

DATA PROTECTION IMPACT ASSESSMENT - Digital Education Health & Care Plan Platform V1.3

Reference number: DPIA-515

Author: Neil Brettell
Email: Neil.Brettell@nottinghamcity.gov.uk

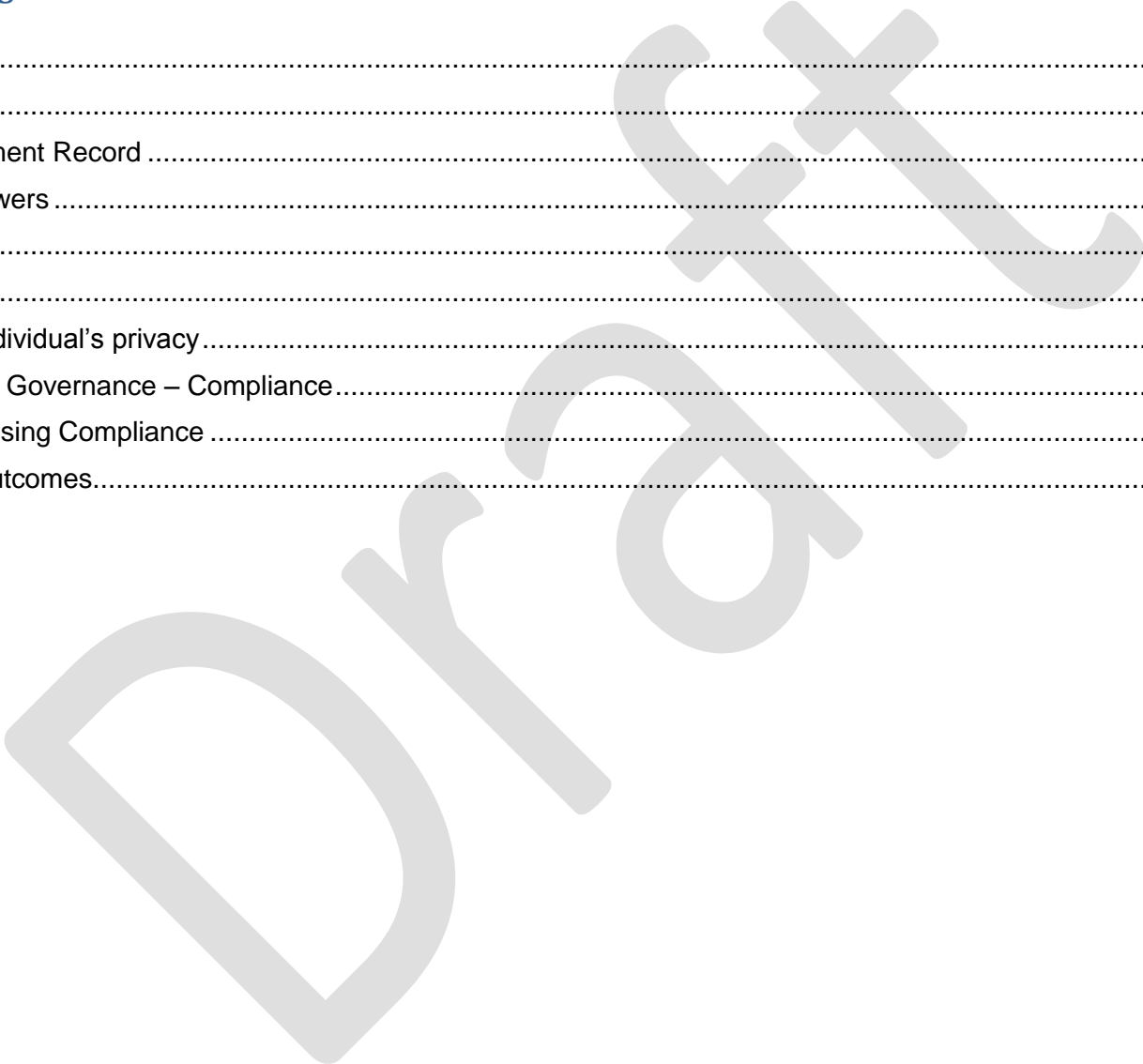
DATA PROTECTION IMPACT ASSESSMENT

When to complete this template:

Start to fill out the template at the beginning of any major project involving the use of personal data, or, where you are making a significant change to an existing process that affects personal data. Please ensure you update your project plan with the outcomes of the DPIA.

Table of Contents

- 1. Document Control 4
 - 1. Control details 4
 - 2. Document Amendment Record 4
 - 3. Contributors/Reviewers 4
 - 4. Glossary of Terms 4
- 2. Screening Questions 5
- 3. Project - impact on individual's privacy 7
- 4. Legal Framework and Governance – Compliance 13
- 5. Personal Data Processing Compliance 15
- 6. Sign off and record outcomes 23



1. Document Control

1. Control Details

Author of DPIA:	Neil Brettell
Owner of project:	Neil Brettell
Contact details of Author:	Neil.Brettell@nottinghamcity.gov.uk

2. Document Amendment Record

Issue	Amendment Detail	Author	Date	Approved
V1.0	Initial draft	Neil Brettell		
V1.1	Comments and amendments on initial draft	Jeremy Lyn-Cook		

3. Contributors/Reviewers

Name	Position	Date
Neil Brettell	Acting Head of Service SEND & Vulnerable Pupils	07.02.2024
Jeremy Lyn-Cook	Information Policy Specialist	


4. Glossary of Terms

Term	Description
EHCP	Education Health and Care Plan
LA	Local Authority
SEND	Special Educational Needs & Disability
PCF	Parent Carer Forum

Author: Neil Brettell
 Email: jeremy.lyncook@nottinghamcity.gov.uk

2. Screening Questions

1. Does the project involve personal data? Yes	If 'Yes', answer the questions below. If 'No', you do not need to complete a DPIA but make sure you record the decision in the project documentation.
2. Does the processing involve any of the following data: medical data, ethnicity, criminal data, biometric data, genetic data and any other special/ sensitive data?	Yes
2. Does the processing involve any systematic or extensive profiling?	Yes
3. Does the project involve processing children's data or other vulnerable citizen's data?	Yes
4. Does the processing involve decisions about an individual's access to a product, service, opportunity or benefit that is based on any evaluation, scoring, or automated decision-making process?	Yes
5. Does the processing involve the use of innovative or new technology or the novel application of existing technologies?	No
6. Does this project involve processing personal data that could result in a risk of physical harm in the event of a security breach?	Yes
7. Does the processing combine, compare or match data from multiple sources?	Yes
8. Does the project involve processing personal data without providing a privacy notice?	No
9. Does this project process data in a way that tracks on line or off line location or behaviour?	No
10. Will the project involve using data in a way it has not been used before?	No
11. Does the project involve processing personal data on a larger scale?	Yes
12. Will the project involve processing data that might prevent the Data Subject from exercising a right or using a service or entering into a contract?	No
If you answered 'Yes' to any <u>two</u> of the questions above, proceed to Question 3 below. If not seek advice from the DPO as you may not need to carry out a DPIA.	

<u>Project Title:</u> Implementation of a Digital Education Health & Care Plan Platform	
<u>Team:</u> SEN Team	
<u>Directorate:</u> People	
<u>DPIA Reference number:</u> <i>DPIA-515</i>	
<u>Has Consultation been carried out?</u>	
Yes. This proposal is as a result of a recommendation from the Department for Education, however, consultation has been carried out with Nottingham City's Parent Care Forum, via their PCF board.	
1. DDM attached?	Yes – OEDM attached  operational-executive -decision-making-forr
2. Written evidence of consultation carried out attached?	No
3. Project specification/ summary attached?	Not currently available
4. Any existing or previous contract / SLA / processing agreement attached?	Not currently available
5. Any relevant tendering documents attached?	Not currently available
6. Any other relevant documentation attached?	Yes. See OEDM above.

3. Project - impact on individual's privacy

Issue	Questions	Examples	Yes/No	Initial comments on issue & privacy impacts
Purpose and means		Profiling, data analytics, Marketing. Note: The GDPR requires a DPIA to be carried out where there is systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling, and on which decisions about individuals are based.		
	Please give a summary of what your project is about (<i>you can also attach or embed documents for example a project proposal</i>).		Please refer to attached OEDM for full description.	Summary: The LA is required to undertake EHC needs assessment and maintain EHCP's for pupils with SEND requiring provision by way of an EHCP. This project is to procure and set up a digitised EHC platform that supports the management of application data. The type of data being processed and data subjects does not change because of this project.
	<p>Aims of project</p> <p>Explain broadly what the project aims to achieve and what types of processing it involves.</p>		A transfer from a current system which utilises electronic document storage to a digital platform which will support the EHCP process from end to end; from request for assessment to EHC Plan and it's review. The digital platform will support engagement, contribution and collaboration on EHC need assessments, plans and reviews.	<p>The project will establish a digital portal enabling applicants (as specified in Section 36 Children & Families Act 2014 (i.e., a "child's parent, the young person or a person acting on behalf of a school or post-16 institution to create and account and view and track applications and data available to them.</p> <p>Currently, partner agencies send EHC assessments to NCC by via email or hard copy. Electronic data is stored on NCC network drives. Hard copy information requires scanning and manual saving of documentation.</p>
<p>Describe the nature of the processing</p> <p>How will you collect store and delete data? Will you be sharing with anyone? You might find it useful to refer to a flow diagram</p>			All data will be processed via a secure online platform hosted by the software provider. Professionals and applicants will have access to their account, with applicants able to transparently view the progress of their application, and professionals able to see report requests, prompts and copies of historic reports they have submitted. The software provider will be established via a commissioning/procurement process. The provider will host software to securely receive and store the personal data. Personal data includes personal	

	<p>or another way of describing data flows. What types of processing identified as likely high risk are involved? Who will have access to the project personal data, how is access controlled and monitored and reliability of staff assessed? Will data be separated from other data within the system?</p>		<p>demographic information and special category information, specifically around a pupils Special Education Needs, Social Care Needs and Health Needs. Currently, this data is transferred by email. There is a high risk of errors using this transfer method which is not desirable given the special category data being processed.</p> <p>Each data subject requires their own account, profile to enable complete separation from other data subjects. There is a requirement to be able to collate reports from all data subjects, and this will be anonymised information.</p> <p>A data sharing agreement designed by Nottingham City LA is signed by the applicant upon application.</p>
	<p>Privacy Implications</p> <p>Can you think of any privacy implications in relation to this project? How will you ensure that use of personal data in the project is limited to these (or “compatible”) purposes?</p>		<p>No.</p> <ul style="list-style-type: none"> • NCC shares too much information about individuals in the EHCP process. • NCC does not establish appropriate contractual arrangements with the platform provider. • Personal information is processed by the provider outside the UK / EEA.
	<p>New Purpose</p> <p>Does your project involve a new purpose for which personal data are used?</p>		<p>No.</p> <p>No. The project is to manage data in a different way to how it is currently managed.</p>
	<p>Consultation</p> <p>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 in NCC? Do you plan to consult</p>		<p>Yes.</p> <p>Consultation has been made with parent carer forum to seek views of parents of disabled children and young people, as well as young people themselves. Consultation has also been made with stakeholder schools and Integrated Care Board (ICB). Views collected were in favour of moving to a digitised system. PCF raised concern around access to digital platforms for families in digital poverty and professional stakeholders, requested that software systems are the same as neighbouring LA's to avoid having to navigate two different software</p>

	Information security experts, or any other experts?			packages. An Equality Impact Assessment is completed to address the PCF concerns around digital poverty.
Individuals (data subjects)	Will the project:	Expanding customer base; Technology which must be used by individuals; Hidden or complex uses of data; Children's data		
	Affect an increased number, or a new group, or demographic of individuals (to existing activities)?		No.	
	Involve a change to the way in which individuals may be contacted, or are given access to services or data? Are there any areas of public concern that you should factor in?		Yes.	See above reference to consultation. It is important to note, that by law the LA cannot limit service users' route of application. Therefore, whilst the majority of applicants will use a digital platform, traditional application methods (including paper, but more commonly email with attachments) will still remain available to those who wish to access them.
	Affect particularly vulnerable individuals, including children?		Yes.	All children and young people applying may have an SEN and disability and would therefore be considered a vulnerable group.
	Give rise to a risk that individuals may not know or understand how their data are being used?		No.	This process allows service users to see live updates of their applications and gives them access to their personal data that is being shared by professionals. This project gives applicants greater access to their personal data than current systems.
Parties	Does the project involve:	Outsources service providers; Business partners; Joint ventures		
	The disclosure of personal data to new parties?		Possibly.	Health and Social Care professionals.
	The involvement of sharing of personal data between multiple parties?		Yes.	As part of the statutory regulations, we are required as part of an EHC needs assessment to seek assessment and advice from multiple professionals.

Data categories	Does the project involve:	Special personal data; Biometrics or genetic data; Criminal offences; Financial data; Health or social data; Data analytics: Note: the GDPR requires a DPIA to be carried out where there is processing on a large scale of special categories of data or of data relating to criminal convictions and offences		
	The collection, creation or use of new types of data?		No.	
	Use of any special or privacy-intrusive data involved? <ul style="list-style-type: none"> • Political opinions • Religious beliefs or philosophical beliefs • Trade union membership • Genetic data • Biometric data • Sexual life • Prosecutions • Medical data • Criminal data (Criminal data processing, i.e. criminal convictions, etc. also has special safeguards under Article 10)		Yes.	The data being stored may include: Religious beliefs Genetic data Sexual Orientation Prosecution/Criminal Data Medical Data
	New identifiers, or consolidation or matching of data from multiple sources? (For example a unique reference number allocated by a new management system)		Yes.	As a software platform is yet to be commissioned this is unknown, but a specification requirement is that each application (pupil) has their own unique identifier.

Technology	New solutions:	Locator or surveillance technologies; Facial recognition; Note: the GDPR requires a DPIA to be carried out in particular where new technologies are involved (and if a high risk is likely)		
	Does the project involve new technology that may be privacy-intrusive?		No.	
Data quality, scale and storage	Data:	New data		
	Does the project involve changes to data quality, format, security or retention? What are the benefits of the processing? i.e. will the new system have automatic retention features? Will the system keep the information in a safer format etc.?		Yes	Information is transferred via an online platform. Users have secure log in details and will only be able to access data sent to them. This offers greater security than current systems where we see frequent data handline errors normally by emails being sent to an incorrect recipient. Professional users only have access to reports that they submit and any reports that we may be required to send to them, for example a final copy of the EHCP. They will also be able to see requests for reports issued from an administrator in the SEN Team. Applicants have access to all information held about them, there is an ability to restrict certain information from applicants e.g. for safeguarding purposes, but the general idea is for a digitised platform to improve transparency and communication.
	Does the project involve processing data on an unusually large scale?		Yes	Data will be held for an estimated 2000-3000 pupils.
Monitoring, personal intrusion	Monitoring:	Surveillance; GPS tracking; Bodily testing; Searching; Note: the GDPR requires a DPIA to be carried out where the project involves systematic monitoring of a publicly accessible area on a large scale		
	Does the project involve monitoring or tracking of individuals or activities in which individuals are involved?		Yes.	The project will support with the educational reviews of pupils with EHCPs.

	Does the project involve any intrusion of the person?		No.	
Data transfers	Transfers	Transfers outside the EEA		
	Does the project involve the transfer of data to or activities within a country that has inadequate or significantly different data protection and privacy laws?		Possibly.	Where the data is processed will depend to some extent on who wins the tender. The contract will restrict or prohibit processing data outside the UK/EEA without NCC consent and appropriate safeguards.

Draft

4. Legal Framework and Governance – Compliance

Ref.	Question	Response	Further action required (and ref. to risk register as appropriate)
1. Applicable laws and regulation			
1.1	Which data protection laws, or laws which impact data protection and privacy, will be applicable to the project?	<ul style="list-style-type: none"> • UK General Data Protection Regulation • Data Protection Act 2018 • Human Rights Act 1998 	EHCP's are only available to residents of England.
1.2	Are there any sector-specific or other regulatory requirements or codes of practice, which should be followed?	<p>The Children Act 2004 (the Act), as amended by the Children and Social Work Act 2017.</p> <p>Children and Families Act 2014</p> <p>Education Act 1999.</p> <p>SEN code of Practice</p>	
2. Organisation's policies			
2.1	Is the project in compliance with the organisation's information management policies and procedures (including data protection, information security, electronic communications)?	Yes.	

2.2	Which policy requirements will need to be followed throughout design and implementation of the project?	Data Protection Policy Information Security Policy Records Management Policy	
2.3	Are any changes/updates required to the organisation`s policies and procedures to take into account the project? Note: new requirements for “Accountability” under the GDPR, including record-keeping, DPOs and policies	No.	
3. Training and roles			
3.1	Will any additional training be needed for staff in relation to privacy and data protection matters arising from the project?	No.	

5. Personal Data Processing Compliance

Ref.	Question	Response	Further action required (and ref. to risk register as appropriate)
1. Personal Data Processing			
1.1	Which aspects of the project will involve the processing of personal data relating to living individuals?	System testing and once the project is live ongoing management of EHCP personal data.	
1.2	Who is/are the data controller(s) in relation to such processing activities?	Nottingham City Council Academy Trusts and schools, Nursery, Private Voluntary Institutes and post 16 settings. This process covers data transfers for pupils aged 0-25. Independent Schools and unregistered alternative provisions. Integrated Care Board (ICB) and NHS Trusts Independent professional therapists and psychologists.	
1.3	Who is/are the data processor in relations to such processing activities?	The platform provider.	
2. Fair and Lawful processing - GDPR Articles 5(1)(a), 6, 9, 12, 13			
2.1	Which fair processing conditions are you relying on? GDPR: Article 6(1) (legal basis for processing) and, for sensitive personal data, Article 9(2).	6(1). Choose at least one of the following for personal data, usually (e) -(Cross out the rest) a) Consent b) Performance of contract c) Legal obligation d) Vital interests e) Public interest / exercise of Authority 9(2) Choose at least 1 for special data- usually g (cross the rest out) a) Explicit consent b) Employment / social security /	

- social protection obligations
- c) Vital interests
- d) Non-profit bodies
- e) Processing made public by data subject
- f) Legal claims
- g) **Substantial public interest**
- h) **Health, social care, medicine**
- l) Public interest for public health
- j) Archiving, statistics, historical research

For any criminal Data

Comply with Article 10 if it meets a condition in Part 1, 2 or 3 of Schedule 1.

- Employment, social security and social protection
- Health and social care purposes
- Public health
- Research

Substantial public interest:

- Statutory and government purposes
- Equality of opportunity and treatment
- Racial and ethnic diversity at senior levels of organisations
- Preventing or detecting Unlawful Acts
- Protecting the public against dishonesty etc
- Regulatory requirements relating to unlawful acts and dishonesty etc
- Journalism etc in connection with unlawful acts and dishonesty etc
- Preventing fraud
- Suspicion of terrorist financing or money laundering
- Counselling

		<ul style="list-style-type: none"> ● Safeguarding of children and of individuals at risk ● Safeguarding of economic well-being of certain individuals ● Insurance ● Occupational pensions ● Political parties processing ● Disclosure to elected representatives ● Informing elected representatives about prisoners <p>Additional Conditions</p> <ul style="list-style-type: none"> ● Consent ● Vital interests ● Personal data in the public domain ● Legal claims ● Judicial Acts 	
--	--	--	--

Note: different conditions may be relied upon for different elements of the project and different processing activities. Also, the scope of special category data is wider under the GDPR, and in particular includes genetics & biometric data, and sexual orientation.

2.2	How will any consents be evidenced and how will requests to withdraw consent be managed?	NCC is not relying on consent as the basis for processing personal information. Consent in relation to set up/activation of the online portal account will be managed via the portal.	
-----	--	---	--

Note: new requirements for obtaining and managing consents within the GDPR.

2.3	Is the data processing under the project covered by fair processing information already provided to individuals or is a new communication needed (see also data subject rights below)?	Currently, this is covered by privacy statements in the application form and parents/carers read and sign up to the information. The privacy materials will need to be uploaded to the electronic platform.	
-----	--	---	--

Note: more extensive information required under the GDPR than under current law, and new requirements on how such information is provided. Also a general principle of “*transparency*”. It is important to assess necessity and Proportionality

2.4	If data is collected from a third party, are any data protection arrangements made with such third party?	No. NCC be relying on partners obligations under the Code of Practice to get them to provide information. See Code of Practice and CAFA 2014	
2.5	Is there a risk of anyone being misled or deceived?	No.	
2.6	Is the processing “fair” and proportionate to the need’s and aims of the projects?	Yes.	
2.7	Are these purposes clear in privacy notices to individuals? (see above)	Yes.	
3. Adequate, relevant and not excessive, data minimisation - GDPR Article 5(1)(c)			
3.1	Is each category relevant and necessary for the project? Is there any data you could not use and still achieve the same goals?	Yes – all categories required.	
Note: GDPR requires data to be “limited to what is necessary” for the purposes (as well as adequate and relevant).			
3.2	Is/can data be anonymised (or pseudonymised) for the project?	No.	
4. Accurate and up to date - GDPR Article 5(1)(d)			
4.1	What steps will be taken to ensure accurate data is recorded and used?	Each applicant will be assigned a unique user name, so data is only transferred relevant to them. There are 2 x decision making panels that oversee reports being issued, and we now undertake termly quality assurance of Education Health and Care plans to improve report contents.	
For example: checks when receiving/sending information from/to third parties, or transcribing information from oral conversations or handwritten documents, any automatic checks on information not meeting certain criteria.			
4.2	Will regular checks be made to ensure project data is up to date?	Yes – SEN Team complete annual review of all pupils with identified needs.	
5. Data retention - GDPR Article 5(1)(e)			
5.1	How long will personal data included within the project be retained?	Data management arrangements continue to be maintained and are not affected by this project.	

		Retention time should DOB plus 35 years as set out in the Information Asset Register. See Information Asset Register (nottinghamcity.gov.uk)	
5.2	How will redundant data be identified and deleted in practice? Consider paper records, electronic records, equipment?	Via annual reviews of pupils. Data management is subject to the policy Information Asset Register (nottinghamcity.gov.uk) .	
5.3	Can redundant data be easily separated from data which still need to be retained?	Yes.	
6. Data subject rights - GDPR Articles 12 to 22			
6.1	Who are the relevant data subjects?	Applicants for EHC needs assessments, or those with EHCP's.	
6.2	Will data within the project be within the scope of the organisation's subject access request procedure?	Yes.	
6.3	Are there any limitations on access by data subjects?	No.	
6.4	Is any data processing under the project likely to cause damage or distress to data subjects? How are notifications from individuals in relation to damage and distress managed?	No. However, if any notifications are received they will be handled by the SEND Team and Information Compliance in line with NCC's existing corporate information rights mechanisms.	
6.5	Does the project involve any direct marketing to individuals? How are requests from data subjects not to receive direct marketing managed?	No.	
6.6	Does the project involve any automated decision making? How are notifications from data subjects in relation to such decisions managed?	No.	
6.7	How will other rights of data subjects be addressed? How will security breaches be managed?	These rights will be processed Information Compliance at Nottingham City Council. All breached will be dealt with by Information Compliance and the Data Protection Officer.	

7. Data Security - GDPR Articles 5(1)(f), 32

For example:

- **Technology:** encryption, anti-virus, network controls, backups, DR, intrusion detection;
- **Physical:** building security, clear desks, lock-leads, locked cabinets, confidential waste;
- **Organisational:** protocols on use of technology, asset registers, training for staff, pseudonymisation, regular testing of security measures.

Describe the source of risk and nature of potential impact on the individuals. Include associated compliance and corporate risks as necessary -What security measures and controls will be incorporated into or applied to the project to protect personal data? Consider those that apply throughout the organisation and those which will be specific to the project. N.B Measures that are appropriate to the nature of the data and the harm which may result from a security breach	Likelihood of harm Remote, Possible or Probable	Severity of harm Minimal, Significant or Severe	Overall Risk Low, Medium or High
<ul style="list-style-type: none"> • Risk of personal information being shared incorrectly or viewed by someone who should not have access. 	Possible	Significant	High
<ul style="list-style-type: none"> • NCC does not establish appropriate contractual arrangements with the platform provider. 	Possible	Significant	High
<ul style="list-style-type: none"> • Personal information is processed by the provider outside the UK / EEA. 	Possible	Significant	High

Identify measures to Reduce Risk- Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk that you have identified

Risk	Options to reduce or eliminate risk	Effect on risk Eliminated/ Reduced or Accepted	Residual risk Low/Medium/High	Measures approved Yes/No

Risk of personal information being shared incorrectly or views by someone who should not have access.	NCC is under is a statutory duty to seek and share subject data with professionals across health and social. However, the new platform will reduce the risk of unauthorised access to data.	Reduced.	Medium.	Yes.
NCC does not establish appropriate contractual arrangements with the platform provider.	NCC will put in place a contract containing appropriate data processing terms.	Reduced.	Low.	Yes.
Personal information is processed by the provider outside the UK / EEA.	The contract will restrict or prohibit processing data outside the UK/EEA without NCC consent and appropriate safeguards.	Reduced.	Low.	Yes.

8. Data processors - GDPR Article 28 & direct obligations in other articles

8.1	Are any data processors involved in the project?	Yes. The new platform provider.	
8.2	What security guarantees do you have?	The contract will establish data management rules under which an external provider will need to operate.	
For example: specific security standards or measures, reputation and reviews			
8.3	Please attach the processing agreement	ADD contract with new platform provider.	
For example: security terms, requirements to act on your instructions, regular audits or other ongoing guarantees Note: new requirements for the terms of contracts under the GDPR (much more detailed than current law).			
8.4	How will the contract and actions of the data processor be monitored and enforced?	Power to audit under the processing agreement.	

8.5	How will direct obligations of data processors be managed?	Under the processing agreement	
Note: New direct obligations for processors under the GDPR, including security, data protection officer, record-keeping, international data transfers.			
For example: fair & lawful, lawful purpose, data subject aware, security, relevance.			
9. International data transfers - GDPR Articles 44 to 50			
9.1	Does the project involve any transfers of personal data outside the European Union or European Economic Area?	Where the data is processed will depend to some extent on who wins the tender. The contract will restrict or prohibit processing data outside the UK/EEA without NCC consent and appropriate safeguards.	
9.2	What steps are taken to overcome the restrictions?	See above.	
For example: Safe Country, contractual measures, binding corporate rules, internal assessments of adequacy			
Note: GDPR has similar methods to overcome restrictions as under current law, but there are differences to the detail and less scope for an “own assessment” of adequacy.			
10. Exemptions			
10.1	Will any exemptions for specific types of processing and/or specific DP requirements be relied upon for the project?	No	
For example: crime prevention, national security, regulatory purposes			
Note: Exemptions under the GDPR to be assessed separately and may be defined within additional EU or UK laws.			

6. Sign off and record outcomes

Item	Name	Date
Measures approved by: (project owner) This must be signed before the DP can sign off on the DPIA.		
Residual risks approved by: (If accepting any residual high risk, consult the ICO before going ahead)		
DPO advice provided: (DPO should advise on compliance, measures and whether processing can proceed)		
Summary of DPO advice:		
DPO advice accepted or overruled by		If overruled, you must explain your reasons
Comments:		
IT Security Officer: Where there are IT security issues		
IT Officer comments:		
SIRO Sign off: (For major projects)		
Consultation responses reviewed by:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA