.7	**Will the information be collected electronically, on paper or both?**	Electronic	Yes
		Paper	No
2.8	**Where will the information will be stored:**		
	The information will be stored in secure computer systems belonging to ESTH.		
2.9	**Will this information be shared outside the organisations listed above in question 3?**		Yes/No
	If yes, describe who and why:		Yes
	The identifiable information may be shared with other organisations providing care to the data subject.		
2.10	**Is there an ability to audit access to the information?**		Yes
2.11	**What roles will have access to the information?** (list individuals or staff groups)		
	Clinical staff providing direct care will have access to person identifiable information. Administrative staff supporting clinical staff and systems may be given access to personal information as required.		
2.11	**What security and audit measures have been implemented to secure access to and limit use of personal identifiable and/or business sensitive information?**		

Username and password	**X**	Smartcard		key to locked filing cabinet/room	
Secure Token Access		Restricted access to Network Files			X
Other: *Provide a Description Below*:					

	• Data Collection:		
	• Use of the System or Service:		
	• Collecting Consent:		
	• Information Governance:	Yes	Annual
2.13	**Are there any new or additional reporting requirements for this change?**	NO	
	• What roles will be able to run reports?		
	Existing clinical and administrate reports will be able to be run by clinicians and admin staff to support direct care and the provision of the service.		
	• What roles will receive the report or where will it be published?		
	Clinical Audit, Commissioners on request, Clinicians service administrative rolls.		
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?		
	Internally reports will be both identifiable and pseudonymised. External reports will normally be anonymous or pseudonymised		
	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?		
	No		

2.14	**If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?**	**Yes/No** Yes
2.15	**Have any Information Governance risks been identified relating to this change?** (if Yes the Risk section below will need to be completed)	No
2.16	**Are individuals informed about the proposed uses of their personal data?**	Yes
2.17	**Are arrangements in place for recognising and responding to requests for access to personal data (SAR)?**	Yes
2.18	**Will individuals be asked for consent for their information to be collected and/or shared?** *If no, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, he change has s251 approval or other:*	No
2.19	How will the data be deleted when no longer required, Please describe below?	

	When no longer required the data will typically be over written. Storage media no longer required will be securely destroyed.	

Information Flows

	Flow 1	Flow 2	Flow 3	Flow 4
Description of information flow	Personal Data from LBM to ESTH to enable vision screening			
No. of records/individuals affected	All LBM school children who are to have their vision screened.			
Opt out procedure	Opt out is provided by LBM and parents / guardians can request ESTH stop processing their and their child data.			
Source of information	Information provided by parents and Guardians to LBM.			
Method of transfer/transmission	Secure email			
Persistent or temporary (if persistent, detail the storage location flowing	Persistent. Data will be			

transfer)	stored in ESTH electronic clinical systems			
Deletion of information	Data will be securely erased / made unavailable when no longer required.			

Please add additional flows as required.

Risks identified and actions required.

Residual risks must be entered onto the Trust risk register.

		Impact				
		1.Trivial	2.Minor	3. Moderate	4. Major	5. Extreme
Probability	1. Rare	Low	Low	Low	Medium	Medium
	2. Unlikely	Low	Low	Medium	Medium	Medium
	3. Moderate	Low	Medium	Medium	Medium	High
	4. Likely	Medium	Medium	Medium	High	High
	5.Very Likely	Medium	Medium	High	High	High

Risk	Probability	Impact	Existing controls:	Additional controls required:	Probability	Impact	Result: is the risk eliminated, reduced, or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the change?
No new	risks have	been	identified					

SIGN OFF	
ICT Help Desk Change Number	**N/A**
Change Name	**Merton School children's Vision Screening by ESTH for London Borough of Merton**
Approved by Caldicott Guardian	
Name	**Dr V. De Silva**
Signature	**<Redacted>**
Date	**02/06/19**
Summary of Caldicott Guardian advice:	
Approved by SIRO	
Name	**Peter Davies**
Signature	**<Redacted>**
Date	**05/06/19**
Summary of SIRO Advice:	
Reviewed by DPO	
Name	**Paul Kenny**
Signature	**<Redacted>**
Date	**05/06/2019**
Summary of DPIO advice:	**N/A**

Residual risks approved by: If accepting high residual risks consult ICO	**N/A**
ICT Use only below	

Further Information

Further guidance is available from the information commissioner's web site. The Privacy Impact Assessment Code of Practice provides the relevant templates and further details on how the process should work.

The code of practice can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

References

Data Protection Act 2018
Caldicott principals
Department of Health Information Security Management Code of Practice
NHS Digital
The National Data Guardian's 10 Data Security Standards
https://ico.org.uk/