DPIA Screening Form – Liberty Protection Safeguards

Summarise what the project and proposed data processing is about	*This DPIA is for the implementation of Mental Capacity (Amendment) Act 2019, commonly referred to as Liberty Protection Safeguards (LPS). LPS will replace Deprivation of Liberty Safeguards (DoLS), which is a statutory function of the local authority as Supervisory Body for people who lack capacity to consent to their care and treatment at registered care settings.* The new legislation (LPS) was expected to be introduced from October 2020, then Spring 2021, and then late Summer 2021. We are still waiting on the code of practice to be released in December 2021 and the public consultation which will enable the implementation. *The proposed data processing is required, a) during the project phase to manage a timely transition and implementation., and b) to be in compliance with the legislation and related Code of Practice to effectively manage LPS applications, for those who meet the eligibility criteria, where Kent County Council is the Responsible Body.*

1	**Does the activity involve…**	**YES**	**NO**	**DPIA Necessary?**
Processing of personal data?		x		If no, a DPIA will not be necessary. If yes, please continue.
2	**Are you planning to…**	**YES**	**NO**	
Use systematic and extensive profiling or automated decision-making to make significant decisions about people.		x		If you answer 'yes' to any of these questions, you **must** carry out a DPIA.
Process special category data or criminal offence data on a large scale.		x		
Systematically monitor a publicly accessible area on a large scale.			x	
3	**Or are you planning to…**			
Make decisions on someone's access to a service, product opportunity or benefit which is based on automated decision-making (including profiling) or involves the processing of special category data.		x		If you answer 'yes' to any of these questions then you **must** carry out a DPIA.
Carry out profiling on a large scale.		x		
Combine, compare or match data from multiple sources.		x		
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.		x		
Process personal data which could result in a risk of physical harm in the event of a personal data breach.		x		
4	**Or are you planning to…**			
Process biometric data.			x	If you answer 'yes' to 2 or more of the criteria in this section 4, a DPIA **must** be carried out.
Process genetic data (other than by a GP			x	

or health professional to provide healthcare)				**OR** If you answer 'yes' to any of these questions, and at least one criteria from section 5 below applies, then you must carry out a DPIA. Even if no additional criteria below apply, **you may still need to do a DPIA depending on the nature of the processing planned.**
Use innovative technology.		x		
Process personal data without providing a privacy notice directly to the individual.		x		
Process personal data in a way which involves tracking individuals' online or offline location or behaviour.		x		
5	**Are you planning to carry out any other….**	**YES**	**NO**	
Evaluation or scoring.		**x**		Where two or more criteria are met, the activity may present a high risk to the rights and freedoms of data subjects and you should conduct a DPIA. Even if only one criteria is met, you may still need to conduct a DPIA if it is considered to present a likely high risk to the rights and freedoms of an individual. If uncertain about whether the risk is likely to be high, conduct a DPIA regardless.
Automated decision-making with legal or significant effects.		x		
Systematic monitoring		x		
Processing of sensitive data or data of a highly personal nature.		x		
Processing on a large scale.		x		
Matching or combining datasets		x		
Processing of data concerning vulnerable data subjects.		x		
Innovative use or applying new technological or organisational solutions.		x		
Processing involving preventing data subjects from exercising a right or using a service or contract.			x	
6	**Other**	**YES**	**NO**	
Are you planning any major project involving the use of personal data?		x		If so, you should consider carrying out a DPIA as good practice.
7	**Has there been a change…**			
In the nature, scope, context, or purposes of existing processing operations		x		You should carry out a new DPIA.

Conclusion	**YES**	**NO**	**Rationale**
Is a DPIA required?	x		
If no, will a DPIA be conducted anyway?			
Summary of DPO advice:			

When you have completed this screening tool please send it to the DPO for logging and advice: dpo@kent.gov.uk

DATA PROTECTION IMPACT ASSESSMENT - LPS

1. Document History

Version Number	Summary of change	Reviewed by (name and role)	Date
0.1	First draft	Sholeh Soleimanifar – Project DOLS Lead	20/09/2019
0.2	Peer Review	Matt Liggins – Senior project Officer	01/10/2019
0.3	Second draft	Sholeh Soleimanifar – Project DOLS Lead	18/11/2019
0.4	DPIA office review	Kate Kremers Ben Watts	25/11/2019
1.0	DPO recommendations updated in Section 12	Sholeh Soleimanifar – Project DOLS Lead	21/01/2020
1.1	Review of DPIA	Robert Underwood – Project Manager	16/12/2021

2. Administrative information

Name of organisation	Kent County Council
Service unit responsible for the project	Portfolio and Project Management Team Adult Social Care and Health
Senior Officer responsible for the project	Akua Agyepong – Senior Responsible Officer Maureen Stirrup – Senior Operating Officer
Project Manager	Glyn Pallister – Senior Project Manager Robert Underwood – Project Manager
Data processor (if applicable)	
Data Protection Officer	Benjamin Watts
[Other key personnel involved in the project]	Sholeh Soleimanifar – Previous Project lead

3. Executive Summary
(complete this section last)

Project Description

The Deprivation of Liberty Safeguards are an amendment to the Mental Capacity Act 2005. The Mental Capacity (Amendment) Act will introduce a new model for authorising deprivations of liberty in care, replacing DOLS with the Liberty Protection Safeguards (LPS). The new law is expected to come into force in October 2020 running alongside the DOLS for the first year. The new legislation (LPS) was expected to be introduced from October 2020, then Spring 2021, and then late Summer 2021. We are still waiting on the code of practice to be released in December 2021 and the public consultation which will enable the implementation.

The Kent LPS project will manage the transition and implementation of the new legislation, in settings where Kent County Council will be the responsible body.

Scope of processing, purposes of the processing and the legal basis for processing

Article 5 of the Human Rights Act states: "*Everyone has the right to liberty and security of person. No one shall be deprived of his or her liberty (unless) in accordance with a procedure prescribed in law*."

The Mental Capacity (Amendment) Act became law in May 2019 and is expected to become operational from autumn 2020. This legislation will replace the existing Deprivation of Liberty Safeguards (DoLS) and Deprivation of Liberty in community settings.
Where a responsible body (care home, local authority, CCG, NHS Trust) thinks it needs to deprive someone of their liberty, they must ask for this to be authorised. The responsible body will then appoint assessors, inhouse or third party, to see if the conditions are met to allow the person to be deprived of their liberty under the safeguards. If any of the conditions are not met, deprivation of liberty cannot be authorised. If all conditions are met, the responsible body must authorise the deprivation of liberty.

Intended benefits for data subjects, third parties and KCC

The intended benefits of the Liberty Protection Safeguards (LPS) is that individuals who need to be deprived of their liberty, and lack capacity to consent to their deprivation to received appropriate care and treatment plans, will have a legal framework to safeguard their interests.

The new legislation is wider in scope than the exiting DoLS, in that it will be applicable from 16 years and above and in any setting. However, the responsible body is dependent on where the person is being deprived. For NHS hospitals, the responsible body will be the 'hospital manager'. For arrangements under Continuing Health Care outside of a hospital, the 'responsible body' will be their local CCG. In all other cases – such as in care homes, supported living schemes etc. (including for self-funders), and private hospitals, the responsible body will be the local authority.

For the responsible body to authorise any deprivation of liberty, it needs to be clear that:
- The person lacks the capacity to consent to the care arrangements
- The person has a mental disorder
- The arrangements are necessary to prevent harm to the cared-for person and proportionate to the likelihood and seriousness of that harm.

Privacy risks and any proposed solutions to mitigate them.

As with processing of any personal and special category data, using multiple platforms, always carries a risk of data security incidents or breach. Data security is taken very seriously and a number of actions are taken to mitigate risks as far as possible:
- All staff must undertake mandatory training in Data Protection (GDPR) and Information Governance – reviewed at least every 2 years, or more frequently is needed
- DOLS and LPS will follow a strict scripted process, with all those engaged in any aspect are fully trained.
- Client information is only shared strictly on a need to know basis
- Documents are shared with external partners, such as the Managing Authority, Independent Mental Capacity Advocate, using password protection, Microsoft SECURE email or Egress Workspace – all of which are encrypted.
- For data analysis purposes data is anonymised to avoid risk of data breach
- In the event of data incidents or data breaches, lessons learnt are shared to avoid similar issues being repeated.

4. Identify the need for a data protection assessment (DPIA)
(complete the screening tool and attach a copy to this DPIA)

What type of processing is involved?	There will be large scale use of sensitive data, data concerning vulnerable data subjects, and potential use of new technologies in the form of Artificial Intelligence to conduct limited areas of the processing, such as transferring information from online applications to the client information system, allocating work to designated workers and payment of invoices.
Reasons a DPIA is required	Features of the processing indicate a likely high risk, as indicated by the DPIA guidance.

5. Description of the Processing
(you may wish to use or attach a data flow and attach to this DPIA)

Description of the Project/Processing	The LPS Project seeks to: 1. Identify the impact of the change in legislation in local policies, practice, protocols and guidance, leading to development of new policies, processes and guidance tools to ensure Kent's compliance with the new legislation. 2. Understand the impact of the change process within the Deprivation of Liberty functions (DOLS and Community), and the interface with operational teams, for 16/17-year olds (Children Services) and 18+ adults 3. Identify what Workforce is required to undertake the work: skills, capacity The above objectives, will ensure Kent will be in compliance with the new legislation, using efficient, effective and robust function(s) to ensure that the Mental Capacity Act works as intended, by providing people lacking capacity a more simplified system of authorisation and robust safeguards in a cost-effective manner, taking into consideration: • Understand the implications of the 2018 Mental Capacity Amendment Act for Kent • Reflect on emerging national developments, particularly Association of Directors of Adult Social Services (ADASS) • Network with colleagues nationally and locally working on the transition from DOLS to LPS • Identify the demand on the LPS provision in Kent • Identify capacity requirements to meet the demand in Kent • Plan interim arrangements to run parallel DOLS and LPS • Understand what the legal and practical implications of the new system will be and what preparations are needed • Understand what the policy implications of the new system will be and what preparations are needed • Identify the performance requirements of the new system will be and what preparations are needed • Reflect on how restrictions of people's liberty can be considered as part of their care and support plans • Understand interdependencies with commissioned services • Explore impact on finance systems, Collaborative Planning, Invoicing

	• Understand legal considerations. Amendments to existing contracts • Explore the implications on Children Services from applications from 16/17-year olds • Reflect on existing Systems (AIS, Lifetime Pathways (LPS), RIO, MOSAIC) • Development of a Performance Framework • Explore Workforce development • Explore Training needs for all stakeholders
What is the scope of the processing?	
Types of personal data	The types of data will include the data similar to that necessary to process DoLS application which is set out within the DoLS application Form. This would include name, date of birth, gender, disability, race, sexual orientation and religion. The application may also contact details for next of kin who need to be consulted as part of the assessment process. The purpose of collecting this information is to ensure the service is equitably accessed by all those who need it, regardless of their protected characteristics. Any protected characteristics that are found to be underrepresented through service reviews, to be investigated and action plans to be put in place to be rectified.
How many individuals will be affected and what geographical area will it cover?	Currently the DOLS office receives in the order of 100 applications per week (~5200 annually). These applications are only from registered care settings for adults of 18 years and over. Under LPS the scope is widened to include 16- and 17-year olds in any setting. However, the responsibility for authorisation will depend on where the deprivation takes place. For the local authority it will be all settings with the exception of hospitals (except private ones) and where funding awarded through Continuing Health Care. The number of applications anticipated under LPS has not yet been defined. In the project assessment phase, the project team will endeavour to calculate the impact of LPS in Kent.
How much data will be collected and used?	DPIA to be reviewed and updated once the LPS process has been mapped, following publication of the Code of Practice
Length and frequency of processing	DPIA to be reviewed and updated once the LPS process has been mapped, following publication of the Code of Practice
How long will the data be retained for?	Data will be retained according to KCC's most recent Data Retention Schedule for digital records, currently up to 7 years. Hard copies are scanned and stored electronically and immediately disposed in the blue confidential bins. All electronic records are stored on KCC servers which are backed up on a regular basis. Electronic files are deleted once they are uploaded to the client system (MOSAIC).
What is the nature of the processing?	
How will the data be collected and what is the source of the data?	It is expected to closely resemble to the data collected under Deprivation of Liberty Safeguards. The data collection process will be mapped once the Code of Practice has been published, which we are still waiting on publication.
How will the data be used and stored	The data will be collected on LPS application forms (currently under development by ADASS) and will be submitted to the appropriate Responsible Body electronically via email or an online platform

	similar to the current DOLS process. The process is not yet mapped out in full, pending the publication of the Code of Practice. Application forms will be stored electronically on the universal (k) drive, until uploaded to MOSAIC, at which point it will be deleted.
How is the data secured and processed in a manner that ensures appropriate security (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)?	Data security is an integral part of the DOLS/ LPS business. All users, including: Admin, managers, practitioners, will have appropriate level of access to shared drives, on a strict access basis, approved by DOLS management. Every user must undertake mandatory data protection and Information Governance training, including refresher training every 2 years. Due diligence is applied at every stage of processing, in particular where third parties are concerned, e.g. Independent Best Interest Assessors, S12 Doctors, and commissioned providers which process data on Kent County Council as third parties. Where information needs to be shared with individuals external to KCC or with partner agencies, data is encrypted using Microsoft SECURE, Egress/ Egress Workspace. Email to compliant organisations, i.e. those listed on central government's 'White List', will be automatically encrypted and transmitted securely without further security measure. Whichever mechanism is used to transmit data, personal data is protected by anonymisation, where the recipient does not need the information for the purpose of the work they are required to undertake. If full personal data is required by the recipient, it will be shared as an attachment to Microsoft SECURE email or upload to Egress. To further protect identification, only initials of individuals and unique reference number (only identifiable to KCC staff) are used in the subject header, rather than a person's Full Name, date of birth or their place of residence. Technology Strategy & Commissioning Secure Email Policy (Version 1.2 – August 2018) sets out acceptable practice, identifies key issues that should be considered and outlines the secure email services that are available. This policy applies to all employees with an authorised KCC computer user account including individuals on temporary and contract assignments. Documents containing personal information are sent using Royal Mail's Signed For service. Every endeavour will be made to prevent loss of data or inappropriate sharing of data by our policies, good practice principles, training and general knowledge regarding data protection. However, incidents may still occur, in which case staff must follow KCC's Data Breach Policy.
How will the data be deleted/disposed of?	Data will be deleted/ disposed of based on Kent County Council's current data retention policy: • Information Management Manual Version 3.1 May 2018, and • Retention Schedule Version 3 July 2019 for projects
Will the data be shared/disclosed to third parties?	Yes. In order to comply with the statutory requirements of the legislation, Kent County Council, as the Responsible Body may have to share data with a number of third parties involved to conduct the necessary assessments and to ensure the rights of the person are safeguarded, such as an Independent Mental Capacity Advocate or an Approved Mental Capacity Professional. These arrangements will be monitored by the DOLS/ LPS teams, as part of the process to assess and authorise the applications.

What types of processing identified as likely high risk are involved?	The reasons processing of data is considered high risk include: • The processing of applications involves both personal, sensitive data including special categories of data provided as necessary to the completion of a DoLS assessment as set out in the application form for a DoLS. • The Data processed will be on a large scale, both volume and geographical scope (county wide)
What is the context of the processing?	
What are the categories of data subject, and do they include children or vulnerable groups?	The data subjects will include 16- & 17-year olds, and adults over 18 years old, who are assessed to lack capacity to consent to their care and treatment arrangements and are assessed to be deprived of their liberty.
What is the nature of the relationship with individuals?	KCC has a legal responsibility to complete DoLS/ LPS assessment for people who are living in care homes, private hospitals, and in community settings, who have restrictive environments and are unable to consent to their living arrangement for the purpose of receiving appropriate care and treatment. KCC is in a relative position of power to the individuals here.
How much control will they have?	Due to their vulnerability it is unlikely the data subject will have much control about the DoLS or LPS application being made. However, all interested parties are consulted, and if the person is found to be un-befriended, they have the right to be supported by an Independent Mental Capacity Advocate (IMCA) and /or an Appropriate Person. The Relevant Persons have the right to expect their data is used appropriately and securely and that it is accurate and up to date.
Would they expect you to use their data in this way?	The Managing Authority or care home should discuss the DOLS/ LPS application with the data subject however due to the fact that they lack capacity to consent to their deprivation to receive care and treatment, the person may not be able to understand or process this information. The Assessment process ensures the person's wishes and beliefs are taken into account and people involved with the person are consulted. The DoLS authorisation also provides a Representative for the person to represent their views
Are there prior concerns over this type of processing or security flaws?	The concerns are around the sharing of information with relevant parties, by email and or post. Any incidents of potential data security incidents have been shared with the Information Resilience & Transparency Team and as a result supplementary measures are in place to ensure these risks are minimised as far as possible.
Is it novel in any way?	No
What is the current state of technology in this area?	KCC has adopted the Government Secure Standard for email to other compliant government organisations using a user's standard gov.uk email address These are automatically encrypted and transmitted securely. For intended recipients who are not given in central government's 'White List', KCC has implemented the Microsoft Office 365 Message Encryption (OME) facility which automatically encrypts the email and its contents (attachments). This facility is activated by either using the Secure Mail button in Outlook or manually typing "[SECURE]" as the first word of the email's 'Subject' line. Data files are stored in KCC systems, with access given only to those who need access to the information as part of their work.

	The Client data platform is recently migrated from AIS to MOSAIC, with access only to staff with KCC login accounts who have completed both the necessary training.
Are there any current issues of public concern that you should factor in?	The reputation of KCC as a local government body, to be compliant with statutory duties, and to be seen to be utilising public funds effectively and efficiently.
Are you signed up to any approved code of conduct or certification scheme?	No
What is the purpose of the processing?	
What do you want to achieve?	The purpose of processing the data is to ensure compliance with LPS legislation.
What is the intended effect on individuals?	People who are eligible to be assessed for DoLS/ LPS will have appropriate assessment and safeguard of an authorisation, as a result of which people will have an appointed representative to monitor their living arrangement and any restrictions.
What are the benefits of the processing for KCC, and more broadly?	Please see above. KCC will be fulfilling its statutory duty as a Supervisory Body under DOLS and Responsible Body under LPS.

6. Consultation			
Who will you consult?	**When will you consult?**	**How will you consult?**	**Responses**
Project Steering Group	At regular steering group meetings within the project lifecycle	Verbally	Responses will be collated and recorded
MOSAIC lead *ICT lead*	During project lifecycle	Direct consultation via email/ face to face meetings	Responses will be collated and recorded
[Procurement]	N/A	N/A	N/A
[data subjects or their representatives]	N/A Data will be anonymised or pseudonymised. Clients and third parties will receive relevant privacy notice to inform what information KCC will share to fulfil its statutory obligations.	N/A	N/A
[Other experts, eg. IT, legal or other			

professionals]			

7. Assess necessity and proportionality	
What is the lawful basis for processing?	The processing of data in relation to Liberty Protection Safeguards are contained within the Mental Capacity (Amendment) Act 2019. Processing is necessary to undertake the necessary assessments under the Act, and to delegate certain tasks to third parties. The Care Act 2014 allows KCC to delegate responsibility to a third party. Article 6(1): - 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 - processing is necessary for compliance with a legal obligation to which the controller is subject For 'special categories of personal data', (such as health, race, ethnicity, sexual orientation) we rely on the following legal bases under Article 9(2): processing is necessary for reasons of substantial public interest (safeguarding of children and of individuals at risk) processing is necessary for the provision of health or social care or treatment or the management of health or social care systems and services Data Protection Act 2018 Schedule 1: The processing is necessary for **Health and Social Care purposes** including preventative or occupational medicine, medical diagnosis, the provision of health care or treatment, the provision of social care and the management of social care systems or services. The data processing by KCC will be carried out under the responsibility of [INSERT JOB TITLE] who is a social work professional. **Safeguarding of children and individuals at risk** The processing of this data will occur when necessary for the purposes of protecting the physical, mental or emotional well-being of an individual at risk (ie KCC has reasonable causes to suspect that an individual has needs for care and support (including protection), is experiencing or at risk of neglect of physical, mental or emotional harm, and as a result of those needs is unable to protect themselves against the neglect or harm or risk of it). In the circumstances consent cannot be given by the data subject, or KCC cannot reasonably be expected to obtain their consent or the provision of consent would prejudice the provision of protection. The legal bases also include actions that can and should be taken by local authorities, including:

	• the Care Act, 2014 • the Health and Social Care Act, 2015• • the Localism Act, 2011 • the Human Rights Act, 1998 the Mental Capacity Act, 2005
Legitimate interests	N/A
What information will you give to individuals?	KCC Privacy Notices General notice to cover adult social care and health https://www.kent.gov.uk/about-the-council/contact-us/access-to-information/gdpr-privacy-notices/adult-social-care-and-health Adult Safeguarding Privacy Notice http://www.kent.gov.uk/about-the-council/contact-us/access-to-information/gdpr-privacy-notices/adult-social-care-and-health/safeguarding. Also, privacy notice for third parties; which makes it clear what information we collect, why and who we share it with. https://www.kent.gov.uk/about-the-council/information-and-data/access-to-information/gdpr-privacy-notices/adult-social-care-and-health/kent-adult-social-care-and-health-third-parties-privacy-notice
Does the processing achieve your purpose?	Yes
Is there another way to achieve the same outcome?	No
How will you prevent function creep and preserve the second data protection principle: 'purpose limitation' (ie only using the data for specific, explicit and legitimate purposes (as set out in a privacy notice) and not further processing the data in a manner that is incompatible with those purposes	[i.e. how will you prevent the use of the data going beyond the purpose for which it was originally intended and obtained.] The project will be subject to regular stage gate reviews within the project lifecycle as well as Project Management processes. Once LPS is operational, the data can only be used for the purpose of authorisation of LPS application. Once authorised, the data is uploaded to MOSAIC, pending future review/ re-authorisation.
How will you ensure data quality and minimisation?	The only data collated is directly related to and necessary for the authorisations of requests for Deprivation of Liberty. Data files will be stored accordance with KCC's retention policy. Sharing of data will be closely monitored both within KCC and external partners – on a need to know basis to ensure compliance with legislation.
How will you ensure personal data is accurate and, where necessary, kept up to date	The accuracy of information is tested at the point of assessment, through consultation with relevant partners, and Appropriate Persons. Data is cross referenced against any historic information held on client system, MOSAIC. Any conflicting information will be checked and corrected at source as soon as it comes to light.
How will you support data subject rights?	Authorisations contains safeguards for the individual including a representative to support their rights and express their views which may include making applications to the Court of Protection. Data protection laws will be upheld. Information will only be shared/ used on a need to know basis. Data will be anonymised/

	pseudonymised where required and only to ensure the data recipient is able to carry out their role.
What measures do you take to ensure processors comply?	DOLS/ LPS is a statutory function of the local authority. To comply with this legislation Kent County Council may either collect personal information directly or receive it from third parties. We only receive personal data from outside agencies or third parties where there is a legal basis for doing so. We do not share the profiles of individual service users with any other organisation or business other than those acting as data processors on behalf of Kent County Council.
How do you safeguard international transfers?	Information will not move outside of the UK.

8. Identify and assess risks
(you can refer to the attached risk matrix to help assess the level of risk)

Risks to INDIVIDUALS

(Remember, a DPIA is focussed on the potential harm to data subjects and should be considered from the data subject's point of view.)

Risk Description	Likelihood of harm	Severity of harm	Overall risk
Examples (please tailor/add/delete as necessary): *[Inadequate disclosure controls, increasing the likelihood of information being shared inappropriately.]*	*[Very unlikely, unlikely, possible, likely, or very likely]*	*[Minor, moderate, significant, serious, major]*	*[High, medium or low]*
[The context in which information is used or disclosed may change over time, leading to it being used for different purposes without people's knowledge or consent.]	Possible	Moderate	Medium Information will be used in accordance with defined processes following a legislative framework. If a concern is raised it could be used as part of Safeguarding process.
[New surveillance methods may be an unjustified intrusion on their privacy.]	N/A		
[Measures taken against individuals as a result of collecting information about them might be seen as intrusive.]	Possible	Moderate	Low DOLS/ LPS under the MCA is a statutory function, which necessitates collation of information to discharge a legal duty.
[The sharing and merging of datasets may allow us to collect a much wider set of information than individuals might expect.]	Possible	Moderate	Medium In considering a DOLS/ LPS application, any previous information held on the Client Systems that may impact on the application will be used to ensure the best outcome is

			achieved for the individual.
[Identifiers might be collected and linked which prevent people from using a service anonymously.]	High	Moderate	High DOLS/ LPS applications contain personal information
[Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.]	Possible	Moderate	Medium Identification is necessary for KCC to comply with its statutory function
[Collecting information and linking identifiers might mean that we no longer use information that is safely anonymised.]	N/A		DOLS/ LPS applications are never anonymous
[Information may be collected and stored unnecessarily, or not properly managed so that duplicate records are created, presenting a greater security risk.]	Possible	Moderate	Medium Duplicate records are rare, but possible
[Failure to establish appropriate retention periods might mean information is used for longer than necessary.]	Possible	Low	Low
[*Insert any other risk to individuals' privacy*.]	N/A		
Organisational risks			
[Non-compliance with the GDPR or other legislation, which can lead to sanctions, fines and reputational damage.]	Possible	Significant	Medium
[Problems may only be identified after the project has launched and will then be more likely to require expensive fixes.]	Possible	Moderate	Low
[The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with KCC.]	N/A		
[Information may be collected and stored unnecessarily, or not properly managed so that duplicate records are created— meaning the information is less useful to the business.]	N/A		
[Public/client/customer distrust about how information is used may damage KCC's reputation.]	Possible	Significant	Medium
[Data losses which damage individuals could lead to claims for compensation.]	Possible	Minor	Low
[Insert any other risk to the organisation]			
Legal compliance risks			
[Non-compliance with the GDPR - i.e. *will the processing meet the principles in Article 5 GDPR, i.e.* • *Fair, lawful, transparent*	Very	Major	*Low*

• *Specified, explicit, legitimate purposes* • *Adequate, relevant and not excessive* • *Accurate and up to date* • *Not kept longer than necessary* • *Processed in accordance with rights of data subjects* • *Protection against unauthorised or unlawful processing, loss, destruction or damage* • *Not transferred outside EEA unless adequately protected.]*	unlikely		
[Non-compliance with the Privacy and Electronic Communications Regulations 2003 (PECR 2003), e.g. if KCC wish to send electronic marketing messages (by phone, email or text), use cookies, or provide electronic communication services to the public]	Unlikely	Significant	Medium
[Non-compliance with sector specific legislation or standards.]	N/A		
[Non-compliance with human rights legislation, eg breaching an individual's Article 8 right to private and family life. You must also ensure your personal data processing has a legitimate aim]	Very unlikely	Significant	Medium
[*Insert any other legal compliance risk, e.g. creating datasets may increase risks/costs through disclosing requirements under the Freedom of Information Act 2000*]			

9. Identify and evaluate measures to reduce risk

Potential solution	Which risk(s) would this action address?	Effect on risk	Residual risk	Cost/benefit/ evaluation	Measure approved?
Examples (please tailor/add/delete as necessary): *[Not collecting or storing [insert description] type of information.]*	[*State which of your identified risk(s) will be addressed by this action.*]	[*Is the risk eliminated, reduced or accepted?*]	*[Low, medium or high]*	[*Is the final impact on individuals a justified, compliant and proportionate response to the aims of the project?*]	*[yes/no]*
[Introducing retention periods to keep information for only as long as necessary.]	information is retained for longer than necessary	Reduced	Low	Yes	
[Secure destruction of information that no longer needs to be retained.]	information is retained for longer than necessary	Reduced	Low	Yes	

[Implementing appropriate technological security measures.]	Prevent/ reduce risk of data breach	Reduced	Medium	Yes	
[Properly train staff and make them aware of potential privacy risks.]	Prevent/ reduce risk of data breach	Reduced	Low	Yes	
[Ensure information is safely anonymised when it is possible to do so.]	Applications cannot be anonymised	Medium	Medium	Risks are proportionate.	
[Provide guidance to staff on how to: *—use the new system, and* *—share data appropriately]*	Prevent/ reduce risk of data breach	Reduced	Low	Yes	
[Ensuring the new system: *—allows individuals to access their information more easily, and* *—makes it simpler to respond to subject access request]*	N/A				
[Ensuring individuals: *—are fully aware of how their information is used, and* *—can contact us for assistance when necessary]*	GDPR Compliance	Risk reduced	Low	Yes	
[Selecting data processors who will provide a greater degree of security.]	GDPR Compliance	Risk reduced	Low	Yes	
[Ensuring agreements are in place with data processors to protect information processed on our behalf.]	GDPR Compliance	Risk eliminated	Low	Yes	
[Ensuring any data sharing agreement makes it clear: *—what information will be shared* *—how it will be shared, and* *—who with]*	GDPR Compliance	Risk eliminated	Low	Yes	

[Insert any other solution you have identified]					

10. ICO consultation	
Does this assessment indicate that the processing involved in the project would present a high risk in the absence of mitigation measures?	No
If yes, can those risks be mitigated by reasonable means in terms of available technologies and costs of implementation?	Yes [*If no, it is necessary to consult with the Information Commissioner's Office (ICO) prior to the processing.*]
If it is necessary to consult with the ICO, has this been done?	Not applicable *[If yes, provide further information.]*

11. Sign off and record of outcomes		
Item	**Name/date**	**Notes**
Measures to reduce risk approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:	**25/11/2019**	*DPO should advise on compliance, measures to reduce risk and whether processing can proceed*
Summary of DPO advice: Many of the processes and procedures have not yet been fleshed out and are part of the ongoing development of the project. At this stage the advice is therefore quite generic. • Currently, the processing in this DPIA is not high risk and measures taken to reduce risk are such that any residual risk has been sufficiently mitigated. • The DPIA does not need to be sent to the ICO as sufficient measures have been taken to reduce risk. This is **subject** to the actions highlighted in Section 12 below being taken.		
DPO advice accepted or overruled by:	**accepted**	*If overruled, you must explain your reasons*
Comments: *[if the advice is accepted, please ensure any actions recommended by the DPO are added to the DPIA and implemented].*		
Consultation responses reviewed by:	**n/a**	*If your decision departs from individuals' views, you must explain your reasons*
Comments:		

This DPIA will kept under review by:	**LPS Project Manager**	*The DPO should also review ongoing compliance with DPIA*

We confirm that we have reviewed this DPIA and are satisfied that:

— it is not necessary to consult with the ICO.

Name(s)	Benjamin Watts Kate Kremers
Job title(s)	General Counsel Senior Solicitor
Date	25/11/2019

12. Actions to be integrated into project plan		
Action to be taken	**Date for completion or frequency**	**Responsibility for action**
1. Ensure that the corresponding condition under the Data Protection Act 2018 (health and social care purposes) can be met by identifying the responsible person overseeing the processing of any special category data under the 'health and social care purposes' condition: *(S11(1) states 'For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out –(a) by or under the responsibility of a health professional or a social work professional, or (b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.)' S204 provides further definition of who may be regarded as a 'social work professional': http://www.legislation.gov.uk/ukpga/2018/12/section/204/enacted*	*Implementation date of LPS - currently 01/10/2020*	*LPS Project Manager*
2. ICT Risk and Compliance should be asked to give a view on the technological risks involved in the use of Artificial Intelligence (mentioned in section 4) and on the details of how the data is used and stored (on page 5) with their recommendations fed back into the consultation section of the DPIA.	*2 months prior to implementation – 01/09/2020*	*LPS Project Manager*
3. Any third parties commissioned to process data on KCC's behalf must be retained by a GDPR compliant contract containing the mandatory terms and conditions as required by Article 28.	*Implementation date of LPS - currently 01/10/2020*	*LPS Project Manager*
4. The DPIA should be updated and submitted to dpo@kent.gov.uk once the LPS process has been mapped, to obtain further advice as necessary.	*3 months prior to implementation - 01/08/2020*	*LPS Project Manager*

Risk Matrix

Likelihood	Very likely	5	5 Low	10 Medium	15 Medium	20 High	25 High
	Likely	4	4 Low	8 Medium	12 Medium	16 High	20 High
	Possible	3	3 Low	6 Low	9 Medium	12 Medium	15 Medium
	Unlikely	2	2 Low	4 Low	6 Low	8 Medium	10 Medium
	Very Unlikely	1	1 Low	2 Low	3 Low	4 Low	5 Low
			1	2	3	4	5
			Minor	Moderate	Significant	Serious	Major
			Impact				