

DATA PROTECTION IMPACT ASSESSMENT

DPIA v0.1 Adult Social Care Service Provision Review

1. Document History			
Version Number	Summary of change◆	Reviewed by (name and role)	Date◆
V0.1	First draft	Tony Nankivell, Project Officer	14/07/2022
V0.2	Second Draft	Tony Nankivell, Project Officer	09/08/2022

2. Administrative information	
Name of organisation◆	Kent County Council (KCC)
Service unit responsible for the project◆	Innovation Delivery Team, Business Delivery Unit, Adult Social Care and Health
Senior Officer responsible for the project◆	Helen Gillivan, Head of Business Delivery Unit, 03000 410180
Project Manager◆	Elizabeth Blockley, Project Manager, 03000 417304
Data processor (if applicable) ◆	N/A
Data Protection Officer◆	Ben Watts 03000 416814
[Other key personnel involved in the project] ◆	Tony Nankivell, Project Officer, 03000 414722 Lee Inman, Project Officer, 03000 412082 Georgina Walton, Senior Project Officer, 03000 415535 Alyson Wagget, Assistant Director (East) Thanet and South Kent Coast, 03000 412483 Barbara Rickman, Assistant Director Service Provision, 03000 410895 Anthony Prime, Commissioner, 03000 410673 Theresa Barwell-Ward, Commercial Manager, 03000 415822 Sandie Atwell, Procurement Lead, 03000 423402 Akua Agyepong ASCH Assistant Director County (Specialisms) Akua.Agyepong@kent.gov.uk (Social Work Professional) Janine Hudson, Social Work Professional, Janine.Hudson@kent.gov.uk

3. Executive Summary◆
<p>The Technology Enabled Care project is a key area of the Making a difference everyday approach which is the main driver of change within Adult Social Care. The programme and this project align with KCC's Strategic Reset Programme and will contribute towards the delivery of the key ambitions of the Authority.</p> <p>The Care Act 2014 places general responsibilities on local authorities relating to the care and support for adults and support for carers in its area. In exercising these statutory duties, Kent County Council ('the authority') must provide or arrange for the provision of services, facilities and resources, or take other steps which it considers will promote an individual's well-being, contribute towards preventing or delaying needs for care and support, promote integration of care and support with health services etc., provide information and advice, promote diversity and quality in provision of services, cooperate generally and</p>

cooperate in specific cases with relevant partners in the exercise of their respective functions relating to adults with needs for care and support and/or relating to carers.

There have been significant developments in social and health care apps and wearables in recent years, and growth in the popularity and uptake of these devices. They provide people with convenience and control to integrate technology into their lives both when well and when ill; they also afford people the ability to share their data with who they want to. For example, the devices can support people in assessing health signs and symptoms, keeping them healthy and managing long term conditions. This in turn can provide value in supporting independent living and the presence of non-traditional care technology brands in the sector may well grow.

The consumer technology / smart home market is rapidly crossing over into the care technology sector. There is undoubtedly an opportunity for KCC to encourage use of technology to support individuals across the county. KCC could consider providing guidance to those wanting to use technology to support independence at home and empower people to live their lives.

As a society, we are adopting digitally enabled solutions in many aspects of our lives; with extraordinary innovations emerging to support people to live independently. For example, technology, such as wearables, smart voice interaction systems, big data analytics and artificial intelligence, can offer so much more than legacy telecare, as a preventive tool to defer the need for or avoid more intensive forms of care. The digital switchover, due by 2025, will be a significant catalyst to the telecare industry, making many of the existing analogue solutions obsolete.

Scope of processing

KCC will engage with one third party provider (acting as a data processor on behalf of KCC) to access the market and purchase devices and equipment on KCC's behalf, as well as to provide a platform that all devices will sync with, to enable KCC to manage them.

Technology Enabled Care could come in the following, but is not limited to, forms:

- Assistive technology - (e.g. smart devices such as televisions speakers, and home hubs, video doorbells, medication dispensers, remote door entry, robotics, wearables etc.)
- Mobile Applications (e.g. promotion of health, for wellbeing, undertaking daily activities etc.)
- Remote monitoring and communication (e.g. tablets, video phones, virtual calls to formal and informal network, sensory impairment communication tools, environment sensors, personal sensors, alarms etc.)

KCC would like flexibility to select any available products and technologies which suit the care package of the service users. The type of data collected, and the nature of the specific processing will depend upon the particular product or technology used.

Ultimately the service users will have a choice as to which technology they would like to use (if any), however recommendations will be made by the relevant Practitioner.

This project is running on the back of a Test and Build pilot project that has been running since early 2022 in three areas, Thanet, Dover, Folkestone and Hythe. A full DPIA was undertaken for that project at the time, and this Countywide offering is seen as an extension of this Test and Build..

Objectives

To design and procure an innovative digital Assistive Technology offer that supports people to live independently and enables the authority, partners and providers to maintain a person-centered approach by being agile to people's needs whilst enabling statutory requirements to continue to be met.

Reasons for processing, lawful basis and processing conditions

Lawful basis Article 6(e): Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 9 processing conditions:

For the processing carried out by KCC Projects Team (and related parties within KCC i.e. the Performance Team which will run and deliver reports for the Projects Team), in order to deploy technology enabled care and evaluate its impact and success:

(g) Necessary for substantial public interest (on the basis of a DPA condition – [also complete Table 2b below](#)) and which

shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of data subjects. Relevant DPA 2018 condition: Schedule 1, paragraph 6 - Statutory and government purposes - necessary for the exercise of a function conferred by an enactment or rule of law (paragraph 6(2)(a)).

For the special category health data that is processed by the healthcare professional using the technology solutions as part of a care plan:

(h) Necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health or social care systems and services (subject to a DPA 18 condition – [also complete Table 1 below](#)) or pursuant to contract with a health professional and subject to the conditions and safeguards in 9(3)

Expected Key Benefits

- People satisfaction
 - This is a key outcome of the Strategic Reset Programme as well as the Making a difference every day approach. With additional assistive technology tools available for Practitioners to utilise to meet care and support needs, it is expected that people’s satisfaction levels should increase
- Partnership working / opportunities
 - Technology Enabled Care will benefit the wider health and social care system and not just the authority once the culture and awareness of the opportunities has been evidenced. For instance, utilising data and information to identify patterns in behaviours to become more preventative rather than reactive in terms of health, care and support delivered
- Demand
 - Providing greater information, advice and guidance on assistive technology across all areas of the social care pathways and how this can be accessed will support demand on formal social care services
 - Utilising assistive technology to provide remote support, targeting those who are in need of support through data and analytics, or empowering the informal support network of people to help manage and respond to changes in need or reactive support (e.g. a fall).
- Cost avoidance, savings and income
 - Through using Technology Enabled Care, there could be opportunities to not only meet the outcomes of people but also reduce or delay escalation of need but also reduce the need for other traditional care and support methods in favour of assistive technology (where suitable). In some instances, assistive technology could prevent the need for any formal social care intervention.
- Environmental
 - Through assistive technology, this could also reduce the needs for physical visits to people we support, therefore reducing the use of vehicles for social care professionals.

4. Identify the need for a data protection assessment (DPIA)

What type of processing is involved? ♦	<p>This DPIA is for the countywide rollout with a five year contract following an initial 1 year trial of Technology Enabled Care. The provision of care by Practitioners is already happening and is not the subject matter of this DPIA, this DPIA is specifically for the use of technology products to assist with the care already being provided.</p> <p>Processing of personal data – there will be the need to use service user names and addresses, client ID from KCC’s social care platform (MOSAIC etc.) and contact details. This is in order to install and manage technology solutions and measure their effectiveness. Additional types of personal data that will be collected and processed for these purposes are detailed in section 5.2(a) and (c) below.</p> <p>Processing of special category data – this will be for KCC use only in order to complete an equalities impact assessment for this project, as well as to deliver the technology enabled care to service users depending on their healthcare plan and medication</p>
---	---

	<p>needs (see details of special category data collected in section 5 below).</p> <p>Combining, comparing or matching data from multiple sources – the project will be using reports from KCC’s social care system MOSAIC as well as information from Strategic Commissioning and the contract care providers they manage in order to identify a suitable cohort of service users. Once the cohort have been selected data will then continue to be combined and compared to evaluate success - this data will be obtained by the Projects Team from the chosen third party supplier’s platform as well as from pseudonymised reports which will be run from the KCC live care platforms (for further details see below).</p> <p>Processing personal data which could result in a risk of physical harm in the event of a personal data breach – as the service users are vulnerable individuals, a personal data breach may result in a risk of emotional or physical harm to those service users.</p> <p>Children’s data – there is scope for the Project to involve use of Technology Enabled Care for children, not just for use by the Adult Social Care team.</p> <p>Depending on the device or solution chosen, the project may involve processing personal data in a way which involves tracking individuals’ online or offline location or behaviour.</p> <p>Evaluation or scoring – as part of the project, there will be a need to assess the success Technology Enabled Care service. This will involve asking service users and potentially their friends and family to partake in a research piece of work (questionnaire / case studies / surveys). This evaluation will also be undertaken with the provider, care providers and front-line staff within KCC’s Adult Social Care.</p> <p>Innovative use or applying new technological or organisational solutions – although this is not new technology, it is based on the findings of the initial Test and Build results.</p> <p>The DPIA will reflect the security arrangements of the third party provider once the providers are known.</p>
<p>Reasons a DPIA is required◆</p>	<p>Based on the types of data being processed and the processing activities noted above, the processing is higher risk and a DPIA must be completed.</p> <p>This is a new major project involving the use and processing of personal data of service users within adult social care at KCC.</p> <p>Whilst the care phone and supporting technology used is not new to the market, it is to the authority and therefore a DPIA should be undertaken to clearly detail the roles and responsibilities of the data controller (KCC) and processor (TBC).</p>
<p>Is this DPIA a review of pre-GDPR processing or does it cover intended processing?</p>	<p><input type="checkbox"/> Pre-GDPR processing <input checked="" type="checkbox"/> Intended Processing</p> <p><u>Timeline of the project</u></p>

	<ul style="list-style-type: none"> • Market Engagement – June 2022 • SSQ – Nov 2022 • SSQ evaluation and ITT – Dec 2022 • ITT evaluation –Anticipated contract start date is Mar 2023
--	---

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

<p>Description of the Project/Processing◆</p>	<p>Referrals</p> <p>For referrals into this provision, this will be undertaken through traditional care act assessments and where Technology Enabled Care can meet identified needs. The type of information that will then be passed to a provider of the Technology will be as follows:</p> <ul style="list-style-type: none"> • Case management reference no. • Name • Address • Contact details (telephone and / or email) • Delivery address for technology (if different to the living address) • Contact details of any contacts or responders (friends, family, formal care providers, partner agencies) • Details of Care package (sensitive) – to help ensure the right technology is identified to meet the needs eg falls detection, video doorbell, Alexa. <p>People will be provided choice and control over their care and support so Technology Enabled Care will not be suitable for all people KCC supports. Those that do agree to receive Technology Enabled Care will be captured in their care and support plans and recorded on the Authority’s case management system in line with existing Practice. Technology Enabled Care is a tool for social care professionals alongside other traditional methods such as care and support in the home.</p> <p>Reporting</p> <p>Client data that will be used within this project (prior to being shared with the Projects Team) is stored on one of the following Kent County Council live database - Mosaic, Liberi or LPS. <u>The Operational Team of Practitioners will have access to full client information on one of these live databases.</u></p> <p><u>The Performance Team are responsible for running MOSIAC and equivalent platforms and have access to the data in order to provide IT support functionality. The Projects Team are responsible for trialling the technology enabled care and evaluating its success, but will not have any access to client information within MOSIAC or the equivalent care platform. The Performance Team will run and share reports from MOSIAC etc. to enable the Projects Team to roll out the project and evaluate its success.</u></p> <p>For any reporting on technology in use, duration in place and type of usage from the Authority’s case management systems, e.g. MOSAIC, the Client data provided to the Project Team will be pseudonymised by the performance team. This will involve using unique identifiers and redaction of names, addresses, contact details, and any other identifiable information not required for the purpose of this project. This process will allow the project to adhere to KCC’s Anonymisation and Pseudonymisation Policy at all times.</p> <p>This pseudonymised report will include an assessment of the suitability of technology for an individual from their Practitioner. These reports are needed to ensure the service we are providing will continue to meet the needs of the clients</p>
--	---

and maximise their independence whilst enabling remote visiting to take place when needed. This information is necessary to assess the impact of Technology Enabled Care for different teams, however it is more sensitive which is why the decision has been made to pseudonymise it before it reaches the Projects Team.

In addition to the data provided in the pseudonymised reports, the Projects Team will obtain information on the type of technology used, the duration that the technology is used for and voluntary feedback provided by the service user and their family and friends (taken at intervals throughout the project to measure impact). This information will be collected and recorded through the chosen third party supplier's platform and will be used alongside the pseudonymised health information to evaluate the project. The information held on the supplier's system will be significantly less sensitive which is why the Projects Team will have full unrestricted access to this. It will include information such as name and address to enable the service provider to install and respond to queries regarding the technology.

It is likely that the provider / partner that the Authority works with will have a CRM of which will be secured on UK / EU servers and will require a separate login and password to do so. Compliance of this system will be checked with the Compliance and Risk Team during the evaluation of the tender responses. Data contained on this system and processed at the request of the authority will likely be:

- Case management reference no.
- Name
- Address
- Contact details (telephone and / or email)
- Delivery address for technology (if different to the living address)
- Contact details of any contacts or responders (friends, family, formal care providers, partner agencies)
- Details of Care package (sensitive as will contain details of that persons requirements such as any extenuating circumstances relating to care) – to help ensure the right technology is identified to meet the needs.

The system may also capture the following types of information:

- Motion sensor
- Temperature sensor
- Technology usage (quantity, duration and reason e.g. a fall or emergency services required)
- GPS location
- Video doorbells (subject to risk assessment following recent case law)

There will be no video surveillance products contained inside a person's home as part of Technology Enabled Care. KCC will not provide this on the basis that video surveillance is invasive and comes with increased processing risk. However, if requested, KCC will make available information, advice and guidance to enable the service user to self-purchase or to purchase via a Direct Payment (controlled by the person or their carer) independently to KCC and to this project.

Products

As part of the TECS project we aim to provide technological solutions specific to an individuals needs by having access to a broad-range of products and looking at the person as an individual and not as a 'one size fits all' approach. This could come in any of the following forms:

- Assistive technology - (e.g. smart devices such as televisions speakers, and home hubs, video doorbells, medication dispensers, remote door entry, robotics, wearables etc.)
- Mobile Applications (e.g. promotion of health, for wellbeing, undertaking daily activities etc.)

- Remote monitoring and communication (e.g. tablets, video phones, virtual calls to formal and informal network, sensory impairment communication tools, environment sensors, personal sensors, alarms etc.)

Data from these products will likely be pooled into a single platform or collated through the Internet of Things (IoT). As the providers and the products are not yet known, further details on this will need to be provided in due course.

Culture Change

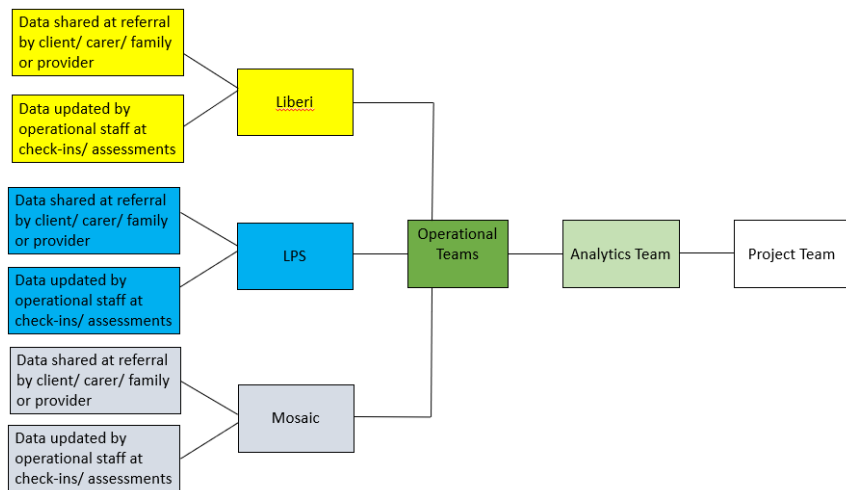
Starting a culture change for technology to be viewed at the outset as a preventative solution instead of using technology as a reactive solution to an incident. This will entail supporting Kent County Council members of staff to be confident using technology and have the appropriate skill levels to learn and use new technology as it becomes available.

The Project Team that will be reviewing the data will be comprised of members of the Innovation Delivery team and appropriate members of KCC operational teams based on their professional skill set (e.g. Commissioning, Finance, Social Care etc).

The data flow diagram below shows where the data will be created and sourced from.

The data will be input manually into the care platform by Practitioners. The analytics/performance team will then generate the pseudonymised reports for the Projects Team from these platforms. The pseudonymised data will be combined by the project team, with data collected directly from the third party service provider's platform, to inform their analysis.

Data Flow



5.1 What is the purpose of the processing?

a) What do you want to achieve? We are processing this data to ensure that the solutions that are being utilised are the best possible solution for the individual dependent on their needs.

b) What is the intended effect on individuals?♦ Technology Enabled Care is designed to empower people and enable to live independently for longer in an environment they want to be in. This will be provided as part of choice and control over their own care and support plan based on their assessed needs under the Care Act 2014. Harnessing Technology Enabled Care will provide greater safety in and out of the home, response in an emergency, prevention of a crisis and assurances to the person and their informal support network. Technology Enabled Care could also be seen as less intrusive, particularly for those who want to be independent and do not want to be reliant of traditional

	<p>care and support provisions if not required.</p> <p>Social Care professionals will benefit by having a greater understanding of technology solutions, be empowered in their role by enabling varied and innovative solutions, be confident in suggesting and using technological solutions resulting in client satisfaction. It may also help demand where technology could replace the need for physical visits for some people with certain types of needs where this allows.</p>
--	--

<p>c) What are the benefits of the processing for KCC, and more broadly?♦</p>	<p><u>Expected Key Benefits</u></p> <ul style="list-style-type: none"> • People satisfaction <ul style="list-style-type: none"> ○ This is a key outcome of the Strategic Reset Programme as well as the Making a difference every day approach. With additional assistive technology tools available for Practitioners to utilise to meet care and support needs, it is expected that people's satisfaction levels should increase. This will be an increased satisfaction for both the end users, their families and friends, but also the KCC staff who support them. • Partnership working / opportunities <ul style="list-style-type: none"> ○ Technology Enabled Care will benefit the wider health and social care system and not just the authority once the culture and awareness of the opportunities has been evidenced. For instance, utilising data and information to identify patterns in behaviours to become more preventative rather than reactive in terms of health, care and support delivered • Demand <ul style="list-style-type: none"> ○ Providing greater information, advice and guidance on assistive technology across all areas of the social care pathways and how this can be accessed will support demand on formal social care services ○ Utilising assistive technology to provide remote support, targeting those who are in need of support through data and analytics, or empowering the informal support network of people to help manage and respond to changes in need or reactive support (e.g. a fall). • Authority <ul style="list-style-type: none"> ○ Through using Technology Enabled Care, there could be opportunities to not only meet the outcomes of people but also reduce or delay escalation of need but also reduce the need for other traditional care and support methods in favour of assistive technology (where suitable). In some instances, assistive technology could prevent the need for any formal social care intervention. We anticipate that the use of this technology should have an additional benefit of releasing some of the capacity in the provider market, where it is currently being used in a traditional face to face approach only. • Environmental <ul style="list-style-type: none"> ○ Through assistive technology, this could also reduce the needs for physical visits to people we support, therefore reducing the use of vehicles for social care professionals.
--	--

5.2 What is the scope of the processing?

<p>a) Types of personal data♦</p>	<p><u>Personal data:</u></p> <ul style="list-style-type: none"> • Case management reference no. • Name • Marital Status • Address • Contact details • Delivery address for technology (if different to the living address)
--	--

	<ul style="list-style-type: none"> · Contact details of any contacts or responders (friends, family, formal care providers, partner agencies) · Age · Living address/ arrangements · Sex <p><u>Special category data, or containing special category data:</u></p> <ul style="list-style-type: none"> · Ethnicity · Disability · Religious Belief · Pregnancy / Maternity Status · Gender Identity/Reassignment information · Sexuality · Details of Care package · Details of medication used <p>Note that the service users' full medical records will only be held within MOSAIC etc and therefore will not be accessible by the Projects Team or third party supplier.</p> <p>The Projects Team has not yet decided the feedback format – i.e. they may receive granular feedback on a service user-by-service user basis which may reveal additional information about a service user, or alternatively this could be an anonymous restricted fields questionnaire with all responses aggregated.</p>
<p>b) How many individuals will be affected and what geographical area will it cover?</p>	<p>Clients This will be a countywide approach for Technology Enabled Care and will cover the whole of Kent</p> <p>The number of people impacted by this change will depend on the individuals assessed needs. Therefore, theoretically although extremely unlikely, all or none of the people we support during this period are suitable for Technology Enabled Care. So all contacts through to Adult Social Care will lead to an assessment and therefore provision of Technology Enabled Care. As an indication we have over 6000 people being supported by traditional Telecare options, and over a thousand are utilising the KARA Carephone. These figures are the base for our current review of how many people will be supported.</p>
<p>c) How much data will be collected and used?</p>	<p>Data will be proportionate to the requirements of the individuals. Those with more complex needs may require / want more assurance and therefore more technology and data is collated. Others may want a more light touch approach and therefore will be provided with an appropriate solution to do so. This will be ascertained through the assessment process for social care Practitioners.</p> <p>As for the provision of Technology Enabled Care, this is yet to be determined until the provider / partners and associated products have been identified following the procurement process. However, here is an indication as to the possibilities:</p> <ul style="list-style-type: none"> · Voice / voice call records (not recordings of the conversation, just data and time stamp types of information). · Status of the technology (inactive / active / errors) · User name · Sequence · Number · Received Local Time · Call Reason · Received Local Time · Battery Level · Charging · Reminder Id · Reminder Scheduled Local Time · Occurred Local Time · Status · Response · Motion / movement · Temperatures

GPS location


Further details will be added here once the offer and provider is understood

d) Length and frequency of processing


The contract between KCC and the provider / partner is for a period of 5 years, commencing from 2023 and therefore concluding in 2028. The data is processed when the technology is requested by the practitioner and is then by the Users, which will occur for each time that an item is identified as being needed.

e) How long will the data be retained for?

Personal information will be kept securely in accordance with [Information Security](#) and GDPR data principles (i.e.: Article 5(1)(e), 'personal data should not be kept any longer than necessary'. It is the responsibility of the project team to ensure this is adhered to.



Information Security Policy.docx



Records Management Policy.p

The project team will adhere to KCC's Records Management Policy (enclosed above) with reference to its Retention Schedule. (See sections AS1 – 6 (excluding AS2.1, AS2.2, AS4.4, AS4.5, AS4.9, AS4.10, AS4.11, AS4.12.15, AS4.12.16, AS4.13, AS5.2, AS6.1) which provides a breakdown of the retention periods relied on by Adult Services).

<i>Project documentation created for internal projects which may not result in a contract</i>	<i>Last action on the project + 6 years</i>
<i>Project files relating to research undertaken to see if projects are viable</i>	<i>End of operational use</i>
<i>Correspondence which does not merit inclusion on the project files</i>	<i>Last action on project + 1 year</i>
<i>Project documentation created as part of a project where the creator is not the project manager or designated record keeper for the project.</i>	<i>Life of Project</i>

All staff working within the Project Team are trained to follow KCC's Data Breach Policy.

Details of the care and support provided to an individual will be added as a record to Mosaic by the practitioner recommending the technology, and depending on which service the individual is receiving will determine the retention period for keeping this information.



5.3 What is the nature of the processing?

a) How will the data be collected and what is the source of the data?

The project team do not and will not have direct access to the case management systems e.g. MOSAIC, therefore they will seek support from the Adult Social Care and Health Performance Team. The provider / partner will also not have access to MOSAIC and will only be provided with the data required to deliver the services set out in the contract and as described in this document.

The assessed needs of the person will be undertaken by the Social Care professionals. Therefore, those who will require Technology Enabled Care as part of their care and support plan will be passed directly to the provider to commence the service provision. This is no different to other purchasing functions within the Authority.

For any reporting on technology in use, duration in place and type of usage from the Authority's case management systems, e.g. MOSAIC, the Client data provided to

	<p>the Project Team will be pseudonymised by the performance team or the operational teams where unique identifiers are needed, including redaction of names, addresses, contact details, and any other identifiers or information not required for the purpose of this project. This data is needed to ensure the service we are providing will continue to meet the needs of the clients and maximise their independence whilst enabling remote visiting to take place when needed. Client data that will be used within this project is stored on one of the following Kent County Council live database - Mosaic, Liberi or LPS.</p> <p>Data from this products will likely be pooled into a single platform or collated through the Internet of Things (IoT). As the providers and the products are not yet know, further details on this will need to be provided in due course.</p>
<p>b) How will the data be used and stored ♦</p>	<p>Project documents will be stored on Microsoft Teams in a folder that has restricted access, which only the project team and their senior management team will also have access. Information and data relating to the person / client will be stored on the case management system. Data will also be retained on the providers CRM / platform in order to effectively deliver the service (as listed above).</p> <p>When reporting is required from the case management system, pseudonymising the data front line teams and the performance team will replace the names with unique identifiers to fall in line with GDPR responsibilities. Below is KCC's Anonymisation and Pseudonymisation policy which complies with ICO 2012.</p> <p> Anonymisation and pseudonymisation p</p> <p>It is likely that the provider / partner that the Authority works with will have a CRM of which will be secured on UK / EU servers and will require a separate login and password to do so. Compliance of this system will be check with the Compliance and Risk Team during the evaluation of the tender responses. Further details will need to be provided once known.</p>
<p>c) 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)? ♦</p>	<p>As part of the Project Team's internal process, once a Teams site has been created, only the member of Project Team working directly on that project is able to grant access to new users accessing the site. The Project Team will control the management of the Teams site and will regularly review the membership of each colleague who has access to the channel to ensure that only relevant users have access. Within the Project Team, peer training for Teams takes place as part of the induction process to ensure staff are familiar and confident with Teams. Teams training has also been made available on Delta, Kent County Council's E-Learning site, which is to be completed by each member of the Project Team. Also as part of the induction process for all members of the Project Team, GDPR training must be completed routinely to ensure staff awareness is at a premium.</p> <p> Data Breach Policy.docx</p> <p>KCC ASCH staff are trained to follow the breach policy (above) and refresh their mandatory training every 2 years, including GDPR (Data Protection Essentials) and Introduction to Information Governance. NHS Data Security Level 1 will also be required by the KCC ASCH staff, and this is required to be refreshed on a yearly basis.</p> <p>It is likely that the provider / partner that the Authority works with will have a CRM of</p>

which will be secured on UK / EU servers and will require a separate login and password to do so. Compliance of this system will be check with the Compliance and Risk Team during the evaluation of the tender responses. Further details will need to be provided once known.


The way in which data is transferred to and from the Authority is yet to be determined and this will need to be updated once known following procurement exercise.

d) How will the data be deleted/disposed of? ♦

Files will be deleted from the MS Teams site in line with their respective retention periods by the Innovation Delivery Team in accordance with KCC policy, see [Records Management Policy](#):

<i>Project documentation created for internal projects which may not result in a contract</i>	<i>Last action on the project + 6 years</i>
<i>Project files relating to research undertaken to see if projects are viable</i>	<i>End of operational use</i>
<i>Correspondence which does not merit inclusion on the project files</i>	<i>Last action on project + 1 year</i>
<i>Project documentation created as part of a project where the creator is not the project manager or designated record keeper for the project.</i>	<i>Life of Project</i>

Generic Project documentation which does not contain personal data, e.g., Project Plans, Risk Logs, Decision Logs, will be kept in line with their retention period (see **5.2 e** of this document) and Disposal-flow-chart below.

 Disposal-flow-chart.pdf

e) Will the data be shared/disclosed to third parties? ♦¹

Yes No

Information may need to be shared with companies to instal the relevant technology.

Generalisations from the data may be used in conversations with suppliers / providers and other Local Authorities that the Project team may speak with, for example “we have X clients using our service” or “50% of our clients are male”. However this will not constitute personal data.

f) What types of processing identified as likely high risk are involved? ♦

The key risks involved are misuse or unauthorised disclosure of special category data about service users, including those that are vulnerable. This is mitigated because of the security measures implemented and limiting access to such data to only those personnel that require access in relation to their job role.

The risk of data subject claims and mistrust is mitigated due to the transparent privacy notice information that will be provided, the choice given to service users and the steps that will be taken during mobilisation to ensure that data is secure before the project is launched with the public.

Reference needs to be made to the Screening Tool criteria selected that identifies the types of processing that are likely to be high risk.

5.4 What is the context of the processing?

a) What are the categories of data

- 0-17 clients using ASCH services (Children’s Service)

<p>subject, and do they include children or vulnerable groups? ♦</p>	<ul style="list-style-type: none"> • 18-25 clients using ASCH services (Children’s Service) • 26+ clients using ASCH services <p>It should be noted that there is an imbalance of power between the data controller and each of the data subjects i.e. it may be harder for data subjects to oppose to the processing of their data. All data subjects are vulnerable groups with these groups including vulnerable children.</p> <ul style="list-style-type: none"> • Carers and parents/guardians • Other relatives and friends <p>In each case to the extent required to provide feedback.</p>
<p>b) What is the nature of the relationship with individuals?♦</p>	<p>The authority is a provider of services to clients. It should be noted that there may be an imbalance of power between the data controller and data subject i.e. it may be harder for data subjects to oppose to the processing of their data.</p> <p>There may be a time when client family/ guardian data is used to ensure robust support networks are in place to support a known client.</p>
<p>c) How much control will they have?</p>	<p>As shown in the General (Privacy) notice to cover adult social care and health: Client rights to request the data the Council holds on them and the right to leave the service etc., remain unaffected. An easy read format of Adult Social Care and Health (General) Privacy Notice is also available to facilitate Learning Disabilities or vulnerable clients.</p> <p>A specific TECS privacy notice will be provided at the point of installation of any technology, and will be published on the KCC web page with the ASCH General Privacy Notice.</p> <p>Under GDP Regulations, clients have a number of rights, which they can access free of charge, which allow them to:</p> <ul style="list-style-type: none"> • Understand what we are doing with their information and for what purpose • Ask to see the information held about them • Ask the authority to correct any mistakes in the information we hold about them • Object to direct marketing • Make a complaint to the Information Commissioners Office/ Ombudsman <p>As part of the project, there will be regular check ins with the people with the technology to make sure it is meeting their needs as assessed. In the event this technology is not, this can be reviewed, and alternative measures put in place to support them.</p>
<p>d) Would they expect you to use their data in this way?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Restructures, Redesign or improvement projects are common within any organisation with the work being undertaken within the TECS project to ensure that clients have the opportunity to remain independent for as long as possible while providing clients the opportunity to have a say in the care they are receiving. The technology solutions advised are to ensure the welfare of the client they are being advised for.</p> <p>Clients would expect that Adult Social Care is advising and implementing the most appropriate and effective care packages to meet their needs, making adjustments</p>

	as their packages progress to ensure it continues to be the most appropriate and cost-effective package to meet their needs. All residents of Kent expect for KCC budgets to be spent based on the best value for money for the taxpayers of Kent, which would include the most efficient ways of working.
e) Are there prior concerns over this type of processing or security flaws?	No.
f) Is it novel in any way?	No – these are established technologies, it is just a new initiative for KCC.
g) What is the current state of technology in this area?	<p>Client data is held inside the Liberi, LPS and Mosaic database and is accessed both directly and through PowerBI, our analytics reporting software, which interfaces with the Liberi, LPS and Mosaic database and runs automatic reports and is managed by the Performance team (ASCH). This data is then exported manually from Power BI and stored in spreadsheets within Microsoft Excel or as a pdf.</p> <p>While existing common technologies have been used to build efficiency into the processing and storage of data, and in regard to this project analysis carried out within Microsoft Excel has been used to identify cases to review, ultimately all outcomes are based on human decisions.</p> <p>Some clients will currently have access to telecare services (such as emergency buttons, sensors etc.) currently, however, Technology Enabled Care project will enable video calling.</p> <p>Devices Alcove eco system is built with security by design and underlying infrastructure is state of the art.</p>
h) Are there any current issues of public concern that you should factor in?	N/A
i) Are you signed up to any approved code of conduct or certification scheme? ♦²	N/A

6. Consultation			
Who will you consult? ♦³	When will you consult? ♦⁴	How will you consult?	Responses ♦⁵
Clients of the affected services	Clients will be consulted within Social Care practices (e.g. assessments, a review) when exploring options for their service provision.	<p>Social Care Practice</p> <p>By visiting a client directly on a visit or attending a virtual meeting/ appointment.</p>	Responses will be received ongoing throughout the project but at a time when the correct solution is being explored.
Providers specialising in technology and innovative solutions	A market engagement event must take place to enable interested providers to register their interest to be a part of the contract and enable the Project Team to make an informed decision around the provider we plan to award the contract too.	Market engagement event to be advertised on the Kent Commissioning Portal for 30 days to allow for submissions. Each provider to	Responses will be received at the outset of the project to enable us to train our winning provider in the new ways of working.

	The winning provider will be consulted regularly throughout the project lifecycle to ensure adequate skill levels and confidence in new way of working.	then create a presentation for the Project Team to understand what they can offer. (Online) meetings and email communications will be the primary method.	
Project Management Team	At all stages of the project.	(Online) meetings and email communications will be the primary method. Regular monthly meetings will take place to ensure all members of the project group can receive updates and give direction.	Responses will be received throughout the project and used to inform the work, where necessary.
Kent County Council's Senior Management Team	At all stages of the project.	(Online) meetings and email communications will be the primary method. Regular monthly meetings will take place to ensure all members of the Senior Management Team can receive updates and give direction.	Responses will be received throughout the project and used to inform the work, where necessary.
Other experts, e.g. IT, legal, Finance or other professionals	Other experts include Cantium (03000 415555), KCC's ICT provider. Akua Agyepong ASCH Assistant Director County (Specialisms) Akua.Agyepong@kent.gov.uk (Social Work Professional)	(Online) meetings and email communications will be the primary method.	Responses will be received throughout the project and used to inform the work, where necessary.

	Janine Hudson, Social Work Professional, Janine.Hudson@kent.gov.uk		
Adult Social Care Governance Lead	During project development	(Online) meetings and email communications will be the primary method.	Responses will be received throughout the project and used to inform the work, where necessary. Provide comments on draft DPIA.
Social Workers/Front Line Staff	During project development and throughout the life of the project	(Online) meetings and email communications will be the primary method	Technology For Independent Living Facilitators in conjunction with the Prescribers and Project Team will keep Social Workers and Front Line Staff aware of any technological developments. NRS will provide direct guidance on using the technology during the install, and will be responsible for ongoing repair to damages and faults.
DPO	DPO Support team to be consulted on the draft of the document.	(Online) meetings and email communications will be the primary method.	DPO Support team will be consulted in the final draft and their comments accounted for in the approved version, where deemed appropriate.

7. Assess necessity and proportionality

a) What is the lawful basis for processing? ♦ ⁶	<i>GDPR Article 6(1) Legal Basis</i>	<i>GDPR Article 9(2) Special Category Data Exception [If processing special category data]</i>
	<input type="checkbox"/> (a) The data subject has given consent for one or more specific purposes <input type="checkbox"/> (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract <input type="checkbox"/> (c) Processing is necessary for compliance with a legal obligation to which the controller is subject <input type="checkbox"/> (d) Necessary in order to protect the vital Interests of the data subject or another natural person	<input type="checkbox"/> (a) Explicit Consent for one or more specified purposes <input type="checkbox"/> (b) Necessary for Employment/Social Security/ Social Protection obligations (subject to a DPA 18 condition – also complete Table 1 below) <input type="checkbox"/> (c) Necessary to protect the vital Interests of the data subject or of another natural person where a data subject is physically or legally incapable of giving consent <input type="checkbox"/> (d) Legitimate activities by foundation, association, or not-for-profit body with political, philosophical, religion, or trade union aim <input type="checkbox"/> (e) Relates to data manifestly made public by data subject <input type="checkbox"/> (f) Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity <input checked="" type="checkbox"/> (g) Necessary for substantial public interest (on

	<p><input checked="" type="checkbox"/> (e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</p> <p><input type="checkbox"/> (f) Necessary for legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child – also complete Legitimate Interests section below</p>	<p>the basis of a DPA condition – also complete Table 2b below) and which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of data subjects</p> <p><input checked="" type="checkbox"/> (h) Necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health or social care systems and services (subject to a DPA 18 condition – also complete Table 1 below) or pursuant to contract with a health professional and subject to the conditions and safeguards in 9(3)</p> <p><input type="checkbox"/> (i) Necessary for reasons of public interest in the area of public health (subject to a DPA 18 condition – also complete Table 1 below)</p> <p><input type="checkbox"/> (j) Necessary for archiving purposes in the public interest, scientific, or historical research purposes in accordance with Article 89(1) (subject to a DPA 18 condition- also complete Table 1 below) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.</p>
--	--	--

<p>b) When required, depending on the Article 9 exception relied upon, you must add the conditions you are also relying on from Schedule 1 of the DPA 2018</p>	<p>If you are relying on Article 9 exemptions b, h, i, or j, you must also identify one of the additional conditions from Schedule 1, Part 1, of the DPA 2018. Listed below in Table 1:</p> <table border="1" data-bbox="319 1209 1552 2065"> <thead> <tr> <th data-bbox="319 1209 558 1288">Table 1</th> <th data-bbox="558 1209 1552 1288">DPA 2018 Schedule 1, Part 1 Additional Conditions</th> </tr> </thead> <tbody> <tr> <td data-bbox="319 1288 558 2065"> <p>Schedule 1, Part 1, DPA 2018 additional conditions that must be met if using GDPR Article 9 Special Category Data exceptions (b), (h), (i), or (j) ◆⁷</p> </td> <td data-bbox="558 1288 1552 2065"> <p><input type="checkbox"/> (1) Employment, social security, social protection ◆⁸ Go to Table 2a</p> <p><input checked="" type="checkbox"/> (2) Health or social care purposes ◆⁹</p> <p><i>9(3)GDPR states that data to be processed for health or social care purpose where under the responsibility of a professional subject to the obligation of professional secrecy under UK law or rules established by national competent bodies or by another person subject to an obligation of secrecy under UK law or rules established by national competent bodies.</i></p> <p><i>S11(1) DPA 18 states that processing must be –</i></p> <p>(a) <i>by or under the responsibility of a health or social work professional</i></p> <p>(b) <i>by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.</i></p> <ul style="list-style-type: none"> Responsible professional: All Practitioners (qualified health and social work professionals) within the network which utilise the technology as part of the care plans for their service users. NB: Akua Agyepong is Assistant Director (Countywide) and Janine Hudson Service Manager, Adult Mental Health <p><input type="checkbox"/> (3) Public Health ◆¹⁰</p> </td> </tr> </tbody> </table>	Table 1	DPA 2018 Schedule 1, Part 1 Additional Conditions	<p>Schedule 1, Part 1, DPA 2018 additional conditions that must be met if using GDPR Article 9 Special Category Data exceptions (b), (h), (i), or (j) ◆⁷</p>	<p><input type="checkbox"/> (1) Employment, social security, social protection ◆⁸ Go to Table 2a</p> <p><input checked="" type="checkbox"/> (2) Health or social care purposes ◆⁹</p> <p><i>9(3)GDPR states that data to be processed for health or social care purpose where under the responsibility of a professional subject to the obligation of professional secrecy under UK law or rules established by national competent bodies or by another person subject to an obligation of secrecy under UK law or rules established by national competent bodies.</i></p> <p><i>S11(1) DPA 18 states that processing must be –</i></p> <p>(a) <i>by or under the responsibility of a health or social work professional</i></p> <p>(b) <i>by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.</i></p> <ul style="list-style-type: none"> Responsible professional: All Practitioners (qualified health and social work professionals) within the network which utilise the technology as part of the care plans for their service users. NB: Akua Agyepong is Assistant Director (Countywide) and Janine Hudson Service Manager, Adult Mental Health <p><input type="checkbox"/> (3) Public Health ◆¹⁰</p>
Table 1	DPA 2018 Schedule 1, Part 1 Additional Conditions				
<p>Schedule 1, Part 1, DPA 2018 additional conditions that must be met if using GDPR Article 9 Special Category Data exceptions (b), (h), (i), or (j) ◆⁷</p>	<p><input type="checkbox"/> (1) Employment, social security, social protection ◆⁸ Go to Table 2a</p> <p><input checked="" type="checkbox"/> (2) Health or social care purposes ◆⁹</p> <p><i>9(3)GDPR states that data to be processed for health or social care purpose where under the responsibility of a professional subject to the obligation of professional secrecy under UK law or rules established by national competent bodies or by another person subject to an obligation of secrecy under UK law or rules established by national competent bodies.</i></p> <p><i>S11(1) DPA 18 states that processing must be –</i></p> <p>(a) <i>by or under the responsibility of a health or social work professional</i></p> <p>(b) <i>by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.</i></p> <ul style="list-style-type: none"> Responsible professional: All Practitioners (qualified health and social work professionals) within the network which utilise the technology as part of the care plans for their service users. NB: Akua Agyepong is Assistant Director (Countywide) and Janine Hudson Service Manager, Adult Mental Health <p><input type="checkbox"/> (3) Public Health ◆¹⁰</p>				

	<p><input type="checkbox"/> (4) Research etc ♦¹¹.</p> <hr/> <p>If you are relying on Article 9 exemption g, you must also rely upon additional conditions from Schedule 1 Part 2 of the DPA 2018. Please go to Table 2b to select the additional conditions being relied upon</p> <hr/> <p>If you are processing data related to Criminal Convictions ♦¹², you must also identify one of the additional conditions from Schedule 1, Part 3 of the DPA 2018 Please go to Table 3 to select the additional conditions being relied upon</p> <hr/> <p>If you are required to have an Appropriate Policy Document by the conditions in part 1, 2 or 3, of Schedule 1 that you are relying on, this Appropriate Policy Document must be in accordance with the guidelines laid out in Schedule 1, Part 4 of the DPA 2018. Please go to Table 2a to confirm these requirements are met.</p> <hr/>
<p>c) Law Enforcement Processing not carried out under GDPR (where applicable) ♦¹³</p>	<p>Law Enforcement Processing under Part 3 of the Data Protection Act 2018 Confirm the underlying statutory authority (the law conferring this function): [ADD NAME OF AUTHORISING LEGISLATION e.g.] and Confirm the lawful basis under DPA:</p> <p><input type="checkbox"/> 35 (2) (a) the data subject has given consent to the processing for the law enforcement purposes, or <input type="checkbox"/> 35 (2) (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority</p> <p>Confirm (where applicable) the lawful basis for any sensitive processing:</p> <p><input type="checkbox"/> 38(4) (a) the data subject has given consent to the processing for the law enforcement purposes and <input type="checkbox"/> 38 (4) (b) an appropriate policy document is in place</p> <p><input type="checkbox"/> 38 (5) (a) the processing is strictly necessary for the law enforcement purpose and <input type="checkbox"/> 38 (5) (b) the processing meets one of the following conditions (from Schedule 8 of the DPA 18):</p> <ul style="list-style-type: none"> <input type="checkbox"/> (1) statutory purposes ♦¹⁴ <input type="checkbox"/> (2) administration of justice ♦¹⁵ <input type="checkbox"/> (3) protecting an individual’s vital interests ♦¹⁶ <input type="checkbox"/> (4) safeguarding of children and of individuals at risk ♦¹⁷

	<input type="checkbox"/> (5) personal data already in the public domain ¹⁸ <input type="checkbox"/> (6) legal claims ¹⁹ <input type="checkbox"/> (7) judicial acts ²⁰ <input type="checkbox"/> (8) preventing fraud ²¹ <input type="checkbox"/> (9) archiving etc ²² And <input type="checkbox"/> 38 (5) (c) an appropriate policy document is in place <input type="checkbox"/> Please tick to confirm your appropriate policy document is attached. <i>If not attached please explain why not</i>
d) Legitimate interests	N/A
e) Any other relevant legal basis or that support the GDPR basis (e.g. legal obligation or statutory purposes)	<p>For the purposes of the public interest processing condition, statutory and government purposes under DPA 2018, Schedule 1, para 6(2)(a) the below legislation confers functions on KCC:</p> <ul style="list-style-type: none"> • Care Act 2014 Part 1.18 • Mental Capacity Act 2005 Part 1.4 • Mental Health Act 1983 Part VIII <p>In addition KCC must have due regard to the Equality Act 2010 when carrying out its functions.</p>
f) What information will you give to individuals?	<p>Clients are directed to the Privacy Notices held on Kent.gov.uk, available here. This notice covers the information we hold about our clients and how we will use it.</p> <p>In addition, a new standalone privacy notice will be drafted for the technology enabled care trial. This will be provided a) in advance by directing the individual to the notice on the KCC site – so that information is available as part of the decision making process; and b) also in hard copy when the user receives their kit.</p> <p>This will be drafted once the third party provided has been selected as the processing details cannot be confirmed until then. Additionally, the information will vary depending on the devices used and so some additional information may need to be provided on a device-specific basis.</p>
g) Does the processing achieve your purpose?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
h) Is there another way to achieve the same outcome?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
i) How will you prevent function creep and preserve the second data protection principle: ‘purpose limitation’ (i.e. 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	<p>The project will have a Business Case with a clear plan and scope identified to ensure that irrelevant information isn't provided or analysed, by using a defined controlled set of questions to the User. This will drive only information gathered that is both relevant to that person, but also required to allow the installation of the agreed equipment.</p> <p>Access will also be restricted by using tiered access rights and password protection. Once the third party provider has been selected, more information will be available on additional technical measures implemented for this purpose.</p>

those purposes ♦	
j) How will you ensure data quality and minimisation? ♦ ²³	<p>People identified as being suitable for this provision will be done so through a care needs assessment. Only those that have needs which can be met by Technology Enabled Care will be referred into the service and those data processed for this purpose.</p> <p>Those that have an assessed need and do not require Technology Enabled Care, their details will not be processed with this provider.</p> <p>Of those that are deemed suitable for this provision based on their needs, only the data required to effectively deliver the service, as listed above, will be processed (see section 5.2(a) and 5.2(c)).</p>
k) How will you ensure personal data is accurate and, where necessary, kept up to date	<p>Client and staff data provided to the Project Team will be pseudonymised by the analytics team or the operational teams where unique identifiers are needed, including redaction of names, addresses, contact details, and any other identifiers or information not required for the purpose of this project. This data that the Project Team does receive, is needed in order to evaluate use of technology enabled care and to ensure the service we are providing will continue to meet the needs of the clients and maximise their independence whilst enabling remote visiting to take place when needed. Client data that will be used within this project is stored on one of the following Kent County Council live database - Mosaic, Liberi or LPS.</p> <p>The data itself has been pulled from the live databases and should therefore be current and correct. In the event of data being in a poor condition (e.g. obvious errors, 'blanks' instead of 0's where appropriate in excel documents) the data will be challenged with the operational team.</p>
l) How will you support data subject rights? ♦ ²⁴	<p>Data subject rights remain unaffected by this work. Data required for the assessment will be minimised as much as possible, pseudonymised, and proportional to the needs of the project.</p> <p>Under GDPR data subjects have rights which can be exercised free of charge (Privacy Notices held on Kent.gov.uk, available here) which allow them to:</p> <ul style="list-style-type: none"> • know what we are doing with their information and why we are doing it • ask to see what information we hold about them (subject access request) • ask us to correct any mistakes in the information we hold about them • object to direct marketing • make a complaint to the Information Commissioner's Office <p>Depending on our reason for using your information they may also be entitled to:</p> <ul style="list-style-type: none"> • ask us to delete information we hold about them • have their information transferred electronically to themselves or to another organisation • object to decisions being made that significantly affect them • object to how we are using their information • stop us using their information in certain way <p>An easy read privacy notice covering KCC Adult Social Care and Health is available on the KCC website to support children/vulnerable adults. The new standalone privacy notice will also be available in an accessible format, to support children/vulnerable adults.</p>
m) What measures do you take to ensure processors comply? ♦ ²⁵	<p>The contract with the third party service provider (not yet selected) contains Article 28 processing conditions.</p>
n) How do you safeguard international transfers? ♦	<p>We are not working with any international suppliers on this project, and do not intend to send any data internationally. The third party service provider contract also prohibits transfers of personal data outside of the EU without consent.</p>

8. Identify and assess risks

(you can refer to the risk matrix attached to help assess the level of risk)

8.1 Risks to INDIVIDUALS

Risk Number	Risk Description	Likelihood of harm	Severity of harm	Overall risk
8.1.1	Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.	<input type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input checked="" type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Significant <input type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.1.2	Collecting information and linking identifiers might mean that we no longer use information that is safely pseudonymised i.e. the projects team may be able to identify the individuals that pseudonymised reports from MOSIAC relate to.	<input checked="" type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> Significant <input type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.1.3	Information may be collected and stored unnecessarily, or not properly managed so that duplicate records are created, presenting a greater security risk.	<input type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input checked="" type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Significant <input type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.1.4	Failure to establish appropriate retention periods might mean information is used for longer than necessary.	<input checked="" type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Significant <input type="checkbox"/> Serious <input type="checkbox"/> Major	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High
8.1.5	Information collected for an individual's formal and informal network without their permission	<input checked="" type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input checked="" type="checkbox"/> Minor <input type="checkbox"/> Moderate <input type="checkbox"/> Significant <input type="checkbox"/> Serious <input type="checkbox"/> Major	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High
8.1.6	Relevant social worker practitioners do not receive enough training to be able to prescribe the correct technology	<input type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input checked="" type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> Significant <input type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.2 Organisational risks				
8.2.1	Non-compliance with the GDPR or other legislation, which can lead to sanctions, fines and reputational damage.	<input type="checkbox"/> Very unlikely <input checked="" type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input type="checkbox"/> Significant <input type="checkbox"/> Serious <input checked="" type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.2.2	Problems may only be identified after the project has launched and will then be more likely to require expensive fixes.	<input type="checkbox"/> Very unlikely <input checked="" type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input type="checkbox"/> Significant <input checked="" type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.2.3	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.	<input type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input checked="" type="checkbox"/> Possible	<input type="checkbox"/> Minor <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Significant	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High

		<input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Serious <input type="checkbox"/> Major	
8.2.4	Public/client/customer distrust about how information is used may damage KCC's reputation.	<input checked="" type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input type="checkbox"/> Significant <input checked="" type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.2.5	Data losses which damage individuals could lead to claims for compensation.	<input checked="" type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input type="checkbox"/> Significant <input type="checkbox"/> Serious <input checked="" type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.3 Legal compliance risks				
8.3.1	Non-compliance with the GDPR - i.e. will the processing meet the principles in Article 5 GDPR ♦ ²⁶	<input checked="" type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input type="checkbox"/> Significant <input checked="" type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High
8.3.2	Non-compliance with sector specific legislation or standards.	<input checked="" type="checkbox"/> Very unlikely <input type="checkbox"/> Unlikely <input type="checkbox"/> Possible <input type="checkbox"/> Likely <input type="checkbox"/> Very likely	<input type="checkbox"/> Minor <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> Significant <input type="checkbox"/> Serious <input type="checkbox"/> Major	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Medium <input type="checkbox"/> High

9. Identify and evaluate measures to reduce risk					
Potential solution	Which risk(s) would this action address? ♦ ²⁷	Effect on risk	Residual risk	Cost/benefit/evaluation ♦ ²⁸	Measure approved?
<p>People will be provided Technology Enabled Care if it can meet their unmet eligible needs following their Care Needs assessment with a social care professional. As part of this process it provides the person with choice and control of their care.</p> <p>Should Technology Enabled Care be selected, information and purpose of the</p>	8.1.1	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	The minimum information is requested, including only using the persons MOSAIC identification number, to reduce the risk of private information being leaked.	<input type="checkbox"/> Yes <input type="checkbox"/> No

equipment and the data collected will be explained to the person in receipt or a representative if preferred. Privacy notice will also be available.					
Information captured will be within the providers compliant database or on the Authority's case management system. Individuals will be identified by their MOSAIC ID number as this is unique to the individual rather than other personal information. All KCC personnel including the projects teams are subject to obligations of confidentiality, meaning that even if service users are identifiable within reports, the risk of unauthorised disclosure is reduced.	8.1.2	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	The majority of the direct Project Team do not have access to MOSAIC details, so could not identify an individual. Those that do have access are bound but the same KCC governance rules regarding using information that they have access to.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Information will be stored on compliant databases and not in spreadsheets outside of these platforms.	8.1.3	<input checked="" type="checkbox"/> Risk eliminated <input type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	No outside spreadsheets will be utilised, so all information is stored only on compliant databases to avoid risk of loss. Staff communications and training will be central to ensure they are fully aware of their responsibilities	<input type="checkbox"/> Yes <input type="checkbox"/> No
Retention of records for the project will be in line with KCC retention policy as set out in section 5 of this document.	8.1.4	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	All retention periods will be followed to ensure we are compliant with data protection principle Article 5(1)€ storage limitations. Staff communications and training will again be central to ensure they are fully aware of their responsibilities	<input type="checkbox"/> Yes <input type="checkbox"/> No
People will be	8.1.5	<input checked="" type="checkbox"/> Risk eliminated	<input checked="" type="checkbox"/> Low	A revised Privacy	<input type="checkbox"/> Yes

informed of their details being used as part of the agreement with the care and support planning process. People can request that these be removed at any point throughout the service provision.		<input type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input type="checkbox"/> Medium <input type="checkbox"/> High	Notice will be supplied detailing exactly what each individuals rights are, and the process they need to follow should they want their details to be removed at any stage.	<input type="checkbox"/> No
Fully trained experienced practitioners will be available at all times to provide guidance and training, and help with ongoing staff knowledge	8.1.6	<input checked="" type="checkbox"/> Risk eliminated <input type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	To ensure that staff are aware of their data protection obligations and therefore ensure that data is used and shared safely and securely	<input type="checkbox"/> Yes <input type="checkbox"/> No
Equipment will be prescribed by KCC in line with the other legislation such as, but not limited to, Care Act 2014, Mental Health Act 1983, Mental Capacity Act 2005 Equality Act 2010, Privacy notices and associated GDPR protocols are adhered to as part of this process. Those who are not known to the Authority, and suitable for Technology Enabled Care, will be provided information, advice and guidance to seek their own solutions with trusted providers of this type of service.	8.2.1	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	Full compliance with GDPR protocols will be followed at all times and be adhered to as part of the ongoing process	<input type="checkbox"/> Yes <input type="checkbox"/> No
The project team will test the compliance of the providers provision during the procurement process. The Authority and the provider will work together to put in place measures to ensure data is secure during mobilisation before introduced to the public.	8.2.2	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	The Authority has experience working with NRS previously, and as part of the Test and Build project. Knowledge of our data security is well known. This will be reviewed throughout the contract to ensure it is kept at a minimum risk	<input type="checkbox"/> Yes <input type="checkbox"/> No
Records relating delivery of the service will be maintained on	8.2.3	<input checked="" type="checkbox"/> Risk eliminated <input type="checkbox"/> Risk reduced	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium	Delivery details of any technology will remain on the NRS	<input type="checkbox"/> Yes <input type="checkbox"/> No

<p>the providers system.</p> <p>Records relating to a person's care and support needs and other personal information will remain on the Authority's case management system only.</p> <p>Records will be aligned using the MOSAIC ID number as a consistent identifier.</p>		<input type="checkbox"/> Risk accepted	<input type="checkbox"/> High	<p>platform, however a persons care and support needs will remain aligned using the MOSAIC ID number accessible by KCC staff only</p>	
<p>People, or their identified representative, will have choice and control on the products used and the care and support received. They will be provided a privacy notice for the Technology Enabled Care service and it will be explained what data is captured to support the decision.</p>	8.2.4	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	<p>I new Privacy Notice has been produced that is specific to this project. This will be provided to users at the time of install in paper format, and access to an electronic version can be obtained at any time from the KNET page should an individual prefer this.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>The project team will test the compliance of the providers provision during the procurement process.</p> <p>The Authority and the provider will work together to put in place measures to ensure data is secure during mobilisation before introduced to the public.</p>	8.2.5	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	<p>All steps taken to ensure data is secure in accordance with our requirements. This Countywide storage will require the need to protect data being treated with the same high priority as was previously shown in the Test and Build project</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>DPIA will be reviewed quarterly to ensure processing remains complaint.</p>	8.3.1	<input type="checkbox"/> Risk eliminated <input checked="" type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	<p>Ongoing review of the DPIA will be carried out by the project team</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>Only Social Care professionals will be prescribing the equipment to people in line with legislation, including but not limited to, Care Act 2014, Mental Health Act 1983, Mental Capacity Act 2005</p>	8.3.2	<input checked="" type="checkbox"/> Risk eliminated <input type="checkbox"/> Risk reduced <input type="checkbox"/> Risk accepted	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	<p>Social Care professionals will be the only people prescribing the technology</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No

10. ICO consultation

a) Does this assessment indicate that the processing involved in the project would present a high risk in the absence of mitigation measures?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
b) If yes, can those risks be mitigated by reasonable means in terms of available technologies and costs of implementation?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – You MUST consult the ICO before the data processing starts
c) If it is necessary to consult with the ICO, has this been done?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Not Applicable

11. Sign off and record of outcomes.

Item	Name	Date
a) Measures to reduce risk approved by: ♦ ²⁹		
b) Residual risks approved by: ♦ ³⁰	Richard Smith	
c) DPO advice provided: ♦ ³¹		
d) Summary of DPO advice: ♦ ³²		
e) DPO advice accepted or overruled by: ♦ ³³		
f) Comments ♦ ³⁴ :		
g) Consultation responses reviewed by: ♦ ³⁵		
h) Comments: ♦ ³⁶		
i) This DPIA will kept under review by: ♦ ³⁷		

—	
Signature ♦ ³⁸	
Name(s)	
Job title(s)	
Date	

12. Implementation of privacy risk solutions & actions to be integrated into project plan

Action to be taken ♦ ³⁹	Date for completion or frequency ♦ ⁴⁰	Responsibility for action ♦ ⁴¹
a) Integrate the DPIA outcomes back into the project plan and update relevant project management paperwork/spreadsheets.		
b) Implement the approved privacy risk solutions:		
c) Review and update the DPIA and project plan at regular intervals.		

Appendix


Table 2a	DPA 2018 Schedule 1, Part 2 Appropriate Policy Document
<p>If relying on any of the conditions in sections 1, 6-28, the existence of an appropriate policy document is an additional mandatory safeguard. Unless an exception is detailed within the conditions in sections 6-28 you must confirm and attach your appropriate policy document.</p> <p>Click here to return to Section 7</p>	<p><input checked="" type="checkbox"/> (5) Requirement for an appropriate policy document when relying on conditions in this part – please tick to confirm you have a policy in place when relying on this condition which meets the following requirements: ⁴²</p> <p>(39) Requirement to have an appropriate policy document in place: the document must (a) explain how your procedures ensure compliance with data protection principles when processing special category data under this condition and (b) explains policies regarding the retention and erasure of that data ⁴³</p> <p>(40) Additional safeguard: retention of appropriate policy document: you have to keep the policy throughout the period you use the data and keep a copy for 6 months afterwards, you have to review it regularly and make it available on request to the Information Commissioner ⁴⁴</p> <p>Special Category Data and Criminal Records Data (Appropriate Policy Document):</p> <div style="text-align: center;">  <p>Special Category Data and Criminal R</p> </div> <p><input checked="" type="checkbox"/> Please tick to confirm your appropriate policy document is attached. If not attached please explain why not</p>

Table 2b	DPA 2018 Schedule 1, Part 2 Additional Conditions
<p>Additional conditions that must be met if using GDPR Article 9(2) Special Category exemption (g): processing is necessary for reasons of substantial public interest based on UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject, in accordance with Schedule 1, Part 2 of the DPA 2018.</p> <p>Please go to Table 2a to confirm your Appropriate Policy Document is attached, if you haven't already</p> <p>Click here to return to Section 7</p>	<p><input checked="" type="checkbox"/> (6) Statutory etc and government purposes ⁴⁵</p> <p><input type="checkbox"/> (7) Administration of justice and parliamentary purposes ⁴⁶</p> <p><input type="checkbox"/> (8) Equality of opportunity or treatment ⁴⁷</p> <p><input type="checkbox"/> (9) Racial and ethnic diversity at senior levels of organisations ⁴⁸</p> <p><input type="checkbox"/> (10) Preventing or detecting unlawful acts ⁴⁹</p> <p><input type="checkbox"/> (11) Protecting the public against dishonesty etc ⁵⁰</p> <p><input type="checkbox"/> (12) Regulatory requirements relating to unlawful acts and dishonesty etc ⁵¹</p> <p><input type="checkbox"/> (14) Preventing fraud ⁵²</p> <p><input type="checkbox"/> (15) Suspicion of terrorist financing or money laundering ⁵³</p> <p><input type="checkbox"/> (17) Counselling etc ⁵⁴</p> <p><input type="checkbox"/> (18) Safeguarding of children and individuals at risk ⁵⁵</p> <p><input type="checkbox"/> (19) Safeguarding of economic well-being of certain individuals ⁵⁶</p> <p><input type="checkbox"/> (20) Insurance ⁵⁷</p> <p><input type="checkbox"/> (21) Occupational pensions ⁵⁸</p> <p><input type="checkbox"/> (23) Elected representatives responding to requests ⁵⁹</p> <p><input type="checkbox"/> (24) Disclosure to elected representatives ⁶⁰</p> <p><input type="checkbox"/> (25) Informing elected representatives about prisoners ⁶¹</p>

Table 3	DPA 2018 Schedule 1, Part 3 Additional Conditions
<p>Additional conditions that must be met if processing data related to Criminal Convictions, as per Schedule 1, Part 3 of the DPA 2018</p> <p>Click here to return to Section 7</p>	<input type="checkbox"/> (29) Consent ⁶² <input type="checkbox"/> (30) Protecting individual's vital interests ⁶³ <input type="checkbox"/> (31) Processing by not-for-profit bodies ⁶⁴ <input type="checkbox"/> (32) Personal data in the public domain ⁶⁵ <input type="checkbox"/> (33) Legal claims ⁶⁶ <input type="checkbox"/> (34) Judicial acts ⁶⁷ <input type="checkbox"/> (35) Administration of accounts used in commission of indecency offences involving children ⁶⁸ <input type="checkbox"/> (36) Extension of conditions in Part 2 of Schedule 1 referring to substantial public interest ⁶⁹ (Please tick the relevant box from Table 2b above) <input type="checkbox"/> (37) Extension of insurance conditions ⁷⁰

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				

**Below is the guidance detailed in the guidance diamonds throughout the DPIA template.
Kindly do not edit this section of the document.
Thank you.**

¹ If yes, include details of who the data will be disclosed to (eg. partnerships or contractors), what data will be disclosed and why, whether there are any information sharing agreements in place, and who will be responsible for the monitoring arrangements or contract management, and whether there is a need or not for a separate DPIA.

² This relates to trade associations and representative bodies who draw up voluntary codes of conduct covering data processing topics that are important to their members. Since December 2019 the ICO can approve both codes of conduct and code monitoring bodies, although there are no ICO approved GDPR codes of conduct at present

³ Project management team; ICT Risk and Compliance; Procurement; Potential suppliers and data processors; Other experts, eg. IT, legal or other professionals; Anyone else with an interest in the project

⁴ State at what stage of the project you will consult

⁵ Summarise the response or advice, including the date given

⁶ It is useful to state the power or duty your activities fall within but this section MUST include your GDPR Article 6 legal basis and any exception relied on under Article 9 (where you are using special category data). This will be identified in the privacy notice given to data subjects.

Where required, depending on the Article 9 exception relied upon, ALSO ADD any condition relied on under Schedule 1 Data Protection Act 2018 PLUS any additional safeguards (eg appropriate policy document). Examples of commonly used conditions include: for employment, health or social care, safeguarding, equality of opportunity or treatment, public health.

If you are relying on the health or social care purposes or the management of health or social care purposes exception please note:

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.'

Please note these legal bases should be consistent with the relevant privacy notice you identify within the DPIA.

⁷ If you are relying on conditions (b), (h), (i), or (j) you also need to meet the additional condition in UK Law, set out in Part 1 of Schedule 1 of the DPA 2018

⁸ Condition is met if the processing is necessary for the purposes of performing or exercising obligations or rights, which are imposed or conferred on the controller or data subject with regards to employment, social security or social protection, and when processing is carried out, the controller has an appropriate policy document in place

⁹ This condition is met if the processing is necessary for health or social care purposes. In this paragraph "health or social care purposes" means the purposes of: preventive or occupational medicine; the assessment of the working capacity of an employee; medical diagnosis; the provision of health care or treatment; the provision of social care; or, the management of health care systems or services or social care systems or services. Subject to the conditions and safeguards in Article 9(3) GDPR and s11(1) DPA 18

¹⁰ This condition is met if the processing: is necessary for reasons of public interest in the area of public health, and is carried out by, or under, the responsibility of a health professional; or, by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

¹¹ This condition is met if the processing: is necessary for archiving purposes, scientific or historical research purposes or statistical purposes; is carried out in accordance with Article 89(1) of the GDPR (as supplemented by section 19); and, is in the public interest

¹² This includes criminal convictions and offences or related security measures including data relating to (a) the **alleged commission of offences** by the data subject, or (b) proceedings for an offence committed or **alleged** to have been committed by the data subject or the disposal of such proceedings, **including sentencing**.

¹³ Where you are processing for the law enforcement purposes as a competent authority (where KCC has a statutory function for any of the following purposes: prevention, investigation, detection or prosecution of criminal penalties, including the safeguarding against and the prevention of threats to public security)

¹⁴ This condition is met if the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and is necessary for reasons of substantial public interest.

¹⁵ This condition is met if the processing is necessary for the administration of justice.

¹⁶ This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

¹⁷ This condition is met if: the processing is necessary for the purposes of: protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual, (this includes protection relating to a particular individual, and protection relating to a type of individual); the individual is aged under 18, or aged 18 or over and at risk; the processing is necessary for reasons of substantial public interest; and, the processing is carried out without the consent of the data subject for one of the following reasons: in the circumstances, consent to the processing cannot be given by the data subject; in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the aforementioned provision of the protection.

For the purposes of this paragraph, an individual aged 18 or over is “at risk” if the controller has reasonable cause to suspect that the individual: has needs for care and support; is experiencing, or at risk of, neglect or physical, mental or emotional harm; and, as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

¹⁸ This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

¹⁹ This condition is met if the processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); is necessary for the purpose of obtaining legal advice; or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

²⁰ This condition is met if the processing is necessary when a court or other judicial authority is acting in its judicial capacity.

²¹ This condition is met if the processing: is necessary for the purposes of preventing fraud; and the processing consists of (i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation; (ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation; or, the processing of personal data disclosed as described in sub-paragraph (i) or (ii). Here, “anti-fraud organisation” has the same meaning as in section 68 of the Serious Crime Act 2007.

²² This condition is met if the processing is necessary for archiving purposes in the public interest; for scientific or historical research purposes; or, for statistical purposes.

²³ Identify considerations given to data minimisation (such as certain types of data subject not included in the scope, data collected being minimised, anonymisation being used, etc.) Data minimisation is a fundamental principle of the GDPR: ‘Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’). State how this is being addressed in the processing.

²⁴ What are the arrangements to ensure data subjects’ rights are protected (eg. Right to be informed, right of access, right to erasure, data accuracy, data portability, etc.). The degree to which all these rights may be relevant will depend very much on the nature of the processing. Also set out any particular special arrangements for vulnerable subjects or where there is an ‘imbalance of power’. Consider who the data subjects are, eg children, vulnerable adults, employees, general public, and how you will support the rights of those specific types of data subjects. For example, having easy read privacy notices for children/vulnerable adults, or, if your Article 6 legal basis is consent, will you regularly review that consent.

²⁵ You should as a minimum confirm that any data processing contract contains the Article 28 mandatory terms. These should be incorporated in Annex 1/a data protection clause, but if in doubt check with the lawyer who has drafted the service contract on KCC’s behalf.

Also consider how these requirements are to be managed (eg to only act on KCC’s instructions, to inform KCC if a sub processor is to be appointed etc

²⁶ i.e. Fair, lawful, transparent; 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.

²⁷ State which of your identified risk(s) will be addressed by this action.

²⁸ Is the final impact on individuals a justified, compliant and proportionate response to the aims of the project?

²⁹ This should be someone in the department who confirms that the Directorate will implement the DPO’s advice on risk **and** the measures in section 9. Remember to integrate actions back into project plan, with date and responsibility for completion.

³⁰ Any residual risks should be approved by the Information Asset Owner (as identified in the Information Governance Management Framework, this is usually the Corporate Director). If there are any residual **high** risks, you will also need to consult the ICO before going ahead. **DO NOT START YOUR DATA PROCESSING UNTIL THE ICO HAS MADE A DECISION.**

³¹ DPO should advise on compliance, measures to reduce risk in section 9, and whether processing can proceed. Add date of DPO Ben Watts' email confirming the processing is not high risk/ advice to reduce residual risks.

³² Add here the bullet points of advice provided within DPO Ben Watts' email.

³³ Insert date DPO Ben Watts' advice was accepted or overruled by the IAO. If the advice is accepted, please ensure any actions recommended by the DPO are added to the DPIA and implemented. If overruled, you must explain your reasons, in the comments below.

³⁴ If the DPO's advice is overruled, this section should explain on what basis and why, (this could be reviewed by an auditor or the ICO and so the reasons should be justified).

³⁵ Name and date of the person reviewing your consultation responses.

³⁶ If your decision departs from individuals' views, you must explain your reasons

³⁷ Insert the name of the Project Manager/ Person responsible for reviewing DPIAs. The DPO should also review ongoing compliance with DPIA

³⁸ Insert the signature, name and job title of the person or persons signing off and approving the DPIA, and the date of the sign off. This DPIA must be signed off by the Information Asset Owner as identified in the Information Governance Management Framework, (usually the Corporate Director)

³⁹ Each recommendation from the DPO's formal email of recommendations should be included in a separate row here with a named person responsible for implementation. That person must ensure that the actions are taken by the date stated.

⁴⁰ Insert the date at which each action is completed, or insert the frequency with which the DPIA will be reviewed and updated, eg monthly

⁴¹ Include the name and title of person

⁴² This condition is met when the controller has an appropriate policy document in place. Unless otherwise noted, a condition in Part 2, of Schedule 1 of the DPA Act 2018 is only met if when the processing is carried out, the controller has an appropriate policy document in place. See also the additional safeguards in Part 4, of Schedule 1

⁴³ If processing personal data in reliance on a condition in part 1, 2, or 3 which requires the controller to have an appropriate policy document in place when the processing is carried out, then the requirement to have an appropriate policy document in place; if the controller has produced a document which: (a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR, in connection with the processing of personal data in reliance on the condition in question; **and** (b) explains the controller's policies regarding the retention and erasure of personal data processed when relying on the aforementioned condition, and gives an indication of how long such personal data is likely to be retained.

⁴⁴ Where personal data is processed in reliance on a condition described in paragraph 38, the controller must during the relevant period: retain the appropriate policy document; review it and, (if appropriate) update it from time to time; and, make it available to the Commissioner, on request, without charge. Nb. 'Relevant period' in this context means a period which begins when the controller starts to carry out processing of personal data in reliance on the condition, and ends at the end of a 6 month period, which begins when the controller stops carrying out this processing.

⁴⁵ This condition is met if the processing is necessary for the reasons of substantial public interest, and is necessary for at least one of the following purposes: (a) the exercise of a function conferred on a person by an enactment or rule of law; or, (b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

⁴⁶ This condition is met if the processing is necessary for: (a) the administration of justice; or (b) the exercise of a function of wither House of Parliament

⁴⁷ This condition is met, (subject to exceptions listed below) if the processing is of a specified category of personal data, [personal data revealing racial or ethnic origin; religious or philosophical beliefs; data concerning health; or sexual orientation]; and is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to the category with a view to enabling such equality to be promoted or maintained. [EXCEPTIONS: Processing does not meet the condition if a data subject has given notice in writing to the controller requiring the controller not to process personal data in respect to which they are the data subject, that notice gave the controller a reasonable period in which to stop processing such data, and that period has ended.] Processing does not meet the condition if it is carried out for the purposes of measures or decisions with respect to a particular data subject, or if the processing is likely to cause substantial damage or substantial distress to an individual.

⁴⁸ This condition is met if the processing:
is of personal data revealing racial or ethnic origin;
is carried out as a part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally;
is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations; and,
can reasonably be carried out without the consent of the data subject.

[Processing can only reasonably be carried out without the data subject's consent where the controller cannot reasonably be expected to obtain their consent, and the controller is unaware of the data subject withholding consent- this does not include a data subject failing to respond to a request for consent].

These conditions are not met if it is likely to cause substantial damage or distress to an individual.

⁴⁹ This condition is met if the processing is necessary for the purposes of prevention or detection of an unlawful act. The processing must be carried out without the consent of the data subject so as not to prejudice those purposes, and is necessary for reasons of substantial public interest. This condition is met if the processing consists of the disclosure of personal data to a competent authority or is carried out in preparation for such disclosure; even if, when the processing is carried out, the controller does not have an appropriate policy document in place. Nb. 'Act' here includes a failure to act.

⁵⁰ This condition is met if the processing is necessary for the exercise of a protective function; must be carried out without the consent of the data subject so as not to prejudice the exercise of that function; and is necessary for reasons of substantial public interest. 'Protective function' in this context means a function which is intended to protect members of the public against dishonesty, malpractice, or other seriously improper conduct; unfitness or incompetence; mismanagement in the administration of a body or association; or failures in services provided by a body or association.

⁵¹ This condition is met if: the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has: committed an unlawful act, or has been involved in dishonesty, malpractice, or other seriously improper conduct; in the circumstances the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; and, the processing is necessary for reasons of substantial public interest. Nb. 'act' includes a failure to act; 'regulatory requirement' means a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or a requirement forming part of generally accepted principles of good practice relation to a type of body or an activity.

⁵² This condition is met if the processing is necessary for the purposes of preventing fraud or a particular kind of fraud, and consists of: the disclosure of personal data by a person as a member of an anti-fraud organisation; the disclosure of personal data in accordance with arrangements made by an anti-fraud organisation; the processing of personal data disclosed as described above.

⁵³ This condition is met if the processing is necessary for the purposes of making a disclosure in good faith under either of the following: section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property); or, section 339ZB of the Proceeds of Crime Act 2002 (disclosures within regulated sector in relation to suspicion of money laundering).

⁵⁴ This condition is met if the processing: is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially; is necessary for reasons of substantial public interest; and is carried out without the consent of the data subject for one of the reasons listed: in the circumstances, consent to the processing cannot be given by the data subject; in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the counselling, advice, or similar confidentially provided service.

⁵⁵ This condition is met if: the processing is necessary for the purposes of: protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual; the individual is aged under 18, or aged 18 or over and at risk; the processing is necessary for reasons of substantial public interest; the processing is carried out without the consent of the data subject for one of the reasons listed: in the circumstances, consent to the processing cannot be given by the data subject; in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned. Nb. An individual aged 18 or over is at risk if the controller has reasonable cause to suspect that the individual: has needs for care and support; is experiencing, or at risk of, neglect or physical, mental or emotional harm; and as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

⁵⁶ This condition is met if the processing: is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over; is of data concerning health; is necessary for reasons of substantial public interest; and is carried out without the consent of the data subject for one of the reasons listed: in the circumstances, consent to the processing cannot be given by the data subject; in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned. Nb. 'individual at economic risk' here means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness, or disability.

⁵⁷ This condition is met if the processing: is (a) necessary for an insurance purpose; (b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health; and (c) is necessary for reasons of substantial public interest,

If the processing is not carried out for the purposes of measures or decisions with respect to the data subject and the data subject does not have and is not expected to acquire rights against or obligations in relation to a person who is an insured person under an insurance contract to which the insurance purpose in (a) relates; or other rights or obligations with such a contract, then the processing does not meet the conditions in (a)-(c) unless it can reasonably be carried out without the consent of the data subject.

Processing can reasonably be carried out without the consent of the data subject only where: the controller cannot reasonably be expected to obtain the consent of the data subject; and the controller is not aware of the data subject withholding consent. This does not include a data subject failing to respond to a request for consent.

Nb. Here, “insurance contract” means a contract of general insurance or long-term insurance; “insurance purpose” means: advising on, arranging, underwriting or administering an insurance contract; administering a claim under an insurance contract; or exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

⁵⁸ This condition is met if the processing: is necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme; is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme; is not carried out for the purposes of measures or decisions with respect to the data subject; and can reasonably be carried out without the consent of the data subject.

Processing can reasonably be carried out without the consent of the data subject only where: the controller cannot reasonably be expected to obtain the consent of the data subject, and the controller is not aware of the data subject withholding consent. This does not include a data subject failing to respond to a request for consent. Nb. Here, “member”, in relation to a scheme, includes an individual who is seeking to become a member of the scheme.

⁵⁹ This condition is met if the processing is carried out: by an elected representative or a person acting with the authority of such a representative; in connection with the discharge of the elected representative’s functions; and in response to a request by an individual that the elected representative take action on behalf of the individual; and the processing is necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative in response to that request,

Where the request is made by an individual other than the data subject, this condition is only met if the processing must be carried out without the consent of the data subject for one of the following reasons: in the circumstances, consent to the processing cannot be given by the data subject; in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing; obtaining the consent of the data subject would prejudice the action taken by the elected representative; the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

⁶⁰ This condition is met if the processing consists of the disclosure of personal data: to an elected representative or a person acting with the authority of such a representative, and in response to a communication to the controller from that representative or person which was made in response to a request from an individual; the personal data is relevant to the subject matter of that communication, and the disclosure is necessary for the purpose of responding to that communication.

Where the request to the elected representative came from an individual other than the data subject, the condition is only met if the disclosure must be made without the consent of the data subject for one of the following reasons: in the circumstances, consent to the processing cannot be given by the data subject; in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing; obtaining the consent of the data subject would prejudice the action taken by the elected representative; the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

⁶¹ This condition is met if: the processing consists of the processing of personal data about a prisoner for the purpose of informing a member of the House of Commons, a member of the National Assembly for Wales or a member of the Scottish Parliament about the prisoner; and the member is under an obligation not to further disclose the personal data. The references to personal data about, and to informing someone about, a prisoner include personal data about, and informing someone about, arrangements for the prisoner’s release.

Nb. here “prison” includes a young offender institution, a remand centre, a secure training centre or a secure college; “prisoner” means a person detained in a prison.

⁶² This condition is met if the data subject has given consent to the processing

⁶³ This condition is met if: the processing is necessary to protect the vital interests of an individual, and the data subject is physically or legally incapable of giving consent

⁶⁴ This condition is met if the processing is carried out: in the course of its legitimate activities with appropriate safeguards by a foundation, association, or other not-for-profit body with a political, philosophical, religious, or trade union aim; and, on the condition that: the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes, and the personal data is not disclosed outside that body, without the consent of the data subjects.

⁶⁵ This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

⁶⁶ This condition is met, if the processing: is necessary for the purpose of, or in connection with, any legal proceedings, (including prospective legal proceedings), is necessary for the purpose of obtaining legal advice; or is otherwise necessary for the purposes of establishing, exercising, or defending legal rights.

⁶⁷ This condition is met if the processing is necessary when a court or tribunal is acting in its judicial capacity.

⁶⁸ This condition is met if: the processing is of personal data about a conviction or caution for an offence under: section 1 of the Protection of Children Act 1978 (indecent photographs of children); Article 3 of the Protection of Children (Northern Ireland) Order 1978 (indecent photographs of children); section 52 of the Civic Government (Scotland) Act 1982 (indecent photographs etc of children); section 160 of the Criminal Justice Act 1988 (possession of indecent photograph of child); Article 15 of the Criminal Justice (Evidence etc) (Northern Ireland) Order 1988 (possession of indecent photograph of child); or, section 62 of the Coroners and Justice Act 2009 (possession of prohibited images of children); or, incitement to commit an offence under any of these provisions.

The condition is met also if the processing is necessary for the purpose of administering an account relating to the payment card used in the commission of the offence or cancelling that payment card; and, when the processing is carried out, the controller has an appropriate policy document in place.

[See also the additional safeguards in Part 4 of Schedule 1 of the DPA 2018] Nb. 'Caution' means a caution given to a person in England, Wales, or Northern Ireland in respect of an offence which, at the time when the caution is given, is admitted.

'Conviction' has the same meaning as in the Rehabilitation of Offenders Act 1974 or the Rehabilitation of Offenders (Northern Ireland) Order 1978. 'Payment card' includes a credit card, a charge card, and a debit card'

⁶⁹ This condition is met if the processing would meet a condition Part 2 of Schedule 1, but for an express requirement for the processing to be necessary for reasons of substantial public interest.

⁷⁰ This condition is met if the processing: would meet the (20) 'insurance condition' in Part 2 of Schule 1, or would meet the (36) condition by virtue if the insurance condition, but for the requirement for the processing to be processing a category of personal data specified