East of England Ambulance Service NHS Trust

Data Protection by Design/Default Policy

Document Reference:	POL055
Document Status:	Approved
Version:	V8.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Head of IG	July 2021	Corporate Records Manager
Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
V1.0	30th July 2012	Approved at EMT
V2.0	23rd February 2015	Review date extension agreed by IGG following approval by EMB

Version	Date	Comments (i.e., viewed, or reviewed, amended approved by person or committee)
V3.0	17th December 2015	Review date extension approved by ELB
V3.1	19th October 2016	Recommended by IGG
V4.0	17th November 2016	Approved by ELB
V4.1	February 2019	Reviewed by Information Governance Team
V4.1	March 2019	Approved by Information Governance Group
V5.0	20 March 2019	Approved by Management Assurance Group
V5.1	July 2019	Approved by IGG Chair's Action
V6.0	20 July 2019	Approved by Management Assurance Group
V6.1	13 May 2021	Approved by IGG
V7.0	19 July 2021	Approved by CRG
V7.1	17 May 2023	Approved by IGG
V8.0	19 June 2023	Approved by CRG

Document Reference	
Recommended at Date	Information Governance Group 17 May 2023
Approved at Date	Compliance and Risk Group 19 June 2023
Valid Until Date	June 2025
Equality Analysis	Completed
Linked procedural documents	Data Protection Policy Information Governance Policy
Dissemination requirements	To all managers and staff via bulletins and intranet
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Paragraph

Page

Appendices

1. Introduction

Under the UK GDPR the Trust has a legal requirement to ensure it has appropriate technical and organisational measures in place to implement the data protection principles effectively and safeguard individual rights.

The Trust must ensure data protection is integrated in all the Trust's processing activities from design through to the end of the lifecycle, including disposal. This is called data protection by design. Data protection by design is about considering data protection and privacy issues upfront in everything you do. Data Protection Impact Assessments (DPIAs) are an integral part of data protection by design and can be used as a tool to identify and reduce the data protection risks and also design more efficient processes for handling personal data.

Data protection by default is ensuring the Trust only processes data that is necessary to meet the specific purpose. All processing should be conducted in line with the data protection principles, specifically data minimisation and purpose limitation.

2. Purpose

This policy sets out how the Trust will embed a culture of data protection by design and default across the organisation. It is essential to minimising data protection risks and building trust amongst both our staff, patients and other stakeholders.

Designing projects or processes with data protection in mind at the outset can reduce data protection breaches, increase awareness of data protection risks and save costs/time in the long-term. Amending or changing systems/software retrospectively to meet data protection regulations is costly, labour-intensive and may affect the operability of the system. The aim of data protection by design is that these considerations are made at the point of conception.

This document will also assist staff undertaking a Data Protection Impact Assessment (DPIA) and defines the process to be followed when completing these assessments.

3. Duties

3.1 Director of Corporate Affairs and Performance

The Director of Corporate Affairs and Performance has a responsibility to the Board for ensuring that data protection by design and by default is embedded across the organisation and that DPIAs are undertaken to support this.

3.2 Directors

Directors are responsible for ensuring a DPIA is completed for any projects/processes/systems within their area and for promoting data protection by design and by default across their work channels and in their departments. This can be delegated to either the managers of the project or someone within the project team.

3.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for ensuring all information risks are correctly identified, proactively managed and that appropriate assurance mechanisms exist. The SIRO will be kept informed of DPIAs through the Information Governance Group meetings.

3.4 Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian will be kept informed of DPIAs relating to patient information through the Information Governance Group meetings.

3.5 Data Protection Officer (DPO)

The DPO is responsible for monitoring compliance with the data protection legislation through policies, audits and training. This includes monitoring how the Trust implements data protection by design and by default and making recommendations. The Data

Protection Officer will be responsible for approving all DPIAs completed within the Trust.

3.6 Project Managers

Project Managers must consider data protection at the initiation of any new project/plan and ensure that a member of the project team is assigned to undertake the DPIA screening and full DPIA if required. The term 'project manager' is used loosely as this refers to anyone who is responsible for initiation of a new project, service, policy, process.

3.7 Information Governance Team

The IG team will support the DPO and Trust directors to promote data protection by design and by default across the organisation. They will support project managers in completing the DPIAs and provide advice before submission to the DPO. The IG team will ensure the DPO is made aware of all DPIAs for final approval.

3.8 All Staff

All staff must be aware of any privacy risks and should assist with the DPIA to ensure these are identified and managed.

3.9 Consultation and Communication with Stakeholders

The Trust is committed to involving staff and key stakeholders in the development, review and monitoring of key data protection policies.

4. Data Protection by Design/Default

In order to be compliant with the requirements of the UK GDPR and to ensure the Trust keeping data protection at the centre of what we do, the Trust should ensure the following:

- Data protection is part of the design and implementation of new systems/services and as an essential component of the core functionality of all processing.

- Anticipation of risks or privacy incidents before they occur and take steps to prevent harm to individuals.
- Only processing the minimum personal data that we need for our purposes and only using the data for these purposes.
- Anonymisation and/or pseudonymisation should be used where possible and encouraged across the Trust.
- Ensuring personal data is automatically protected in any IT system or business practice so individuals do not have to take any specific action to protect their privacy.
- Providing the identity and contact information of those responsible for data protection both internally and externally.
- Adopting a 'plain language' policy for any public documents and providing individuals with the tools to determine how we are using their personal data.
- Offering strong privacy defaults, user-friendly options and controls and respect user preferences.
- Using data processors and/or other systems/products that pass the Trust's internal due diligence check in terms of data protection.
- Using privacy-enhancing technologies (PETs) to assist the Trust in complying with data protection.
- Assisting staff who are undertaking a Data Protection Impact Assessment and providing guidance on the procedure for this.

Although most of this will be business-as-usual, the Data Protection Officer will complete an annual data protection by design/default audit in order to ensure the Trust is meeting these obligations. Considerations of data protection by design/default will also be considered as part of any Data Protection Impact Assessment.

4.1 Pseudonymised and anonymised data

Pseudonymised data is the processing of personal data in a way that it can no longer be attributed to a specific individual without the use of additional information. An example would be the Trust's CAD reference numbers. You can only link the CAD back to a specific individual if you have the relevant information and the Trust has

technical and organisational measures in place to ensure the relevant information is accessed separately.

The legislation is clear that pseudonymisation is another security measure and the data itself is still classified as personal data.

Anonymised data is data that has been stripped of any personal identifiers and therefore the individual is no longer identifiable. If you can use other information to re-identify the individual then this information is pseudonymised, not anonymised. Truly anonymised data can help limit the potential data protection risk.

When you are working, try to use pseudonymised or, even better, anonymised data when you can to reduce the amount of unprotected personal data that is being transferred and therefore the risk of a data protection breach.

5. Data Protection Impact Assessments

The purpose of a DPIA is to allow an organisation to analyse the proposed processing and identify and minimise data protection risks. It will enable the Trust to ensure that privacy and data protection compliance is built into any systems or processes that hold or process information. It does not have to indicate that all risks are eradicated, in fact this is very unlikely, but it should help the Trust to document them and assess if the risk is justifiable or not. Completing the assessment may also help the Trust to focus on broader compliance issues, such as financial or reputational.

Under the UK GDPR, there is a legal obligation to complete a Data Protection Impact Assessment for any high-risk processing. This could include any of the following and should be read alongside the European Data Protection Board guidelines. This list is not exhaustive and guidance should be sought from the Information Governance Team and/or the Data Protection Officer:

- use systematic and extensive profiling with significant effects;

- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.
- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

All Data Protection Impact Assessments should be completed by the Project Manager with support from the Information Governance Team. A screening tool can be used to establish if a DPIA is required initially (Appendix A). The full DPIA template is in Appendix B.

The Data Protection Officer will approve all DPIAs and has a duty to consult with the ICO if any high risks identified as part of the processing cannot be mitigated.

Once complete the DPIA should be routinely reviewed, specifically if anything changes as the project develops or changes during implementation (see Appendix C).

6. Equality Analysis

An Equality Analysis has been completed for this policy (Appendix E).

7. Monitoring

See Monitoring Table – Appendix D

8. References

Data protection impact assessments | ICO

Data protection by design and default | ICO

9. Associated Documents

Data Protection Act 2018

General Data Protection Regulations (GDPR)

Privacy and Electronic Communications (EC Directive) Regulations

Appendix A Screening questions

Project Name:

Project Lead:

Project Overview:

Date screening completed:

Outcome:

The below screening questions are to determine if a full-scale DPIA is required. These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. The final decision should be made in conjunction with the Information Governance team and/or Data Protection Officer.

	Activity	Yes/No
1	Will the processing use systematic and extensive profiling of individuals or profiling on a large scale? (e.g. automated processing to evaluate certain things about an individual).	
2	Will it involve processing special category or criminal offence data on a large scale?	
3	Will it systematically monitor publicly accessible places on a large scale?	
4	Will it use profiling or special category data to decide on access to services/opportunities?	
5	Will it involve the processing of genetic or biometric data?	
6	Will it use innovative technology in combination with any of the EDPB criteria?	
7	Will it combine, compare or match datasets/data sources?	

	Activity	Yes/No
8	Will it involve processing without directly providing the individuals with a privacy notice?	
9	Will it involve processing individual's personal data with a view to tracking their online/offline locations?	
10	Will it involve processing children's personal data for profiling or automated decision-making purposes, including online information services?	
11	Will it involve processing that could result in the risk of physical harm in the event of a security breach?	
12	Will it involve processing of sensitive data or data of a highly personal nature?	
13	Will it involve the processing of data concerning vulnerable data subjects?	
14	Will it involve processing that involves preventing individuals from exercising a right or using a service?	
15	Does the processing include the use of new software or a new collection method?	
16	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
17	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
18	Will the project require you to contact individuals in ways that they may find intrusive?	

Appendix B – Data Protection Impact Assessment Template

Sample DPIA Template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in the ICO's DPIA guidance.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Project details

Name of manager completing DPIA	
Title of project	
Date DPIA completed	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Risk	**Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. See the Risk Matrix in Appendix D	**Likelihood of adverse effect** 5,4,3,2,1	**Severity of adverse effect** 5,4,3,2,1	**Overall risk rating** Overall risk + Likelihood multiplied by Severity
1a	Loss of data			
2a	Unavailability of data			
3a	Misuse of data			
4a	Integrity/accuracy of data			
5a	Unauthorised access			
6a	Unauthorised disclosure			

Step 6: Identify measures to reduce risk

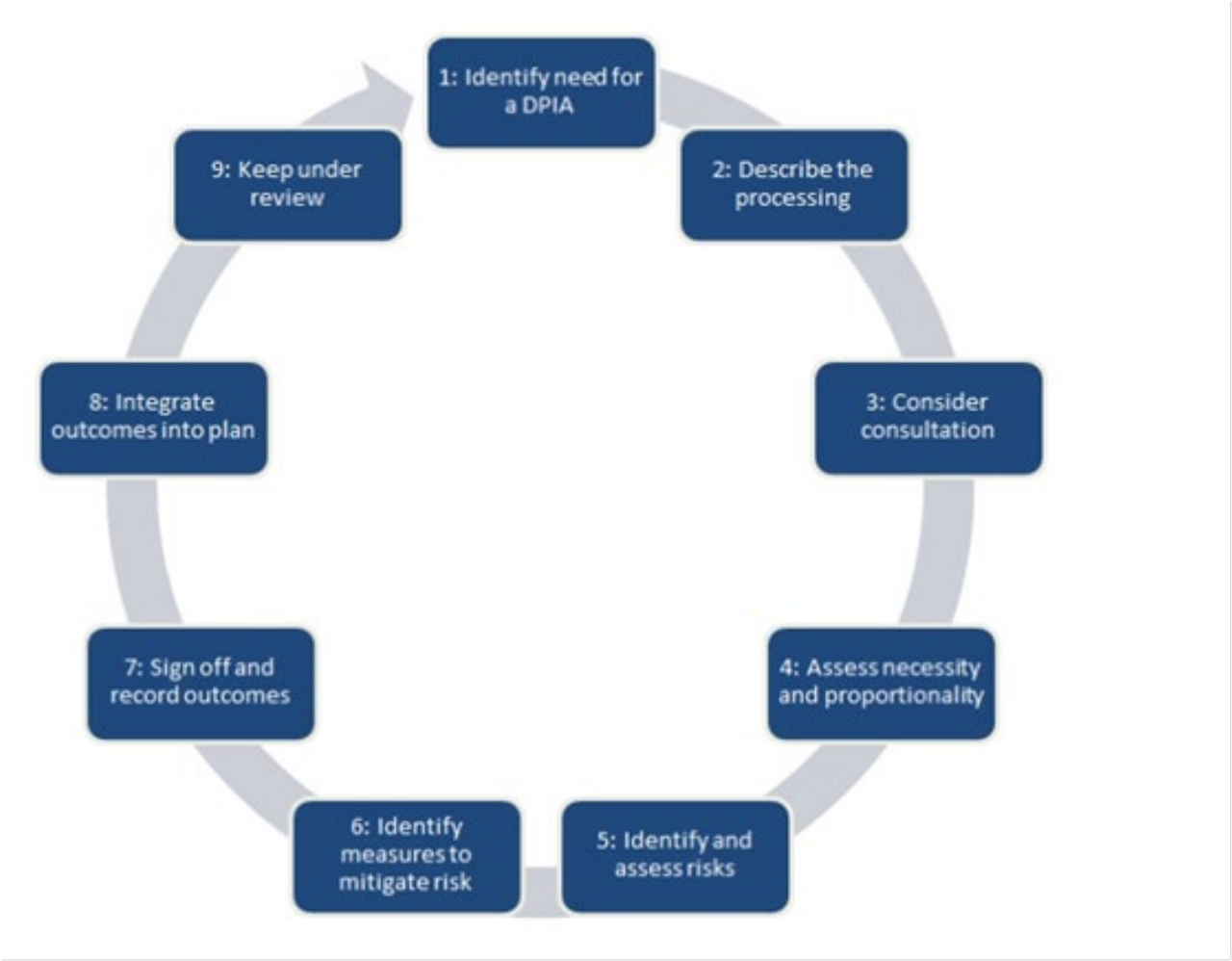
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to control the risk**. Include solutions for reducing or controlling the risks listed above.	**Effect on risk**	**Residual risk** This score should match the Severity Scoring above	**Risk control score** Risk control score = Effect multiplied by Residual
1a	Loss of data			
2a	Unavailability of data			
3a	Misuse of data			
4a	Integrity/accuracy of data			
5a	Unauthorised access			
6a	Unauthorised disclosure			

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA
DPIA Valid until date (VDU)		We recommend a minimum of 3 years after approval date, unless there are significant changes to the processing or risks.

Appendix C – Procedure to complete a DPIA

The Trust has adopted the following process for conducting a DPIA (in line with ICO guidance):



Procedure to complete a DPIA

1 Identifying the need for a DPIA

A DPIA must be completed before any processing of data is started that is 'likely to result in a high risk'.

The need for a DPIA should be identified as part of an organisation's usual project management process by using the screening questions in Appendix A of this document. Once completed the screening checklist should be discussed in conjunction with the IG team and/or Data Protection Officer.

2 Describing the information flows

Describe the information flows of the project and how the data will be processed. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information.

3 Consider consultation with stakeholders

It is always advisable to discuss the DPIA with a member of the IG team and/or Data Protection Officer. Relevant staff and patient groups should also be consulted with if the project will impact upon their individual rights.

4 Identifying the privacy and related risks, including an assessment of the necessity and proportionality.

You need to identify any privacy or legal risks to both individuals (for example, damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy, limitation of individual rights) and to the organisation (for example damage to reputation, or the financial costs of a data breach).

You should consider the necessity of the project and if there will be an impact upon individual rights, you should assess if this is proportionate to the aims of the project. You should also consider data minimisation and pseudonymisation.

The principles of data protection by design and default should be part of the consideration process when completed the DPIA.

5 Identifying and evaluating privacy solutions or ways to mitigate the risk.

Explain how you could address each risk. Some might be eliminated altogether whereas other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach and think about the available resources, and the need to deliver a project which is still effective.

6 Signing off and recording the DPIA outcomes

A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Make sure that the risks have been signed-off at an appropriate level, this can be done as part of the wider project approval. All DPIAs should be approved by the Data Protection Officer and minuted at the Information Governance Group.

The Trust's website informs the public that DPIAs will be shared upon request.

7 Integrating the DPIA outcomes back into the project plan

The DPIA findings and actions should be integrated with the project plan. It might be necessary to return to the DPIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

A DPIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.

Record what you can learn from the DPIA for future projects.

Appendix D- Risk Assessment Matrix

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No Adverse effect	1	1	2	3	4	5
			1	**2**	**3**	**4**	**5**
			Not occurred	**Not Likely**	**Likely**	**Highly Likely**	**Occurred**
			Likelihood of an adverse effect (harm)				

Appendix E – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Identification and completion of DPIAs	The completion of the DPIA is the responsibility of the Project Manager (support provided by IG team and DPO)	The DPIA and checklists will all be checked by the IG Team/Data Protection Officer and minuted at the Information Governance Group. DPIAs will also be approved by the Data Protection Officer.	As often as a DPIA is completed	The summarised DPIA and checklists	Completed DPIAs will be minuted at the Information Governance Group	Information Governance Group	The Project Manager will be responsible for implementing any accepted recommendations with support from the IG team and the DPO.

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Data protection by design/default	Data Protection Officer/IG team	Annual audit completed by Data Protection Officer	Annual	Audit will be presented to the Information Governance Group.	The IGG will read and interrogate any report to identify deficiencies in the system and act upon them.	Actions identified by DPO to be implemented in conjunction with IG team.	Lessons will be shared with all the relevant stakeholders.

Appendix F – Equality Analysis

Equality Impact Assessment

EIA Cover Sheet	
Name of process/policy	Data Protection by Design/Default Policy
Is the process new or existing? If existing, state policy reference number	Existing but amended
Person responsible for process/policy	Legal Services Manager (DPO)
Directorate and department/section	Clinical Quality/Compliance and Standards
Name of assessment lead or EIA assessment team members	Legal Services Manager (DPO)
Has consultation taken place? Was consultation internal or external? (please state below):	Internal consultation at Information Governance Group

<table>
<tr>
<td>The assessment is being made on:</td>
<td>
<table>
<tr><td>Guidelines</td><td></td></tr>
<tr><td>Written policy involving staff and patients</td><td>X</td></tr>
<tr><td>Strategy</td><td></td></tr>
<tr><td>Changes in practice</td><td></td></tr>
<tr><td>Department changes</td><td></td></tr>
<tr><td>Project plan</td><td></td></tr>
<tr><td>Action plan</td><td></td></tr>
<tr><td colspan="2">Other (please state)
Training programme.</td></tr>
</table>
</td>
</tr>
</table>

Equality Analysis
What is the aim of the policy/procedure/practice/event? The purpose of the policy is to set out the Trust's arrangements for embedding data protection across the organisation.
Who does the policy/procedure/practice/event impact on? **Race** ☐ **Religion/belief** ☐ **Marriage/Civil Partnership** ☐ **Gender** ☐ **Disability** ☐ **Sexual orientation** ☐ **Age** ☐ **Gender re-assignment** ☐ **Pregnancy/maternity** ☐
Who is responsible for monitoring the policy/procedure/practice/event? Legal Services Manager (DPO)
What information is currently available on the impact of this policy/procedure/practice/event? None. The impact of the policy is not currently monitored by EEAST. Any issues would be identified through patient or staff feedback and logged as a patient experience or incident on the Trust's DATIX system. Issues or cause for concern will also be picked up through the DPIA process. This information will be used to inform future policy reviews.
Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event? No
Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? No **Race** ☐ **Religion/belief** ☐ **Marriage/Civil Partnership** ☐ **Gender** ☐ **Disability** ☐ **Sexual orientation** ☐ **Age** ☐ **Gender re-assignment** ☐ **Pregnancy/maternity** ☐

Please provide evidence:

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? No, the policy is consistent in its approach regardless of these protected characteristics.

Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Please provide evidence:

Action Plan/Plans – SMART

Equality and Diversity Training for the Legal Services Manager (DPO) and wider Information Governance Team to ensure they are able to identify any negative impact on groups of people. This is part of the Trust's annual mandatory training programme and will be monitored by the Training and Education Department.

Specific

Measurable

Achievable

Relevant

Time Limited

Evaluation Monitoring Plan/how will this be monitored?
Who – Legal Services Manager (DPO) and Information Governance Team.

How - Each instance will have to be considered on a case-by-case basis but the expectation is that measures will be taken to ensure there are no negative impacts when embedding data protection across the organisation. Adjustments can be made through the Data Protection Impact Assessment process to ensure no individual is negatively impacted.

By – As and when identified.

Reported to – Equality and Diversity Lead.