Data Protection Impact Assessment 2025

for the

National Audit of Eating Disorders (NAED)

NAED DPIA review date: July 2025
Next review due: March 2026
RCPsych DPIA Template September2020 V3.0

Contents

Data Protection Impact Assessment

Overview

If you're conducting a project that will use personally-identifiable information, whether you're collecting it or it's being given to you, or you want to use an existing store of data in a different way, you are required to complete a *Data Protection Impact Assessment* (DPIA). Examples of the sort of personal data which will attract a DPIA are: pseudonymised, special category (sensitive), healthcare, social care, financial, but this list is not exhaustive.

This document comprises two sections:

1. A set of screening questions to clarify whether a DPIA is required.
2. A template form for a DPIA, based on guidance issued by the Information Commissioner's Office (ICO).

Please refer to the annexes for help with completing the DPIA.

Section 1: Screening questions

These questions are intended to help you decide whether a DPIA is necessary. If you answer 'yes' to any of these, a DPIA is required. You should also consider completing a DPIA for projects which are already running where these screening questions may apply. You may expand on your answers as the project develops if you need to.

1. Does the project involve the collection of new information about individuals? *Re-use of data collected for a different purpose is covered by question 4.*	Yes – data will be extracted from the Mental Health Service Dataset (MHSDS), Hospital Episode Statistics (HES) and Office for National Statistics (ONS) relating to eating disorders care.
2. Does the project compel individuals to provide information about themselves or ask others to disclose it on their behalf? *For example, a Trust providing data about an individual patient's care.*	Yes – data is submitted by Trusts to the MHSDS, HES and ONS. The NAED is requesting access to these routine datasets.
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No patient-level data will be made available to organisations or people who have not had routine access to it before. Data at the patient-level will only be viewable to the services for which that data is submitted. The only exception to this is the access obtained by the NAED and its sub-processer, Crown

	Informatics LTD, to process the data. Aggregated/anonymised data will be made publicly available on an interactive online dashboard with small numbers hidden to avoid re-identification.
4. **Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**	Yes – data from these sources have not been used for the purpose of a national eating disorder audit before. Data will be analysed to provide local, regional and national level benchmarking against 12 audit metrics.
5. **Does the project involve you using new technology that might be perceived as being privacy intrusive?** *For example, the use of biometrics, facial recognition or fingerprint technologies.*	No
6. Will the project result in you making decisions or taking action against individuals in ways that could have a significant impact on them?	No
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? *For example, health records, criminal records or other information that people would consider to be private. Or any sensitive personal data (see Annex 4).*	Yes – Data collected will include sensitive data relevant to an individual's care under mental health services including gender, ethnicity, psychological and other interventions. Additionally, data pertaining to hospital admissions, social deprivation and death will be collected.
8. Will the project require you to contact individuals in ways that they may find intrusive?	No
9. Does the project involve any data concerning vulnerable individuals who may be unable to easily consent or	Yes - data will be collected on people with eating disorders and mental health difficulties

oppose the processing, or exercise their rights? *This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, or patients.*	(including those who lack capacity to consent to care) and will include the elderly, young people aged under 18 years old, and others who may be unable to consent (e.g., those with learning disabilities and other vulnerable groups).
10. Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes – The data will be obtained by requesting access routine datasets including the MHSDS, HES and ONS, containing information submitted as part of clinical care.

Section 2: Data Protection Impact Assessment Form

Step one: Identify the need for a DPIA

Explain what the project aims to achieve and what the benefits will be to the College, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified drawing on your answers to the screening questions.

The National Audit of Eating Disorders (NAED) is a new audit programme commissioned by the Healthcare Quality Improvement Partnerships (HQIP) as part of the National Clinical Audit and Patient Outcomes Programme (NCAPOP) on behalf of NHS England. The audit programme will run from August 2024 to July 2027. The overarching quality improvement objectives focus on key areas of quality care namely that services are safe, effective, patient centred, timely, efficient and equitable.

By collecting, linking, analysing and reporting data on eating disorders access and treatment, the NAED seeks to drive improvement of the identification and appropriate management of eating disorders (ED) and the quality and consistency of services for children and young people (CYP), adults of working age and older adults.

In its healthcare improvement strategy, the NAED outlined 4 healthcare improvement goals. The purpose is to assess whether patients seen by ED services in England receive consistent, high-quality care in relation to the NAED audit measures that are aligned to a set of professionally agreed guidelines and standards, to identify areas for improvement and to empower stakeholders to use audit data to stimulate improvement in care delivery and outcomes. The goals are as follows:

1) **Increase access to care**: Increase the percentage of patients receiving NICE concordant treatment within the appropriate timeframe according to whether they have been assessed as urgent or routine.
2) **Improve the offer and uptake of NICE concordant treatment:** Increase the percentage of patients being offered and taking-up NICE concordant treatment.
3) **Improve patient outcomes**: Improve the recording of patient-reported outcome measures (PROMs) and clinician-reported outcome measures (CROMs) related to physical and mental health.

4) **Reduce health inequalities** Achieve parity of esteem across the following areas: Children and Young People (CYP) and adult services, geographical location, ED diagnoses.

The NAED are contracted to deliver 12 audit metrics using routinely collected sources to benchmark the performance of ED services at local, regional and national levels. These metrics were developed in collaboration with key stakeholders, including clinicians, service users and carers to ensure they reflected the areas of importance to those using services (see section 2 for full metric list). The obtaining of confidential patient information is essential to facilitate their measurement. Patient identifiers are required to link the datasets. The NAED intends to use the following data sources:

Mental Health Services Data Set (MHSDS)
Hospital Episode Statistics (HES)
Office for National Statistics (ONS)

The NAED will be publishing benchmarked data against the metrics on a quarterly basis from July 2026, on an interactive online dashboard. The dashboard will provide ED services with an overview of their performance at national, regional, and local levels. Services will be able to compare their performance across teams and services within their Trust/region, accessing run charts to identify trends in their data. Aggregated data will be made available to the public.

The NAED Quality Improvement Network will facilitate learning events and webinars on QI methodology, led by our QI experts and clinical and service user advisors, that support teams to use audit data for improvement activities. The approach will use the Institute for Healthcare Improvement's 'Model for Improvement'. Forums will allow audit participants to share their improvement projects and examples of good practice, including videos, interviews, blogs, and newsletters.

In 2027, a 'state of the nation' report will be produced, summarising national trends in the data and sitting alongside recommendations from the NAED's clinical and lived experience advisors. The accessible report will be co-produced with Beat and the NAED's Service User and Carer Advisory Group (SUCAG).

The methodology the NAED has been contracted to use involves the unconsented processing of patient data from routinely collected and pre-existing datasets. It is because of this that a DPIA was deemed necessary.

Step two: Describe the information flows

Please describe the collection, use and deletion of personal data here.

Include: where you are getting the data from, where it will be stored, where it could be transferred to, and the number of individuals likely to be affected. Please ensure you identify the Data Controller and Data Processor/s within the flows and any sub-contracted parties.

National Audit of Eating Disorders (Core Audit)	
Data source	*MHSDS, HES and ONS data*
Output	- Online dashboard (local, regional and national level) - State of the nation report (July 2027) - *QI learning workshops and webinars* - *Peer-review articles* - *Conferences (e.g. Congress)*
Data shared with	*StatsConsultancy – external statistician will be sent pseudonymised sections of data for analysis.* *Crown Informatics LTD – online dashboard provider will be sent pseudonymised data for upload onto the platform.* *Beat – aggregated/anonymised data will be shared with third party charity Beat and our Service User and Carer Advisory Group (SUCAG) to provide feedback o audit findings and co-produce outputs.*
Contains identifiable personal information?	*Yes – Identifiable and pseudonymised data* *Identifiable field(s): CareProfLocalTeamID*
Contains sensitive information?	*Yes – Information relating to individuals' care under mental health services will be processed*
Electronic Storage	*Microsoft Azure Secure Server – Accessed only by named individuals within the CCQI granted security clearance. All identifiable information will be transferred here for secure storage and pseudonymisation before export onto the RCPsych Sharepoint.* *RCPsych Sharepoint – Pseudonymised data will be transferred from the secure*

	server onto the general server for processing and analysis. *Crown Informatics LTD – Pseudonymised data will be uploaded onto the online data dashboard for the display of aggregated outputs.*
Paper/Hard copy storage	*No*
Comments	

Registered Trust/Organisation Audit Contacts	
Data source	Submission from Trust/organisation via registration form.
Output	Correspondence (emails, letters)
Data shared with	N/A
Contains identifiable personal information?	Yes
Contains sensitive information?	No
Electronic Storage	On RCPsych SharePoint (with restricted access)
Paper/Hard copy storage	No
Comments	

Step three: Consultation requirements

Explain what practical steps you will take to ensure you identify and address Data Protection risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process. For example, 'Discussed storage with Information Security Team'.

- Discussed College IG policy and data management processes with project team
- Discussed GDPR requirements with internal Data Protection team and GDPR leads
- Discussed secure storage for identifiable data with IS team

Step four: Identify the Data Protection and related risks

Identify the key Data Protection risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Use Annex 2 to help identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk
Identifiable data are securely transferred from NHS England onto the Microsoft Azure secure sever	Personal identifiable data, could cause harm or distress if accessed/lost/shared	Data are subject to unlawful access or processing, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage
Identifiable data held on third party servers (Microsoft Azure)	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are copied and/or retained longer than required, is subject to unlawful access or	Could lead to regulatory fines, reputational damage.

		processing, or is lost or shared as part of a data breach	
Personal pseudonymous data are collected on thousands of service users which are uploaded to Crown Informatics LTD online dashboard to display analysis results	Personal and sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Sensitive, pseudonymous data held on third party servers (Crown Informatics LTD)	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are copied and/or retained longer than required, is subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Sensitive pseudonymous data are stored on thousands of service users, which is copied across software files for analysis	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Identifiable or pseudonymous data (electronic) accessed by unauthorised staff at RCPsych	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, or is lost or shared as part	Could lead to regulatory fines, reputational damage.

		of a data breach	
Pseudonymous datasets shared by email	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Laptop containing personal data that is lost or stolen	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage
The wrong datasets are shared with members, containing data on service users from other organisations	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.

Step five: Identify solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary.

For example, the production of new guidance or future security testing for systems. Risks may include those affecting individuals, organisations or third parties (e.g. misuse or overuse of data, loss of anonymity etc.), compliance risks with GDPR or other relevant legislation, corporate risks (e.g. reputational, loss of trust of service users or the public).

- NAED team will request deletion of data from Microsoft Azure to comply with Section 251 for handling identifiable information.
- Contract is in place with Crown Informatics LTD and Microsoft Azure, who appropriate hold security credentials: ISO 27001.
- Only RCPsych approved laptops are used with appropriate security protections.
- Pseudonymous datasets are stored on secure sharepoint with restricted access to project folders. Computer terminals time-out and require password access.
- Identifiable datasets are stored on Microsoft Azure servers (outside RCPsych system), and access will be granted only to named staff via remote desktop, allowing all access to be logged. Only pseudonymous versions of the dataset will be stored on RCPsych sharepoint.
- Policy is to review retention of datasets annually.
- After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.
- Delete pseudonymous data held on third party servers (Crown Informatics LTD) when no longer required.
- Identifiable data will be retained as per Section 251 approval, with any extension to this requiring revised Section 251 approval.
- All shared datasets are password protected; no identifiable data are returned to sites. Checking procedure in place within team for all datasets sent.

Step six: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Person Responsible and deadline for completion	Approved by
Identifiable data are securely transferred from NHS England onto the Microsoft Azure secure sever	Contract is in place with Microsoft Azure, who appropriate hold security credentials: ISO 27001.	Philippa Nunn, Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research
Identifiable data held on third party servers (Microsoft Azure)	Contract is in place with Microsoft Azure, who appropriate hold security credentials: ISO 27001.	Phil Burke, Head of IS Completed	Dr Alan Quirk, Head of Clinical Audits and Research
	Only named RCPsych staff will have access to Microsoft Azure via remote desktop. All access will be logged	Phil Burke, Head of IS Completed	Dr Alan Quirk, Head of Clinical Audits and Research
	Identifiable data will be retained as per Section 251 approval, with any extension to this requiring revised Section 251 approval.	Philippa Nunn Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research

Datasets shared by email	All shared datasets are password protected.	Philippa Nunn Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research
	Data emailed are made anonymous. No identifiable information will be included in the datasets when emailed.	Philippa Nunn Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research
Laptop containing pseudonymous data that is lost or stolen.	Only RCPsych approved laptops are used with appropriate security protections. No identifiable data are stored on laptops.	Philippa Nunn Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research
Data (pseudonymous or identifiable) accessed by unauthorised staff at RCPsych	Pseudonymous datasets are stored on secure sharepoint with restricted access to project folders. Computer/laptop terminals time-out and require password access. Identifiable data are stored on Microsoft Azure servers. Only named RCPsych staff have access via remote desktop. All access is logged.	Phil Burke, Head of IS Completed	Dr Alan Quirk, Head of Clinical Audits and Research
Sensitive data are collected on thousands of service users for the audit. Pseudonymous versions of the datasets are	Pseudonymous datasets are stored on secure SharePoint with restricted access.	Phil Burke, Head of IS Completed	Dr Alan Quirk, Head of Clinical Audits and Research
	Policy is to review retention	Philippa Nunn Programme Manager	Dr Alan Quirk, Head of Clinical

copied across software files retained for long-term statistical analysis	of datasets annually.	Ongoing	Audits and Research
	After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Philippa Nunn Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research
	Identifiable datasets are stored on Microsoft Azure servers. Only named RCPsych staff will have access to these. All access is logged. Identifiable data will be stored for the period granted by Section 251 approval.	Phil Burke, Head of IS Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research
Sensitive data held on third party servers (Crown Informatics LTD)	Contract is in place with Crown Informatics LTD, who hold appropriate security credentials.	Philippa Nunn Programme Manager Complete	Dr Alan Quirk, Head of Clinical Audits and Research
	Only RCPsych staff have access to the raw data on Crown Informatics LTD. Teams will have access to their own pseudonymous data using a secure username,	Philippa Nunn Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research

	password and two-factor authentication process. All other data available to teams will be aggregated.		
	The NAED team will request data are deleted from Crown Informatics LTD servers once no longer required.	Philippa Nunn Programme Manager Ongoing	Dr Alan Quirk, Head of Clinical Audits and Research

Step seven: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any Data Protection concerns that may arise in the future?

Action to be taken	**Date for completion of actions**	**Responsibility for action**
NAED team will request Crown Informatics LTD and Microsoft Azure to delete data retained, once no longer required.	Ongoing	Programme Manager
Contract is in place with Crown Informatics LTD and Microsoft Azure who hold appropriate security credentials.	Completed	Programme Manager/ Head of IS
All shared datasets are password protected.	Ongoing	Programme Manager
Only RCPsych approved laptops are	Completed	Head of IS

used with appropriate security protections		
Data emailed are made anonymous. No identifiable information will be included in the datasets when emailed.	Ongoing	Programme Manager
Pseudonymous datasets are stored on secure SharePoint with restricted access to project folders. Computer terminals/ RCPsych laptops time-out and require password access.	Completed	Programme Manager
Policy is to review retention of datasets annually.	Ongoing	Programme Manager
After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Ongoing	Programme Manager
Identifiable data will be stored for the period allowed according to Section 251 approval. Any retention past this date will require further Section 251 approval.	Ongoing	Programme Manager

Annex 1

Primary contact for advice and guidance

Richa Sharma
Head of Membership Services and Faculties – Data Protection Officer
richa.sharma@rcpsych.ac.uk
020 3701 2589

Annex 2

The data protection principles and relevant questions

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the General Data Protection Regulation, Data Protection Act 2018 or other relevant legislation, for example the Human Rights Act.

Personal data shall be:

1. **processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');**

    a) Have you identified the purpose of the project?

    b) How will you tell individuals about the use of their personal data?

    c) Do you need to amend or create a new privacy notice/s?

    d) Have you established which conditions for processing apply?

    e) If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

    f) If your organisation is subject to the Human Rights Act, you also need to consider:

    g) Will your actions interfere with the right to privacy under Article 8?

    h) Have you identified the social need and aims of the project?

    i) Are your actions a proportionate response to the social need?

2. **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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');**

    a) Does your project plan cover all of the purposes for processing personal data?

b) Have you identified potential new purposes as the scope of the project expands?

c) Consider using the Data Categories table at Annex 4 to help you identify the purposes of your collection/processing – this may help you evaluate the scope of the data required for your project.

3. **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');**

   a) Is the quality of the information good enough for the purposes it is used?

   b) Which personal data could you not use, without compromising the needs of the project?

4. **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 ('accuracy');**

   a) If you are procuring new software does it allow you to amend data when necessary?

   b) How are you ensuring that personal data obtained from individuals or other organisations is accurate?

5. **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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');**

   a) What retention periods are suitable for the personal data you will be processing?

   b) Are you procuring software that will allow you to delete information in line with your retention periods?

6. **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 ('integrity and confidentiality').**

    a) Do any new systems provide protection against the security risks you have identified?

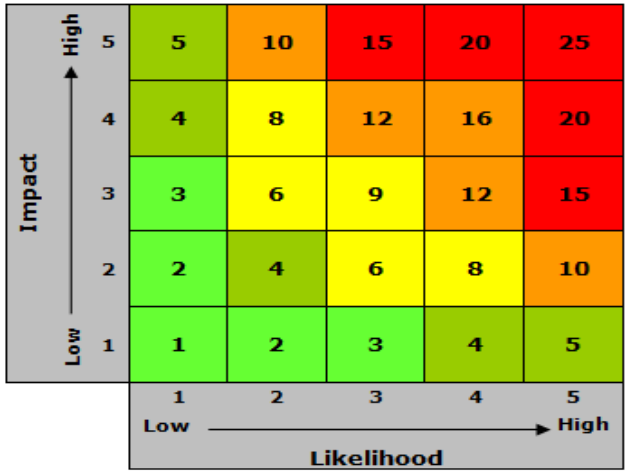
    b) What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Annex 3

Risk and Issues Log

Risk No	Risk Description	Likeli-hood	Severity of Impact	Raw Risk Score	Mitigation	Likelihood	Severity of impact	Residual Risk	Owner

1-3	Low likelihood & low severity of impact
4-5	Low / medium likelihood & low / medium severity of impact
6-9	Medium likelihood & medium severity of impact
10-16	Medium / high likelihood & medium / high severity of impact
15-25	High likelihood & high severity of impact



NAED DPIA review date: July 2025
Next review due: March 2026
RCPsych DPIA Template September2020 V3.0

Annex 4

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name			
NHS number			
Address			
Postcode			
Date of birth			
Date of death			
Age			
Sex			
Marital Status			
Gender			
Living Habits			
Professional Training / Awards			
Income / Financial / Tax Situation			
Email Address			
Physical Description			
General Identifier e.g. Hospital No/Paris ID			
Home Phone Number			
Online Identifier e.g. IP Address/Event Logs			
Website Cookies			
Mobile Phone / Device No			
Device Mobile Phone / Device IMEI No			
Location Data (Travel / GPS / GSM Data)			
Device MAC Address (Wireless Network Interface)			
Sensitive Personal Data			

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Physical / Mental Health or Condition			
Sexual Life / Orientation			
Family / Lifestyle / Social Circumstance			
Offences Committed / Alleged to have Committed			
Criminal Proceedings / Outcomes / Sentence			
Education / Professional Training			
Employment / Career History			
Financial Affairs			
Religion or Other Beliefs			
Trade Union membership			
Racial / Ethnic Origin			
Biometric Data (Fingerprints / Facial Recognition)			
Genetic Data			
Use of Mental Health Legislation/DoLS etc.			
Care Data including interventions, procedures, surgery etc.			
Spare			

Document Information (Office use only)

Title of document	Data Protection Impact Assessment
Version number	3
Type of document	Template for Assessment
Purpose of document	To capture the impact of project related data collection including pseudonymised, special category (sensitive), healthcare, social care, financial (this list is not exhaustive).
Target audience	All College staff and contractors
Distribution	Intranet (electronic)
Consultation	Interim Director of Information Services. GDPR Project Steering Group.
Approved by	Richa Sharma
Date of approval	2 September 2020
Author	Kathryn Campling GDPR Consultant
Review date	2 years or sooner is required

Document Control (Office use only)

Version Number	Reason for Change	Description of Change	Date of Change	Author
Draft	Original draft	Creation	June 2018	Kathryn Campling GDPR Consultant
V1.1	Amendments to include Table of contents, cover page, document control, tables and risk register annex 3	Updates	June 2018	Susie Griffin GDPR Project Manager
V2	Acceptance of all comments and update of 'approved by' and 'date of approval.'	Formatting	January 2019	Rebecca Danks Committee Administrator & GDPR Project Coordinator
V3	Reviewed following staff feedback	Review	September 2020	Rebecca Danks Senior Committee Officer