

Kallidus LMS

Data Protection Impact Assessment

October 2024

V1.0



**NHS fraud.
Spot it. Report it.
Together we stop it.**

Executive Summary

This document contains information in relation to *Kallidus LMS*

The document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (June 2023).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

[Government Security Classifications Policy June 2023.docx \(publishing.service.gov.uk\)](#)

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: **'OFFICIAL-SENSITIVE'**

The document is subject to CROWN COPYRIGHT. It is provided in confidence under existing laws, regulations and agreements relating to the protection of data and shall be so protected. The information contained herein is proprietary and shall only be used for the purposes intended at release. It shall not be reproduced, adapted or used in, whole or in part, for any other purpose without the prior written consent of the Secretary of State for DEPT in the Government of the United Kingdom.

Nothing contained herein should be construed as endorsing any particular Technical Solution to any United Kingdom Government Invitation to Tender.

Table of contents

Executive Summary2

Links & Dependencies.....5

1. Data Protection Impact Assessment Requirement & Process6

 Introduction.....6

Kallidus LMS - General Description7

 Data Protection Impact Assessment.....7

 Ownership 19

2. DPIA Report 19

 Section 1: Data Maintenance and Protection Overview..... 19

 Section 2: Uses of the Application and the Data..... 19

 Section 3: Data Retention.....20

 Section 4: Internal Sharing and Disclosure of Data20

 Section 5: External Sharing and Disclosure of Data20

 Section 6: Notice/Signage20

 Section 7: Rights of Individuals to Access, Redress and Correct Data.....20

 Section 8: Technical Access and Security.....21

 Section 9: Technology21

3. Compliance Checks21

 DPA 2018 Compliance Check21

 The Privacy and Electronic Communications Regulations.....21

 The Human Rights Act.....21

 The Freedom of Information Act.....22

 Conclusion.....22

Annex A - Definition of Protected Personal Data.....23

Annex B - Data Protection Compliance Check Sheet.....24

Document Control					
PM	Ref	Document owner	Version No	Issue Date	Amendments
WD Lead/L & D Officer	DPIA Kallidus LMS	DPO	V0.1	April 2024	Initial creation
WD Lead/L & I G Officer	DPIA Kallidus LMS	DPO	V1.0	October 2024	Final

Prefix	
Reference:	DPIA (Kallidus LMS)
Date:	October 2024
Author:	Workforce Development Lead/L & D Officer
Data Owner:	Corporate Affairs (Information Governance)
Version:	1.0
Supersedes	N/A

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	June 2023	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

- 1 The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.
- 2 DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.
- 3 To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.
- 4 A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also affect other fundamental rights and interests:
 - a. "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to **physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data¹..."
- 5 Under GDPR you must carry out a DPIA where for example you plan to:
 - b. process special category or criminal offence data on a large scale.
- 6 The ICO also requires a DPIA to be undertaken for example, where you plan to:
 - c. use new technologies;
 - d. match data or combine datasets from different sources;
 - e. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- 7 DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection

¹ GDPR - Recital 75

obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

9 This DPIA is related to the NHSCFA Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

Kallidus LMS - General Description

Reporting on Learning and Development activities and Performance Management monitoring are core requirements of the business. The Learning Management System (LMS) will enable all the data to be kept securely in one place and negate the need for various spreadsheets and single task systems managed by various people.

The data will be collected from NHSCFA and Kallidus will process the data on a regular basis to ensure the information on the LMS is accurate and up to date.

This is the first DPIA to be completed on the system and it has been carried out by the Information Governance Officer, in consultation with the Workforce Development Lead and the Information Governance and Risk Management Lead.

The Kallidus LMS, in addition to GDPR is also required to comply with other relevant HMG legislation including. Where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

To ensure the Kallidus LMS meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template comprised of seven steps:

Step 1 - Identify the need for a DPIA

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

Step 7 - Sign off and record outcomes

STEP 1: Identify the need for a DPIA

Explain broadly what the system/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.

The project aims are to have the ability to report meaningful management information to organisational leaders. This information will be used to support the development of policy processes and procedures within NHSCFA.

In addition, this information will be a core data source that will enable the accurate and timely reporting of specific metrics in the future.

The processing of this data is to simply report meaningful management information that is easily digestible and usable by the organisation, currently NHSCFA has various pieces of information in different spreadsheets and systems which take time and resource to collate and merge into something meaningful. The use of formula, counts, calculation, sums, lookups will be made in the processing of this data to calculate the amount and frequency of learning activities taken up by colleagues' compliance with Statutory and Mandatory learning, and completion of required performance reviews and objective setting meetings within the organisation.

The requirement to conduct a DPIA has been identified by the Governance SMEs.

At this point in time, our intention is to extract core data on a routine basis and analyse for patterns, and for key statistics. It is the protection of this data in its raw format that has mainly prompted the DPIA. In addition, Workforce Development want to provide assurance to the organisation people that we are processing this data in a safe, legal and ethical way that supports the business. See the scope of processing for fields and range of data.

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?
2. What is the source of the data?
3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?
4. Why types of processing identified as 'likely high risk' are involved?

1 The data will be extracted from Staff Establishment reports received monthly by HR from BSA. The data will be entered into Kallidus via CSV files which are uploaded using Filezilla. The data will be processed to meet management information requirements to inform decision making within NHSCFA. Currently this is a lengthy and resource intensive task collecting information from various sources to create these reports. The information will be restricted based on assigned permissions. Physical touch points of the data will also be minimised after the initial data extrapolation and implementation phases of the LMS project have been completed. Any reports will be shared to management within NHSCFA in pdf/word versions with no embedded data.

2: The data will be stored in a secure folder on PWD Lead personal drive . The retention of this data will be retained for a specified period of time for statistical purposes, given that the intention is to report routinely, it is envisaged that aggregate datasets are requested to cover late data entries and account for changes, , We are recommending that Training records be retained until 6 years after someone leaves and Performance Management data is retained for 6 years in line with the current data retention schedule which states that data sets from ESR are retained for 6 years. Statistical reporting will be retained within NHSCFA archives for reference and trend analysis and anonymised. If we were to follow advice provided by the CIPD we would apply the this as best practice given this data is HR related, we envisage this being no longer than six years once reported:

3: The raw data will be made available to Kallidus in order to update the platform on a regular basis with accurate and up to date information of learners and users. The raw data will be shared with Kallidus via an uploaded CSV file through Filezilla.

4: PWD specialist will process (data in line with agreed Standard Operating Procedure. This will include personal data which could identify an individual and will be removed as far as possible consistent with maintaining coherence of the data set .No data collected is considered high risk.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?
2. How much data will you be collecting and using?
3. How often?
4. How long will you keep it?
5. How many individuals are affected?
6. What geographical area does it cover?

1. Data Fields to be included on the LMS are:

REDACTED

No special category or criminal offence data will be included.

2. We are collecting the minimum data to allow the approved reports to be produced.
3. Frequency could be as often as daily
4. Guidance from Governance and HR will be requested regarding "Leavers' data" all other data will remain on the system during the lifetime of a colleague's employment with CFA. The Data Retention Schedule states that data sets from ESR are retained for a period of 6 years and data from CPOD 6 years for internal staff use and 3 years for external staff use with a caveat of 6 years after termination of employment
5. This applies to all NHSCFA staff & Board
6. It will cover England

Describe the context of the processing:

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

1. Relationship is professional – processing NHSCFA data on behalf of NHSCFA
2. Employees will have no control on the production of management information, however employees will have the opportunity to change their ESR records from which the data is extracted.
3. Yes this is standards business reporting across the NHS
4. No – employees only
5. No prior concerns
6. Proprietary to Kallidus – but not new technology.
7. Always evolving and changing and needing periodic review.
8. No
9. The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network. (Supplier response provided.)

Intentionally left blank

Describe the purposes of the processing:

1. What do you intend to achieve?
2. What is the intended effect on individuals?
3. What are the benefits of the processing, for you and more broadly?

1. Production of quality management information and responses to requests for records from staff
2. To allow a structured and informed approach to personal development and performance management.
3. Benefit to NHSCFA has already been discussed within this document and in point 1 & 2.

STEP 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?
2. Who else do you need to involve within your organisation?
3. Do you need to ask your processors to assist?
4. Do you plan to consult information security experts or any other experts?

1. Those in PWD who led the procurement are the subject matter experts and understand the needs of the business reports and user interface that was required. There would have been no benefit in canvassing further afield for views and would have vastly increased the procurement timescales and sign off processes.
2. Technology; Comms, Digital Design, PWD, SMT BSA
3. Not for this system
4. Yes we have already consulted internally with Governance and security specialists. We have also enquired of the provider and have attached their response for review to this same email.

4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?
2. Does the processing actually achieve your purpose?
3. Is there another way to achieve the same outcome?
4. How will you prevent function creep?
5. How will you ensure data quality and data minimisation?
6. What information will you give individuals?
7. How will you help to support their rights?
8. What measures do you take to ensure processors comply?
9. How do you safeguard any international transfers?

1(Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) / DPA The lawful bases for processing are set out in Article 6 of the GDPR is:

- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. Processing is necessary for the performance of a contract to which the data subject is party .

2.Yes

3.As -previously mentioned we could extract the data separately from various sources including spreadsheets and other internal systems and then bring together manually .

4.Introduce core data which is relevant to the process and regularly review the data. Information from the BSA spreadsheet is redacted before forward disclosure to Training and Development.

5. Data Quality will be monitored through the regular uploading of up to date information from NHSBSA and the ongoing reviewing of that data by the workforce Development team during daily usage.

6.Individuals will be able to see their own data that is on the system . The data will be visible to their line managers to support performance reviews and development conversations.

7.Ensure compliance with the DPA, protecting personal data and its integrity, ensuring governance is applied at key stages without minimising the operational need to change specific reporting criteria.

8.The plan for this data is to incorporate key management information and support recording and reporting where necessary within the set areas of the system

9.There is no requirement to conduct international transfer this data

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	Likelihood of harm Remote, Possible or Probable	Severity of harm Minimal, Significant, or Severe	Overall risk Low, Medium or High
Data Breach	Possible	significant – sensitive data which could identify individuals	Low

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.	Effect on risk Eliminated, Reduced, Accepted	Residual risk Low, Medium, High	Measure approved by SMT Owner Yes-JB
There are no risks identified as medium or high risk for this DPIA.			JB

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by SMT Owner:	Yes	Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by SMT Owner:	Yes	If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by the Information Governance Officer:		The DPO should also review ongoing compliance with DPIA

Ownership

The following table describes the roles and responsibilities

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	PWD LT Lead
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Kallidus
Data Protection Officer	

1 DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The impact level of the Kallidus System was assessed as OFFICIAL/OFFICIAL SENSITIVE and it can only be accessed internally.
2. The following measures briefly describe what controls have been implemented to protect the Kallidus System and the personal data recorded:
 - a. The Kallidus System is accessed by approximately 225 members of staff from NHSCFA as users only, this includes 4 people who are the database administrators with access to the whole system .
 - b. The Kallidus System does have direct interconnections with other NHSCFA systems and applications to allow access to policies and documents that relate to the learning on the Kallidus System.
 - c. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.
3. It is assessed that there are no residual privacy risks to the personal data used by the Kallidus System
4. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

5. PWD Lead has responsibility for the administration of the System
6. Information in the Kallidus System could include;

7. No sensitive data is processed.

8. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

9. The Kallidus System is subject to NHSCFA Data Handling and Storage Policy. .Following a 6 year retention period data is automatically deleted by the Kallidus System.

10. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

11. The System is accessed by approximately 225 members of staff from NHSCFA, each with restricted access permissions to their own personal data, and includes 3 database administrators .

Section 5: External Sharing and Disclosure of Data

12. The only information shared with external organisations, would be if it was requested for the administration of justice.

Section 6: Notice/Signage

13. The data subject is aware that we hold the data for them

NHSCFA's privacy policy on its website hosts separate sections in relation to data collection, retention and storage. This broadly covers all elements of the NHSCFA usage of data, in a nonspecific manner.

14. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this Database/System and therefore outside the scope of this DPIA.

Section 7: Rights of Individuals to Access, Redress and Correct Data

15. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

16. It is unlikely that many access requests will be received as the personal data recorded is all in relation to training records and appraisals which individuals can access themselves on the system.

17. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

18. All NHS employees and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

19. The security and technical access architecture of the Database/System is as explained in this DPIA:
The application and the hosting infrastructure was assessed at **Official-Sensitive** and the hosting infrastructure is subject to the ISO27000 and ISO27001
20. Access is restricted to internal staff only.
21. The technical controls to protect the database include: *[confirm with ISA and amend accordingly]*
 - a. Anti-virus protection;
 - b. Permission based access controls to shared drive.
 - c. Logging, audit and monitoring controls.
 - d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

22. The Database/System holds personal information obtained electronically and is located in the NHS Counter Fraud Authority data centre.

2 Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the Kallidus System, and the personal data that it records, and its business activities, are compliant and maintain compliance with:
 - a. The GDPR and the Data Protection Act in general;
 - b. The Data Protection Principles;
 - c. The interpretations of the Principles.
2. **This is not a recommendation but a requirement of law.**
3. The roles and responsibilities for the protection of personal data are described in the NHSCFA security policy.
4. The Database/System processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed (see Annex B) describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, See; also Annex A.

The Privacy and Electronic Communications Regulations

The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

5. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

6. As a public authority we are compliant with the provisions of the Freedom of Information Act, in proactively publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, no personal information would be disclosed under the Freedom of Information Act as this would breach the data protection principles.

Conclusion

7. There are no residual privacy risks to the personal data recorded in the Database/System. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA PWD
Project	Kallidus LMS

2. Contact position and/or name.

(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Redacted
Branch / Division	Corporate Affairs,NHSCFA

3. Description of the programme / system / technology / legislation (initiative) being assessed.

(Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

Kallidus is a learning management system. It delivers reliable reporting and management recording. Reporting on Learning and Development activities and Performance Management monitoring are core requirements of the business. The Learning Management System(LMS) will enable all the data to be kept securely in one place and negate the need for various spreadsheets and single task systems managed by various people.

4. Purpose / objectives of the initiative (if statutory, provide citation).

NHSCFA leads on a wide range of work to protect NHS staff from economic crime.

The purpose of the Database/System is:

The project aims are to have the ability to report meaningful management information to organisational leaders. This information will be used to support the development of policy, processes and procedures within NHSCFA.

In addition, this information will be a core data source that will enable the accurate and timely reporting of specific metrics in the future.

5. What are the potential privacy impacts of this proposal?

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the Kallidus System has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

6. Provide details of any previous DPIA or other form of personal data* assessment done on this initiative (in whole or in part).

This is the first DPIA carried out on the system.

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

***IMPORTANT NOTE:**

'Personal data' means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Page left intentionally blank.

NHSCFA offices

Coventry

Cheylesmore House,
5 Quinton Road
Coventry
CV1 2WT

London

7th Floor
10 South Colonnade
Canary Wharf
London
E14 4PU

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH