Data Protection Impact Assessment for the National Neonatal Audit Programme (England, Scotland, and Wales)

Document control:

	Name and role	Contact details
Document Completed by	Rachel Winch, NNAP Project Manager	rachel.winch@rcpch.ac.uk 020 3861 1910
Data Protection Officer name	Adele Picken, Head of Information Governance	Adele.Picken@rcpch.ac.uk 020 7092 6030
Document approved by (this should not be the same person that completes the form).	Adele Picken, Head of Information Governance	Adele.Picken@rcpch.ac.uk 020 7092 6030
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5143673	

Date Completed	Version	Summary of changes
23/11/2020	0.1	Draft as part of PIA meeting- following change to data flow
26/11/2020	0.2	JE edits to draft
27/11/2020	0.3	Further edits to draft by RCPCH Head of IG
04/12/2020	0.4	Update following CAG application and verification of storage
01/03/2021	0.5	Update following confirmation of section 251 approval and HSC-PBPP application
01/04/2021	0.6	Review by Head of Information Governance, RCPCH and further updates by RW in consultation with IS team.
01/04/2021	1.0	Head of Information Governance final review and sign off
28/03/2022	1.1	Annual review by NNAP PM Rachel Winch, to incorporate Scottish data flow and amendments to English and Welsh data flow under Section 251.
04/07/2022	1.2	Review and amendments by Rachel Winch (NNAP PM), and Adele Picken (Head of Information Governance).
01/08/2022	1.3	Amendments by Rachel Winch (NNAP PM) following HSC-PBPP feedback, with review by Adele Picken (Head of Information Governance).

Contents

Screening questions

Please complete the following checklist:

	Section	Yes or No	N/A	Comments
1.	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	N		
2	Does your project involve any sensitive information or information of a highly personal nature?	Y		
3.	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where there is an imbalance in the relationship between the position of the individual and the controller.	Y		
4.	Does your project involve any innovative use or applying new technological or organisational solutions? This could include biometric or genetic data, the tracking of individuals' location or behaviour?	N		
5.	Does your project match data or combine datasets from different sources?	N		
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	N		
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	Y		
8.	Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project?	Y		Existing project which undergoes a change in data flow as of 1 April 2021.

Data Protection Impact Assessment

This Data Protection Impact Assessment (DPIA) template and guide is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. This tool will help organisations which process personal data to properly consider and address the privacy risk that this entails.

DPIA can be used alongside existing project management and risk management methodologies.

Conducting a DPIA is now a legal requirement under the GDPR (General Data Protection Regulation) which will start on the 25th May 2018 and the new UK Data Protection Act. By completing a DPIA, this will help to ensure that your project is compliant with GDPR and UK data protection legislation. This document will be updated if further ICO guidance is published or there is change in legislation.

A DPIA is the basis of a "privacy by design" approach, to help meet privacy and data protection expectations of customers, employees and other stakeholders. A DPIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project.

Purpose and benefits of completing a DPIA

- A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.
- Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.
- The DPIA will help determine the appropriate controls needed to protect personal data i.e. technical, procedural and physical.
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a DPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.
- The ICO may often ask an organisation whether they have carried out a DPIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with Data Protection legislation.

Supplementary guidance

- Data Protection Impact Assessment under GDPR guidance
- ICO's conducting privacy impact assessments code of practice
- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing code of practice may help organisations to identify privacy risks associated with sharing personal data with other organisations.
- The ICO's codes of practice on privacy notices, as well as other more specific guidance, will also help an organisation to focus DPIAs on those issues.
- The Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The

Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

DPIA methodology and project information.

At what stage in the project did you conduct this DPIA? E.g. planning stage, changes to the existing project, in retrospect.

Upon changing the data flow to require the RCPCH to hold section 251 approval to receive data for England and Wales, HSC-PBPP approval to receive data for Scotland.

Describe the overall aim of the project and the data processing you carry out

The NNAP assesses whether babies admitted to neonatal units in England, Scotland and Wales receive consistent high-quality care. We identify areas for quality improvement in relation to the delivery and outcomes of care.

DPIA Consultation

We advise you to consult with as many relevant people as possible (both internal and external stakeholders**)** while conducting this assessment, consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. Consultation can take place at any point in the DPIA process and may include the project management team, Data Protection Officer, designers, IT provider, procurement team, data processors, communications team, patients, stakeholders, corporate governance and compliance teams, researchers, analysts, statisticians and senior management.

You must consult with the Data Protection Officer regarding the impacts on privacy. Please state below that you have.

If you decide against seeking the views of data subjects or their representatives e.g. this would be disproportionate or impracticable, then the justification must be made clear in the box below. In the box below name the stakeholder group, date consulted and how consulted. Please insert another box if you consulted with many different stakeholder groups.

Consultation for data flow change:

- Vice President for Science and Research
- RCPCH CEO
- RCPCH Director of Research and QI
- HQIP
- RCPCH Data Protection Officer
- Project Board have been informed following agreement of change in data flow.

General NNAP audit

RCPCH Data Protection Officer and Head of Information Governance, RCPCH

NNAP Project Board were consulted on the content of the fair processing/privacy notice leaflet (March/April 2018). There will be a review in a year at the end of the contract extension. The NNAP Project Board includes representatives from the following:

- NNAP Clinical lead (consultant neonatologist)
- Neonatal Nurses Association
- Neonatal trainees
- Parents
- Bliss charity
- Neonatal Critical Care Clinical Reference Group
- Neonatal Networks
- British Association of Perinatal Medicine
- The Neonatal Society
- Consultant neonatologists working in England, Scotland and Wales
- NNAP project team

Publishing your DPIA report

Publishing a DPIA report is not a legal requirement but you should consider publishing this report (or a summary or a conclusion) and you should send it to your stakeholders. Publishing the DPIA report will improve transparency and accountability, and lets individuals know more about how your project affects them. Though there may be a need to redact/remove sensitive elements e.g. information on security measures.

State in the box below if you are going to publish your DPIA. If so, please provide hyperlink to the relevant webpage if this has been done already or insert the date you intend to publish it.

Published on the NNAP pages of the RCPCH website, at: https://www.rcpch.ac.uk/resources/national-neonatal-audit-programme-transparency-open-data

Data Information Flows

Please describe how personal information is collected, stored, used and deleted. Use your data flow map and information asset register to help complete this section. Explain what personal information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. Completing this section can help identify potential 'function creep', unforeseen or unintended uses of the data for example data sharing. Please see NNAP data flow map: https://www.rcpch.ac.uk/resources/national-neonatal-audit-programme-transparency-open-data

Processing activity description	Type of data involved		Data flow	Controller/processor
Clinical data entered by neonatal units on BadgerNet system	Personal and Special Category data (identifiable)		Neonatal unit to Clevermed Ltd.	Data controller: NHS Trust/Health Board Data Processor: Clevermed Ltd
Clinical data stored by Clevermed Ltd. on BadgerNet system	Personal data and Special Category (identifiable)		None.	Data processor: Clevermed Ltd Data controller: NHS Trust/Health Board
Neonatal Dataset SQL Database created within the Clevermed Microsoft Azure environment containing full neonatal dataset extracted from BadgerNet (not accessible by RCPCH)	Personal data and Special Category (identifiable)		None.	Data processor: Clevermed Ltd Data controller: NHS Trust/Health Board
Patients opted out nationally removed from dataset by Clevermed (England only)	Personal data and Special Category (identifiable)		None.	Data processor: Clevermed Ltd Data controller: NHS Trust/Health Board
NNAP Database synchronised to a 'mirror' NNAP SQL server database on RCPCH Azure hosting infrastructure	Personal data and Special Category (identifiable)		Clevermed Ltd to RCPCH	Data processor: RCPCH Data controller: HQIP
(England and Wales) If NNAP data is to be linked or shared, the RCPCH send list of NHS numbers to NHSD for national opt out programme check	Personal data and Special Category (identifiable)		RCPCH to NHS Digital	Data processor: RCPCH Data controller: NHS Digital Data controller: HQIP

(England and Wales) NHSD send list of NHS numbers to RCPCH, removing any that have opted out under the national opt out	Personal data and Special Category (identifiable)		NHS Digital to the RCPCH	Data processor: RCPCH Data controller: NHS Digital Data controller: HQIP
(England and Wales) Opt outs removed and data cleaned.	Personal data and Special Category (identifiable)		None.	Data processor: RCPCH Data controller: HQIP
Quarterly neonatal unit reports shared with neonatal unit and respective networks only. Data quality and completeness episode lists shared with neonatal units responsible for the data.	Aggregated data (non-identifiable) Episode lists – Pseudonymised - BadgerNet ID (hospital identifier) only, no other patient identifiable information.		RCPCH to neonatal units and networks	Data processor: RCPCH Data controller: HQIP
Re-extracted, cleaned data used to develop tables and statistical outputs for NNAP reporting	Pseudonymised/ limited access deidentified becomes anonymised and aggregated data (non-identifiable)		RCPCH	Data processor: RCPCH Data controller: HQIP

Transferring personal data outside the European Economic Area (EEA)

If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries, or how the data is adequately protected).

Not applicable – data will not be transferred outside of the EEA.

Justification for collecting personal data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. In certain circumstances it may be unlawful to process information not described in the transparency information (privacy notice/fair processing material) which informs individuals how their personal data is being used.

It may not be necessary to process certain data items to achieve the purpose. They may be irrelevant or excessive leading to risk of non-compliance with the Data Protection Act.

In the tables below list and justify personal data items needed to achieve the lawful aim of a project that requires information on individuals and their personal characteristics. Insert as many more lines that you need. Work through the table of items and decide whether or not you should be collecting the information, examine each data field and decide if you need it.

There are two sections in the table below, one for personal data and one for personal sensitive data items.

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	N		
NHS number/CHI number	Y		BABY - Used as a baby's unique national identifier in a neonatal episode and will allow the RCPCH to de-duplicate the NNAP dataset, linking care episodes for a baby that may occur in multiple neonatal units and follow up care provided in other hospitals. MOTHER - Used as a mother's unique national identifier and ensures that twins, triplets and other multiple births can be identified as associated with a single mother which is important for certain NNAP audit measures.
Address	N		
Postcode	Y		Used to establish LSOA deciles (DataZone & SIMD in Scotland) derived through the postcodes so that deprivation will form one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Date of birth	Y		MOTHER - Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.

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]*
			BABY - Used as part of the criteria to derive the analysis for NNAP audit measures which have time-bound elements where the time between admission and delivery of the care process forms part of the success criteria, an example being "Does an admitted baby born at less than 32 weeks gestational age have a first temperature on admission which is both between 36.5–37.5°C and measured within one hour of birth?".
Date of death	Y		BABY - Used as part of the criteria to derive the analysis for the Mortality to discharge in very preterm babies audit measure which asks, "Does a baby born at less than 32 weeks gestational age die before discharge home, or 44 weeks post-menstrual age (whichever occurs sooner)?".
Age	Y		MOTHER – Calculated from date of birth. Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Sex	Y		Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Marital Status	N		
Gender	Y		Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Living Habits	Y		Smoking status for matching analysis
Professional Training / Awards	N		
Income / Financial / Tax Situation	N		
Email Address	N		
Physical Description	N		
General Identifier e.g. Hospital No	Y		Unique GUID to identify a single neonatal admission for an infant. The infant's EntityID is used to connect admission and demographic details to daily summary forms and other ad-hoc events recorded in relation to the infant (Rop Screenings, Sepsis screening, Developmental data, etc.).
Home Phone Number	N		
Online Identifier e.g. IP Address/Event Logs	N		
Website Cookies	N		
Mobile Phone / Device No	N		
Device Mobile Phone / Device IMEI	N		

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]*
No			
Location Data (Travel / GPS / GSM Data)	N		
Device MAC Address (Wireless Network Interface)	N		
Sensitive Personal Data			
Physical / Mental Health or Condition	Y		Of mother and baby. Used to compare outcomes for babies.
Sexual Life / Orientation	N		
Family / Lifestyle / Social Circumstance	Y		Smoking status or previous pregnancies, or index of deprivation (linked to postcode) for analysis.
Offences Committed / Alleged to have Committed	N		
Criminal Proceedings / Outcomes / Sentence	N		
Education / Professional Training	N		
Employment / Career History	N		
Financial Affairs	N		
Religion or Other Beliefs	N		
Trade Union membership	N		
Racial / Ethnic Origin	Y		Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Biometric Data (Fingerprints / Facial Recognition)	N		
Genetic Data	N		
Medical Treatment	Y		Required for analyses (steroids, magnesium sulphate etc)

Data quality standards for personal data

In the box below, describe how you will ensure that personal data is accurate and kept up to date.

The NNAP is an annual audit, in which new data is used every calendar year. During the audit year, the NNAP provides quarterly data quality reports of aggregated data and episode lists so that neonatal units and networks can check the quality of the data they submit to the audit.

Data quality and validation checks are carried out on the data prior to analysis for the national report.

Individual's rights

If your project uses personal data you must complete this section.

If your project uses personal data you must state how fairness and transparency will be achieved e.g. privacy notices on websites, posters, and leaflets. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to children should be in such a clear and plain language that the child / vulnerable person can easily understand.

In the box below, please define the way you have ensured that individuals are aware of the rights, if they request those rights how will they achieve them? For example if an individual requests a copy of their information held by you, describe how you would do this. You can insert any relevant policy or process guides in the appendix at the end of this document if they are not already available on your website. This section does not refer to the personal information held about your audit staff.

Please see NNAP parent information leaflet: https://www.rcpch.ac.uk/resources/national-neonatal-audit-programme-your-babys-information

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
Individuals are clear about how their personal data is being used.	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Not applicable.
Individuals can access information held about them	Included in the privacy notice.	If a parent makes an SAR on behalf of their child to NNAP we will forward this onto the Trust/Health Board providing their care. We have a specific procedure for dealing with rights requests in relation to clinical audits and this will be followed.	The personal data we hold about you is provided by your unit. We can let you know which categories of data we collect but you will need to contact your unit directly for a copy of your personal data as they are data controllers of your patient record.
Request erasure (right to be forgotten) in certain circumstances, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes	Included in the privacy notice.	As the data is being processed for a public interest, this right does not apply. If we receive a request, we will respond to this affect. Any requests relating directly to the patient record will be forwarded to the Trust/ Health Board. We have a specific procedure for dealing with rights	The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care.

		requests in relation to clinical audits and this is outlined in this procedure.	
Rectification of inaccurate information	Included in the privacy notice.	Forward the request to the Health Board/Trust who are data controller of the patient record. We have a specific procedure for dealing with rights requests in relation to clinical audits and this will be followed.	Any requests to amend or update your personal data should be sent to your unit as data controller. If we receive any requests, we will forward these to the unit.
Restriction of some processing	Included in the privacy notice.	Forward the request to the Trust /Health Board who are the data controller of the patient record. We have a specific procedure for dealing with rights requests in relation to clinical audits and this will be followed.	Any requests for restriction of processing should be sent to your NHS Trust/Health Board and they will inform us where applicable.
Object to processing undertaken on some legal bases	Included in the privacy notice.	Forward the request to the Trust/ Health Board who are the data controller of the patient record.	**Right to Erasure and Right to Object** The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you do not want your personal data to be used for future rounds of the NNAP, please let your neonatal unit know and they will remove you from the submission so that we don't receive the data. The Health Board providing your neonatal care will still retain your overall healthcare data.

Complain to the Information Commissioner's Office;	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units. Individual can contact the ICO directly with a complaint via the email provided on our privacy notice to them.	England and Wales: You do also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at casework@ico.org.uk if you have concerns about the way your baby's personal data are being handled. Scotland: You do also have the right to lodge a complaint with the Information Commissioner's Office (ICO) – Scotland at Scotland@ico.org.uk if you have concerns about the way your baby's personal data are being handled.
Withdraw consent at any time (if processing is based on consent)	Not applicable.	Not applicable.	Not applicable.
Data portability (if relevant)	Not applicable.	Not applicable. Data is not collected directly from the data subject, part of a contract or based on consent.	Not applicable.
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Healthcare Quality Improvement Partnership (HQIP) is the data controller of the National Neonatal Audit Programme and can also be contacted if you have any questions about how your information is being used for the audit. Please direct any queries for the Healthcare Quality Improvement Partnership Data Protection Officer to: communications@hqip.org.uk.
In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will protected (e.g. the recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	The NNAP does not share identifiable or pseudonymised data from Scottish services with others. Personal data shall not be transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
To know the legal basis under which their information is	Included in the privacy notice.	Published on our website, distributed	Processing is permitted under the UK General Data Protection

processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?		electronically to neonatal units. We are processing under schedule 6(e) and schedule 9(i) of UK GDPR.	Regulation (UK GDPR) on the following legal bases: • Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is justified through commissioning arrangements which link back to NHS England and the Welsh Government. • Article 9 (2) (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. This is justified as the NNAP aims to drive improvements in the quality and safety of care and to improve outcomes for patients. We also protect your privacy rights by providing you with the ability to choose for your data to not be included in the audit.
To know the purpose(s) for the processing of their information.	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	We use information about your baby's care to help neonatal units in England, Wales and Scotland to improve the care and outcomes for other babies.
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Not applicable	Not applicable- there is no statutory obligation for parents to provide their baby's data to the NNAP audit.	Not applicable
The source of the data (where the data were not collected from the data subject)	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Neonatal unit staff enter your baby's information onto a secure electronic record system named BadgerNet. All neonatal units share information from these

			electronic records with the National Neonatal Audit Programme (NNAP) project team within the RCPCH, via another processor, Clevermed Ltd, who manage the BadgerNet system used by neonatal units to record clinical data.
Categories of data being processed	Included in the privacy notice. Data dictionary.	Published on our website, distributed electronically to neonatal units. Full data dictionary published on our website.	Neonatal unit staff enter your baby's information onto a secure electronic record system named BadgerNet. All neonatal units share information from these electronic records with the National Neonatal Audit Programme (NNAP) project team within the RCPCH, via another processor, Clevermed Ltd, who manage the BadgerNet system used by neonatal units to record clinical data. This includes sensitive personal data, including NHS or CHI Number (Baby and Mother), Date and time of admission to neonatal care (Baby), Date and time of discharge from neonatal care (Baby), Date and time of birth (Baby), Date of death (Baby), Date of birth (Mother), Ethnicity (Mother), Gender (Baby), Postcode of usual address (Mother) and information about the care that mum and baby received and any related health conditions. The NNAP project team only uses the information for the purpose of the National Neonatal Audit Programme to monitor and try to improve standards of patient care.
Recipients or categories of recipients	Included in the privacy notice.	The College may receive data access requests. (England and Wales) Any requests to access data will require a completed DARs request form. For Scotland, no identifiable or pseudonymised data will be shared.	England and Wales: Data will only ever be shared in a pseudonymised format and only with the approval of HQIP. For HQIP to approve the request, the requestor must be able to demonstrate compliance with stringent data protection policies and arrangements and the aims of the research must be approved, as per HQIP's guidance to applicants. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory

			ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Scotland: The NNAP publishes data in anonymised, aggregated form. No individual babies are identified in any of our reports. The NNAP does not share identifiable or pseudonymised data from Scottish services with others.
The source of the personal data	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Neonatal unit staff enter your baby's information onto a secure system for electronic records. All neonatal units share information from these electronic records with RCPCH.
To know the period for which their data will be stored (or the criteria used to determine that period)	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	The NNAP team at the RCPCH acts as the data processor on behalf of HQIP, who are the data controllers for the NNAP data. The RCPCH will hold the NNAP data for as long as it is contracted to deliver the NNAP. All patient identifiable data will be deleted at the end of our contract. If HQIP commissions the RCPCH to deliver the NNAP under a new or extended contract, then the data will be retained by the RCPCH for the period of the new contract.
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	Not applicable.	Not applicable.	Not applicable.

Privacy Risks

Types of Privacy risks

- Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organisation), for example; failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regards to the individual's privacy.

In the box below insert the number of individuals likely to be affected by the project. This could be the number of unique patient records your project holds now and how many more records you anticipate receiving each year.

Each year, the NNAP includes information about approximately 100,000 babies. There is likely to be a small increase on this number each year.

Please complete the table below with all the potential risks to the Individuals of the information you hold on them, your corporate risks and compliance risks.

When completing the table you need to consider if:

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate and compliance risks

In the table, list the corporate risks to your organisation which could include reputational damage, loss of public trust, financial costs and data breaches. Below these, insert any compliance risks.

Possible corporate risks include:

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Examples of compliance risks include:

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the GDPR.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Managing Privacy and Related risks

There are many different steps you can take to reduce a privacy risk. For example

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Use your project plan and a detailed explanation of information flows to identify more precisely how a general risk may occur. For example, there may be particular points in a process where accidental disclosure is more likely to happen.

The DPIA actions should be added to into your project plan and risks added to your contract review documentation.

Privacy Risks and Actions Table

Please see appendix 2 for additional guidance on completing this table

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 -In significant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk OR Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Non-compliance with UK GDPR principle a- not having lawful grounds for processing. This could lead to a sanction by the ICO with a monetary fine and damage to RCPCH reputation	2	3	6	**Reduced**	The legal basis for using this information is that it allows us to carry out a task that is in the public interest. In respect of the NNAP the public interest is protected through ensuring that high standards and quality of neonatal care continue. In England, privacy rights are also protected by the National Opt Out programme which is applied to this data In this case, the legal bases for processing under UK GDPR are Article 6 (1) (e) and Article 9 (2) (i). This is outlined in the privacy notice and also included in the Section 251 application (England and Wales) and HSC-PBPP application (Scotland). The legal	We have informed data subjects via the privacy notice of the legal grounds for processing. We have also had this assessed as part of the CAG section 251 application (England and Wales) and HSC-PBPP application (Scotland). The accountability requirement is fulfilled by documenting this in the RCPCH IAR.	Already in place	NNAP Project team

					grounds for processing and the public interest argument are documented on the RCPCH Information Asset Register.			
Individuals have the right to be informed about how their data will be used including any push notifications or cookies if an online service. Failure to inform them can lead to inadequate consent (legal grounds for processing), sanctions by the ICO, fines and reputational damage.	2	3	6	**Reduced**	The privacy notice includes all the required information under the UK GDPR. This is on the website and circulated to participating neonatal units, who will be responsible for further dissemination. The privacy notice is aimed at parent/carers. There are no push notifications or cookies used on the system. Consent is not required for this processing activity.	The Privacy notice has been distributed to all neonatal units and is available on the RCPCH website so that it is easily accessible to all parent/carers of data subjects.	Complete	NNAP Project Team
Design by default- data minimisation, only retaining the information necessary for the specified purpose for which it is collected. The more data that is processed, the more risk there is data being compromised which can lead to sanctions by the ICO and reputational damage as well as data subject damage and distress. Principle c- data should be adequate and limited to what is necessary.	2	2	4	**Reduced**	The data dictionary will be reviewed and any changes signed off by the NNAP Project Board. Only this data will be extracted from Badgernet.	By considering each data category and providing justification, only the limited amount of data for the purpose of the audit will be collected where it is necessary.		NNAP Project Team
If data is not securely deleted, it is at risk of being lost, stolen or accessed without authorisation. This would be a breach of principle f of UK GDPR and could lead to a sanction by the ICO, a fine and reputational damage.	2	2	4	**Reduced**	A copy of the data will be segregated from other data on Badgernet and transferred to RCPCH. The data will be stored on a separate server, segregated from all other data and stored on its own designated server/area so	Data will be destroyed in line with NHS Digital guidelines. A certificate of destruction will provide detail of the destruction method used and evidence of		NNAP Project Team

					that it can easily be extracted and deleted when required. NHS guidelines will be followed for destruction. As part of the procurement process, the NNAP team will ensure that the data can be destroyed using multi pattern pass data wiping using a commercially licenced tool, not freeware, in line with NHS Digital guidelines. When deleted, a certificate of destruction will be completed to detail how the destruction has been undertaken.	destruction. By segregating the data, it will be possible to delete the data fully.		
If data is not securely transferred, it is at risk of being stolen, lost or damaged. This could lead to ICO sanctions, fines and reputational damage as well as substantial damage and distress to the data subjects if the information falls into the wrong hands.	2	3	6	**Reduced**	RCPCH IS and IG have been consulted on the data flow decisions to ensure secure transfer options are selected where required. A mirror instance of the NNAP dataset is created on the RCPCH Microsoft Azure server via SQL to SQL sync to the Clevermed Microsoft Azure server. A pseudonymised version of the NNAP data will be created within the RCPCH Azure environment and it is this pseudonymised version of the data that the NNAP project team will work with. Pseudonymised patient episode lists provided by the RCPCH to the responsible trust on a quarterly or monthly basis	By consulting experts, information security and information governance considerations will be incorporated.		NNAP team

					for the purposes of data quality and completeness checks. These patient lists will contain BadgerNetID and additional information about the status and completeness of data fields strictly limited to that required for purpose of ensuring data quality and completeness and will relate to patients cared for by that trust only. Patient episode lists will be provided alongside "quarterly reports", which are anonymised and aggregated results tables. The data flow has also been approved by CAG.			
If staff do not have appropriate training and levels of data protection awareness, this will be non-compliance with principle f of UK GDPR which could lead to sanctions by the ICO, fines and reputational damage.	2	3	6	**Reduced**	All RCPCH staff are required to undertake mandatory Data Protection and Information Security Training when they start at the college as well as a refresher every two years. Training is a mixture of eLearning and face to face training. R&QI staff are also required to annually undertake the MRC online data protection training. For HSC-PBPP all staff who have access to the data will have completed MRC online training every 3 years. The college's DPO/Head of IG has a Data Practitioners Certificate and undertakes regular refresher training.	By staff being aware of their data protection responsibilities they are less likely to cause a breach.		NNAP team/RCPCH Head of IG

Inappropriate access permissions are set on the system putting the data at risk of being lost, stolen or accessed without authorisation. Non-compliance with principle F also could lead to ICO sanctions, reputational damage and a fine	2	3	6	**Reduced**	Access will be based on the principle of least privilege. Authorised users are documented in the NNAP System Level Security Policy which will be reviewed annually by the NNAP team. The NNAP server has been audited by an independent auditor and IP restrictions and password protection put in place to prevent inappropriate access. Any requests for access will need to be approved by the NNAP Project Manager.	By using the principle of least privilege, access to data is only given where necessary. By assigning responsibility to the NNAP Project Manager, access can be monitored.		NNAP project team
Duplicated copies of the same information stored in two different places	2	2	4	**Reduced**	The RCPCH server is a mirror of the Badgernet server and it allows for 'live' updates. Versions of the identifiable data will be saved on the Azure server at regular (quarterly or monthly) intervals with version controls applied. The identifiable data will not be copied and stored anywhere else, apart from the back up. Pseudonymised versions of the database will be taken from saved on the RCPCH Microsoft Azure server at regular (quarterly or monthly) intervals for analysis at a given snapshot in time. Only authorised staff will have access.		Ongoing	

Inappropriate grounds for disclosure could lead to information being accessed by those who shouldn't access it and could lead to reputational damage, ICO sanction and fines	2	3	6	**Eliminated**	All new data sharing agreements are reviewed by the RCPCH Data Protection Officer. Any access requests (England and Wales) will need to be made via a DARs request form and access approved by HQIP and the NNAP project manager. Before information is shared it will be checked for any opt outs by the national opt out programme. Only aggregated non-identifiable data is published publicly.	To ensure that the DSA is fit for purpose	As and when necessary	NNAP project team/ RCPCH DPO
If data is not securely stored, it is at risk of being stolen, lost or damaged. This could lead to ICO sanctions, fines and reputational damage as well as substantial damage and distress to the data subjects if the information falls into the wrong hands	1	5	5	**Reduced**	Server storage has been selected in consultation with IG and IS and is ISO 27001 certified storage. Data is segregated from the main college network and stored on a separate server. Only non-identifiable data will be stored on the College servers, except for Episode Lists containing BadgerID and other non-identifiable information. Access to the server is restricted to those who require it for supporting the audit and maintenance of the server. Pen tests will be undertaken regularly on the system. The RCPCH completes an annual DSP Toolkit.	By segregating the data on our servers, this provides additional security to the data by reducing the risk of a data breach. If the college systems were compromised, this data may not be affected. This will also ensure that the data can be deleted with the required mechanisms and other data not impacted. By having secure storage, this reduces risk of data breach.		

If data is transferred outside of the EU without adequate protection, the data will not have the same level of protection as it does in the UK. If there is not an adequacy safeguard in place, this will be non-compliance with Chapter V of UK GDPR and could lead to a fine, ICO sanction and reputational damage	2	2	4	**Eliminated**	The NNAP team will check with any processors that they do not, and none of their sub-processors (including support services) will transfer any personal data outside of the UK. The RCPCH will not transfer any identifiable data outside of the UK.	By not transferring any personal data outside of the UK, this eliminates the risk of an international transfer.		NNAP project team
There is no consent for the use of cookies - data is being collected without appropriate legal grounds. This could lead to ICO sanctions, reputational damage and a fine	1	2	2	**Eliminated**	NNAP online use cookies. There is a notification of cookie use on the platform. Most of these are necessary for the site to function. It also uses analytical cookies to improve user experience, highlight issues and gather statistical information. A cookie policy is available and there is a consent mechanism.	By ensuring there is an appropriate consent mechanism in place, this will ensure consent is gained before any cookies are used, where necessary.		NNAP project team
If there is a data security breach and appropriate procedures are not in place, the data controller will not be able to reach its legal requirements for reporting to the ICO and could face a further fine as well as reputational damage	2	3	6	**Reduced**	If there is a data breach, RCPCH will follow its Security Breach Procedure. All RCPCH staff are made aware of the security breach procedure as part of the Data Protection training. The NNAP Project Manager will also ensure all members of the team are aware of the procedure and what to do in the event of a security breach. Any contracts with sub-processors will include provisions for reporting breaches promptly to RCPCH. RCPCH will inform HQIP of any breaches at a	By having adequate procedures in place, action can be taken promptly to contain the situation and reduce the risk of further damage and distress.		NNAP Project team/Head of IG

					reportable level in line with their contract and HQIP as data controller will make the decision as to whether the breach is reportable to the ICO.			
Online services directly targeting product/service to children or likely to be used by children is not compliant with the ICO Code of Practice on Age Appropriate Design. This could lead to breach of UK GDPR and an ICO sanction, reputational damage and fines as well as have a negative substantial impact on children and young people by not apply appropriate safeguards to protect their privacy rights	0	0	0	**Eliminated**	There are no online services targeting products or services to children.	N/A	N/A	NNAP Project team
Data collection seen as intrusive by individuals due to the opt out rather than consent approach.	2	2	4	**Reduced**	Renewal of public information leaflet which includes all information required by UK GDPR. This will provide information for parents on how they can opt out of their baby's data being used in the audit. It will clearly explain the purpose of processing the data and the legal justification. The national opt out will be applied before the data is processed by RCPCH (England and Wales).	Communicates the purpose and legal basis for processing data.	Already in place	NNAP project team
Where the legal grounds for processing is consent, individuals have the right to withdraw this consent at any time and the data must not be further processed. Where there is no mechanism in	0	0	0	**Eliminated**	Consent is not relied upon in this instance.	N/A	Alternative legal grounds already in place	NNAP Project Team

place for the individual to withdraw consent and no process to action and document the withdrawal of consent this will be in breach of principle a of UK GDPR- not having lawful grounds for processing. The individual will also not be able to action their right to object and will not have been fully informed about the processing. This could lead to a sanction by the ICO with a monetary fine and damage to RCPCH reputation.								
Undertaking direct marketing without appropriate legal grounds leading to non-compliance of UK GDPR and PECR could lead to ICO sanctions, reputational damage and fines	0	0	0	**Eliminated**	No direct marketing is undertaken. If there are any plans to market the audit in the future, the RCPCH IG team will be consulted.	N/A	N/A	NNAP Project team
System for opt out is not robust enough	2	3	6	**Reduced**	If NNAP data is to be linked or shared, the RCPCH will send a list of NHS numbers to NHS Digital (England) who will then send a list of NHS numbers with anyone who has opted out removed. NNAP will apply to records before processing further. RCPCH is currently developing a system to enable opt outs to be applied if the data is further shared, using the mesh mailbox in line with NHS guidance. There will be no onward sharing of Scottish data and there is no national opt-out in Scotland. A mechanism	By following guidance from the NHS, the national opt out will be appropriately applied and captured.	Complete d	NNAP project team

					exists on the Badgernet clinical system to capture local requests for their data to not be processed for the purpose of the NNAP.			
There are not appropriate sub-processor contracts in place and there has been no due diligence checks on these leaving the College in breach of Article 28 of UK GDPR	2	3	6	**Eliminated**	Article 28 contractual clauses are included in the contract between HQIP and RCPCH. There will be UK GDPR Article 28 contractual clauses in the contract between RCPCH and any of the sub-processors used. This will include ensuring that any further sub-processors used are also contractually bound to comply with equivalent data protection clauses as agreed between the RCPCH and HQIP. Any sub-processors which have access to the identifiable data, will be contractually required to evidence DSP toolkit submission on an annual basis. This will include any back up providers. Any new suppliers will also undergo an appropriate due diligence process as part of the college's tender process. The NNAP team will ensure that any new contracts or renewals will be reviewed by the RCPCH DPO and the Head of Governance to ensure compliance.	This will ensure that Article 28 contracts are in place with any party that processes the personal data and that any sub-processors are contractually bound to equivalent data protection requirements as between RCPCH and HQIP.	RCPCH/HQIP contract in place, all subcontract renewals in place by April 2022	NNAP project team

					RCPCH will hold any contracts with sub-processors but the NNAP team will ensure that HQIP have oversight of any contracts with sub-processors.			
Non-compliance with Article 28- to have appropriate data controller/processor contractual clauses in place could lead to an ICO sanction, a fine and reputational damage	2	3	6	**Eliminated**	The RCPCH and HQIP contract will include UK GDPR Article 28 contractual clauses. RCPCH will also be contractually required to evidence a DSP toolkit. The NNAP team will ensure that the RCPCH Head of IG and Head of Governance will review any contracts.			
The scope of the project changes and this PIA is not reviewed- this could lead to serious risks that are not appropriately mitigated and could lead to ICO sanctions, reputational damage and fines	2	3	6	**Accepted**	There will be an annual review of this PIA. If there are any changes in process this PIA will be reviewed with the IG team. Processes and guidance will be reviewed on a regular basis and with any change to the project methodology. If the audit team are considering merging datasets, they will first talk to the DPO about the UK GDPR implications and whether we need to make any changes to the privacy notice or reconsider our legal grounds for processing.	Ensures timely review of communication and processes if there is a change in the project.	As needed.	NNAP project team
Non-compliance with principle e of UK GDPR- data must not be kept for longer than necessary. Failure to comply could lead to	2	2	4	**Accepted**	Data will be kept until the end of the contract with HQIP and then deleted as requested by HQIP.	Ensures regular review if there are any changes to IG	NA	NNAP project team

ICO sanctions, reputational damage and fines					RCPCH retains college retention schedules to document retention as well as holding regular clear out days to review information.	permissions or project methodology.		
Back ups are kept for longer than necessary and are not kept securely so the data is at risk of being breached or of failure to comply with principle e of UK GDPR- data must not be kept for longer than necessary. This could lead to ICO sanctions, reputational damage and fines	2	2	4	**Reduced**	The Microsoft Azure Server, which hosts identifiable data, is backed-up every 5-10 minutes and back-ups are stored for 7 days.			NNAP Project team
Server data storage is sub-contracted out by the processor and there is no control or checks in place to ensure they are offering adequate security and the College is able to retain suitable control over the data. This could lead to non-compliance with principle f, having appropriate security in place	2	3	6	**Reduced**	The data is stored on a Microsoft Azure server. RCPCH IS set up the server with the support of CleverMed to ensure appropriate controls and checks are in place. The set up will be appropriately tested to ensure correct security settings and access permissions are set up before going live. The technical set up will be documented by the NNAP team in a System Level Security Policy with support from RCPCH IS and will include who will have responsibility for pen tests and admin access.	An independent audit has been carried out and remedial works undertaken to ensure that the server is compliant with ISO27001 and UK Official and UK NHS standards.	Complete	NNAP Project Team
Non-compliance with principle d of UK GDPR- data must be kept up to date and accurate. Failure to comply could lead to ICO sanctions, reputational damage and fines	1	2	2	**Accepted**	The NNAP is an annual audit, in which new data is used every calendar year. During the audit year, the NNAP provides quarterly data quality reports of	Neonatal units and networks are given the opportunity to quality assure data regularly.		NNAP project team

					aggregated data so that neonatal units and networks can check the quality of the data they submit to the audit. Data quality and validation checks are carried out on the data prior to analysis for the national report.	Data quality and validation process assures quality of final annual data.		
If individuals cannot action their privacy rights , this will mean non-compliance with article 13-22 of UK GDPR and could lead to ICO sanctions, reputational damage and fines	2	2	4	**Accepted**	The RCPCH has a specific documented procedure for dealing with rights requests in relation to clinical audits. The NNAP Project Manager will ensure that audit staff are aware of this procedure and know what to do with a request. The IG team will update the procedure to reflect the changes to the collection of patient data. As the data used is directly from the patient record, any requests will be forwarded to the trust/health board, who are the data controller for the patient record and are able to do appropriate verification checks. As the data is being processed for a public interest, the right to erasure does not apply. The privacy notice will detail each of the rights and how to action them.	RCPCH will forward on requests straight to the trust/health board to deal with these as they are the data controller of the information and therefore responsible for making these decisions. By informing data subjects via the privacy notice, they will be aware of their rights and how to action them.		NNAP project team

					The contract between HQIP and RCPCH will clarify responsibility for dealing with any rights requests received in relation to the audit. The Information Sharing Agreement between Scottish Health Boards and HQIP also clarifies responsibility for dealing with any rights requests in relation to the audit for Scottish data.			
UK GDPR outlines certain requirements in relation to automated decision making and profiling. If the profiling or decision making is solely automated organisations must also comply with Article 22 of UK GDPR. Failure to comply with the requirements set out in the UK GDPR, could lead to ICO sanctions, reputational damage and fines.	0	0	0	**Eliminated**	There is no automated decision making or profiling used to make decisions that might affect the data subject. If this is used in the future, this PIA will be reviewed with the RCPCH DPO.	N/A	N/A	NNAP Project Team
If staff are not appropriately trained in safeguarding practices and are not appropriately vetted, this could put the safety of the children we work with in jeopardy. It is important that personal data relating to children is only shared with those who have received appropriate training internally and only with those who are justified in having access to it to safeguard the CYP we work with. It is important we have the documentation to evidence appropriate staff	1	3	3	**Reduced**	HQIP have a process for raising serious concerns relating to the data, the NNAP Project Manager will ensure the NNAP Project team is aware of this. There is no direct contact with patients and so there are very unlikely to be safeguarding issues raised. Furthermore, it usually takes around 5 months until the data is viewed by RCPCH so it is unlikely any	Although it is low likelihood, there is a process in place so that appropriate action can be taken if needed.		NNAP Project Team

training and vetting if a safeguarding concern is raised to show we have taken appropriate safeguarding steps. As well as the damage and distress this can cause to the CYP, if we are unable to evidence this, the organisation could face sanctions as well as serious reputational damage.					safeguarding concerns will not have been picked up.			
Corporate risks & compliance risks section								
What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 - Insignificant 2-Minor 3-Moderate 4-Major 5- Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk OR Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Volunteers and Officers not having appropriate data protection training	1	3	3	**Reduced**	Update guidance given to officers and volunteers where they will be handling College personal data. Also investigating an e-learning module option.	They will receive appropriate training and therefore have better data protection awareness	August 2022	Data Protection Committee/Information Governance/People Services
Differing approach across the four nations	1	2	2	**Reduced**	Head of IG to regularly communicate with the four nations and ensure they are made aware of all internal information governance policies and procedures and received data protection training. Head of Media and	This will ensure staff have the same level of awareness as staff in the London office	Ongoing	Head of IG

					External Affairs sits on DPC and communicates back to nations			
Lack of resource to manage information governance	1	3	3	**Accepted**	Information Governance has a specific budget and there is one full time permanent member of staff and one full time permanent supporting member of staff. If further resources are required, the Head of IG will submit a proposal to SMT.	There is an internal process to request further resources if necessary.	Ongoing	Head of IG/SMT
Data stored outside of College systems (personal mobiles, laptops, homeworking)	3	2	6	**Accepted**	It is not practically feasible for all systems to sit within the centralised College network as it is near impossible to control the purchase of systems within the College.	N/A. This risk is accepted. When staff do purchase new IT systems, they will be required to do a PIA which they will need to submit as part of their proposal to SMT so the Head of IG should at least be able to ensure the system is compliant	Ongoing	All staff
Overload of SAR's (now that there is no charge)	1	2	2	**Accepted**	At the moment we have a relatively low number of SARs. The Head of IG and SIRO will monitor this and, if there is a significant increase, look at ways to prioritise workload or whether additional resources are needed	N/A	Ongoing	Head of IG
Non-compliance with UK GDPR leading to sanctions or breaches.	1	3	3	**Reduced**	Comprehensive framework of IG Policies and Procedures, adequate staff training and appropriate security measures in place. Completion of the UK GDPR work programme to bring	Greater awareness of the importance of data protection compliance across the organisation	Ongoing	Head of IG

					the College in line with the new legislation			
Duplicate information is less efficient to the business	1	3	3	**Accepted**	Comprehensive framework of IG Policies and procedures as well as staff training will support staff in good records management practice	Better records management practice	Ongoing	All staff
Losing future bids for audits because of a serious breach and lack of trust in RCPCH	1	3	3	**Reduced**	Ensure a good awareness of the importance of Data Protection compliance across the College will reduce the risk of a security breach	Reduce a risk of a security breach if staff are more aware of the importance of compliance and their responsibilities	Ongoing	All staff
Loss of trust in the RCPCH following reputational damage by a breach.	1	3	3	**Accepted**	Ensure a good awareness of the importance of Data Protection compliance across the College will reduce the risk of a security breach	Reduce a risk of a security breach if staff are more aware of the importance of compliance and their responsibilities	Ongoing	All staff
Data losses leading to claims for compensation by individuals	1	3	3	**Reduced**	All new high risk processing activities will need to undertake a PIA which will look at how to mitigate this risk	By design by default, this will reduce the risk of data loss by building in data security to new systems	Ongoing	All staff/Head of IG
Existence of contact lists separate to Care leading to silos of information, inaccurate and out of date information being used in relation to our members and non-members. Particularly, not applying up to date marketing suppressions	4	2	8	**Reduced**	Most direct marketing is managed through the college's central CRM, Care. Where there are exceptions sitting outside the process, this will also be documented on the Information Asset Register so that we fulfil our legal requirements in terms of accountability and Governance.	By having one source of truth for our membership files and for our member and non-member contacts, which is accessible throughout the College, this will reduce duplication and information silos	Ongoing	C&B/IS/ All Staff
Downloading of data onto servers/ cloud based platform which do not have an adequate	2	3	6	**Reduced**	Staff are required to undertake the PIA screening questionnaire if using a new	By undertaking a PIA we are able to identify risks early on	Ongoing	All staff

level of security in place for the type of data that is being processed					system as part of the PIA Policy. Any system/platform that requires SMT approval will need to submit an SMT paper and it is a requirement of any SMT paper to provide details of whether or not a PIA has been undertaken under the legal/contract section. There will be an annual update of the Information Asset Register which will ask information asset owners to update their relevant sections and any new systems will be captured and noted by the Head of IG to further investigate if necessary	before development so that we can choose an alternative supplier if they do not meet our security requirements or find ways to mitigate the risk.		