DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The General Data Protection Regulation (GDPR) introduced a new mandatory requirement for organisations to identify and then assess high risks to the rights and freedoms of individuals associated with any proposals to process personal data, particularly special category personal data. Please refer to the Council's Privacy by Design Policy.

Below is set out a template DPIA form which users are expected to save a copy and complete. The form is divided into 3 parts. Part One should be completed first. If necessary Parts Two and Three should then be completed. Each Part contains further guidance and instructions. Part Three is divided into 3 sections

Instructions on how to complete DPIA

NB: For any DPIA's relating to Adult Social Care/Children's Services and Public Health (ASC/ChS/PH) please contact Jan Boucher, Information Governance/Caldicott Support Manager, at Janice.boucher@rbkc.gov.uk who can support you in this process.

1. Seek advice from the statutory Data Protection Officer [DPO] on whether you need to complete a DPIA.
2. Obtain a copy of the DPIA Form from the DPO website
3. Contact the Information Management Team [IM Team] or DPO to obtain a unique reference number
4. Complete the DPIA Screening Section – Part One
5. If you answer **No** to any of the screening questions, liaise with the IM Team or for ASC/ChS/PH the IG/Caldicott Support Manager to confirm and then arrange for your head of service or project sponsor (whichever is appropriate) to sign this off.
6. Maintain a copy of Part One in your project folder and send a copy to the IM Team for entry onto the DPIA Register so that this can be recorded against your project
7. If you answer **Yes** to any of the screening questions go on to complete Part Two, and then the risk assessment in Part Three.
8. Complete the DPIA form and liaise with the IM Team to agree mitigations and record actions to be taken to reduce any identified risks. This also includes agreeing timescales for either completing mitigation actions and/or keeping the risks under review.
9. Obtain recommendations from the IM Team or the DPO (whichever is appropriate), add these to your form and send to your Head of Service or project sponsor for final sign off as Information Asset Owner (IAO).
10. Attach a copy of your completed Parts 1-3 of the DPIA to your project folder.

11. Send a final copy of your completed DPIA to the IM Team who will maintain a record of it in the council's DPIA Register
12. If you are required to implement or review your mitigations against an agreed timetable, please include these in your DPIA action plan and complete the online Review Actions columns against your registered DPIA
13. All queries about the DPIA should quote the DPIA Unique Reference Number.
14. Details of all relevant council policies and guidance can be found on the DPO and IM Intranet Pages

PART ONE

DATA PROTECTION IMPACT ASSESSMENT [DPIA] - SCREENING QUESTIONS

DPIA Screening Questions to determine if a DPIA is needed. If the answer to any of these questions is yes, users **must** complete Part Two Data Protection Checklist and Part Three Data Protection Risk Assessment. If the answer is No to **all** the questions in this Part, you do not need to undertake the rest of the DPIA. In Part One Use the end column (Description) to provide additional information

DPIA Reference Number:	
Project Title	Insurance Tender 2024-2029
Process Owner	Ray Chitty , Head of Insurance Service
Author (i.e. person completing this DPIA)	Beverly Mills , Assistant Head of Insurance
Date Completed	07/12/2023

	PART ONE: SCREENING				
	Question	Examples	Yes	No	Description (Optional)
1.	Information about individuals will be collected.	Names, addresses, DOB, ethnicity	☒	☐	Remember to consider the rights and freedoms of individuals over how their data is being used. The DPIA questions are aligned to the UK GDPR and challenge you to make sure that your project or processing meets its requirements.

					Claimants where required making a claim against the Council will be asked to provide names, addresses, date of birth. For claims received a data protection notice is provided. If the claim is sent directly to the Council from the Claimant/ Claimant's solicitor, we provide a fair obtaining notice which confirms that we will use data as follows: '*We are required to send you this information to comply with Data Protection Act 1998. It explains how we may use your details and tells you about the systems we have in place that allow us to detect and prevent fraudulent claims.* *The Council is a subscriber to the Claims & Underwriting Exchange (CUE). The CUE system is an insurance industry shared database of insurance claims that helps compensators and insurers identify non-disclosure, concurrent claims activity and prevent fraud'.* *A notice explaining how the Council will use the data is also issued, which includes Ant-Fraud purposes,*

					management information, compliance with legal obligations and responsibilities. Additionally, we explain how the data will be processed. Claims submitted via the online portal system are covered by the claims portal privacy notice, which allows the Council to share information with our insurers Data is also processed in accordance with the general Council data policy requirements.
2.	Individuals will be required to provide information about themselves.	Names, addresses, DOB, ethnicity	☒	☐	Claimants where required making a claim against the Council will be asked to provide names, addresses, date of birth
3.	Information about individuals will be disclosed to other organisations or people or transferred outside of the UK. This includes HR and OH data about Council staff.	Social services, debt advice, police, fraud prevention	☒	☐	Is the information you plan to collect likely to be shared? The information may be shared with the insurance company who will be considering the claim or making a claim payment. Additionally, data shared with solicitors acting on behalf of the Council in defence of a claim

4.	Information about individuals will be used for a different purpose than that for which it was originally provided.	Utilising names & addresses for unrelated marketing campaigns		☒	
5.	New technologies, or a new application of existing technologies, will be used.	New technologies might include fingerprint recognition, facial recognition, biometrics etc. New self-service solutions for residents, or development of new database applications using existing customer data	☐	☒	Are you planning to use new technologies like facial recognition, fingerprinting or other forms of biometric methods to identify and/or verify users.
6.	Automated decisions or actions against individuals with no human intervention will be taken that can have a significant impact on them.	Automatically sending out arrear's letters to tenants in arrears without a manual check.	☐	☒	
7.	Profiling information about individuals will be carried out and used to make decisions on someone's access to a service, opportunity or benefit.	Targeting people based on profiling data such as age, ethnicity or religion for services and goods	☐	☒	All claims are assessed on the merit of the claim and based on the insurance policy cover and UK law.
8.	Personal data from multiple sources is combined, compared or matched.	Use of data warehouse for determining fraudulent housing benefit claims	☐	☒	Are you planning to do any data matching for individuals or groups?
9.	Personal data is processed without providing a privacy notice directly to the individual.	New data collection form is introduced with no privacy notice or declaration	☐	☒	
10.	Personal data will be processed in a way which involves tracking individuals' online or offline location or behaviour.	Lone worker devices, cookies, google analytics	☐	☒	

11.	Children's personal data will be processed.	Tenancy household composition	☒	☐	Where the claimant is a child
12.	CCTV will be used.	Recorded image or video will be captured, which may include identifiable images of people.	☐	☒	
13.	Personal data will be processed which could result in a risk of physical harm in the event of a security breach.	Domestic violence, people flagged as a high risk to staff or other customers.	☐	☒	

Recommendation	
Is a DPIA required?	Yes ☒ No ☐
If No, obtain sign off from the IM Team and place a copy on the project file	
Author (i.e. person completing this DPIA)	Beverly Mills
Date Completed	28/12/2023
IMT Sign Off	

PART TWO

PART TWO: **DATA PROTECTION IMPACT CHECKLIST**
Part Two is to be completed if you answered **Yes** to any section of Part One: DPIA Screening. Part Two is intended as a guide to help you identify how your project or initiative will engage the GDPR and Data Protection Act 2018. This will then enable you to complete Part Three (sections 1, 2 and 3) which focus on the risks and issues associated with your proposed processing of personal data. P**lease** complete the Part Two Checklist.

DPIA Reference Number:	
Project Title:	Insurance Tender 2024-2029
DPIA Completed By:	Beverly Mills
Project Sponsor:	Ray Chitty
Date DPIA Completed:	07/12/2023

	Question	Guidance	Response
1.	Explain broadly what the project aims to achieve and what type of processing it involves.	*You may find it helpful to refer or link to other documents, such as a project proposal brief or PID.*	The award of insurance contracts to meet statutory requirements and provide financial protection for the Councils assets and liabilities. Data is only collected where required to support a claim made against the Council.

	Question	Guidance	Response
2.	Please describe the data that you will be processing. Including whether the data subjects are tenants, service users, Council employees etc.	*List sets of data rather than individual fields, such as customer names, contact information, customer representatives, household members, addresses, profiling data, arrears data, and repairs history.*	Data will include name, address, date of birth, which are required to proceed with the claim they individual is making against the Council.
3.	Is the Council the Data Controller, the Data Processor or a Joint-Controller?		Data Controller
4.	What volume of personal data is being processed?	*How many data subjects (approximately) will be in the dataset being processed?*	It is difficult to provide an exact figure as the data collected relates to claims to be made against the Council in future years., approximately in the region of 600 claimants per year based on past claim data numbers.
5.	What is the lawful basis for processing the data? For example, tenancy agreement, lease, contract, specific consent.	*If you do not have a lawful basis then you cannot process the data. You need to seek advice from the IM Team on the lawful basis before proceeding with this project.*	To process, investigate and settle a claim made against the Council. An insurance claim cannot be pursued without this information.
6.	Are you using the data in a way that differs from the reason it was originally collected?	*You cannot use the data for a different purpose etc. without reviewing your lawful basis, and steps taken to notify the service users whose data you intend to process.* *If the answer is yes, i.e. you intend to use for a different purpose seek advice from the Council's IM team before proceeding.*	No , only for the purposes of handling the insurance claim.

	Question	Guidance	Response
7.	Is there another way of achieving the same project outcomes that does not involve processing individuals' data? What other options have you considered?	*This is to ensure that the scope of the project and data processing is in proportion with the expected outcomes.* *Consider whether any data items can be removed, but still achieve the same ends.*	No, it would not be possible to handle a claim without the claimant providing their name, address and where relevant DOB.
8.	Does the data / processing include any of the following categories of data? If yes, please indicate which ones and provide a justification for processing the data: • Other household members or named individuals • Named children • Health & medical information including vulnerability • Race and ethnic origin; • Politics and trade union membership • religion; • genetics & biometrics (where used for ID purposes); • health; • sex life or sexual orientation.	*If you collect any of these categories, you must take extra care when processing this data.* *You cannot request data because they may be useful in the future.* *If any apply (you will be processing special category/sensitive personal data) consider adding this as part of your risk assessment.* *Consider whether all the data items specified are required for the processing? Can any be removed, but still achieve the same ends?*	Children details may be provided if the claim is being made on behalf of a person under 18 years of age. Health and medical information may be sought if the claimant is making a personal injury claim against the Council and details of the injury or illness and prognosis etc would need to be provided to evidence their claim is valid.

	Question	Guidance	Response
9.	What is the source of the data?	*Examples include the customer themselves, a representative of the customer, another organisation e.g. NHS partners, voluntary sector etc. Or another WCC/RBKC department.* ***List all that apply.*** *If you are receiving data from a third-party organisation (excluding WCC/RBKC departments) you must be able to explain how you obtained the data and provide copies of any data sharing agreements, contracts or both.*	Information will be provided by the claimant themselves or their solicitor they have appointed to act on their behalf.
10.	Has a privacy notice been made available to all the data subjects?	*Have data subjects been informed about this new processing, and any third-parties that will have access to their personal data?*	Yes issued to claimants when claim received.
11.	What checks do you have in place to ensure the data will be accurate and kept up to date?	*Reasonable steps must be in place to ensure that data is accurate and kept up to date. Explain how your proposal will maintain accuracy*	General Council guidelines are followed.
12.	How will you ensure that the data collection process is secure, has an Information Security Questionnaire been completed and reviewed by the Information Security Team?	*Examples of potentially non-secure data collection include, paper forms, unencrypted devices, non-secure email, use of fax machines.*	The information is retained on a secure system with password access limited to the relevant users/claim handlers.
13.	Who will you be sharing data with, and how will you be sharing the data? Will the data ever be moved outside of the UK?	*List all third-party organisations and WCC/RBKC departments.* *You must have data sharing agreements in place, if you are sharing with third party organisations (excluding WCC/RBKC departments).*	Remember to consider the rights and freedoms of individuals over how their data is being used. The DPIA questions are aligned to the UK GDPR and challenge you to make sure that your project or processing meets its requirements. Claimants where required making a claim against the Council will be asked to provide names, addresses, date of birth. . For claims received a data protection notice is provided. If the claim is sent directly to the Council from the Claimant/ Claimant's solicitor,

	Question	Guidance	Response
		Examples of data sharing mechanisms include, automated data extracts, data manually uploaded onto an external website, emails to the organisation, posted forms or other documents. *Consider whether data sharing is compliant and secure as part of your risk assessment.*	we provide a fair obtaining notice which confirms that we will use data as follows: 'We are required to send you this information to comply with Data Protection Act 1998. It explains how we may use your details and tells you about the systems we have in place that allow us to detect and prevent fraudulent claims. The Council is a subscriber to the Claims & Underwriting Exchange (CUE). The CUE system is an insurance industry shared database of insurance claims that helps compensators and insurers identify non-disclosure, concurrent claims activity and prevent fraud'. A notice explaining how the Council will use the data is also issued, which includes Ant-Fraud purposes, management information, compliance with legal obligations and responsibilities. Additionally, we explain how the data will be processed. Claims submitted via the online portal system are covered by the claims portal privacy notice, which allows the Council to share information with our insurers Data is also processed in accordance with the general Council data policy requirements.
14.	Where will the data be stored and/or processed?	*Please list all relevant systems, business applications, network drives, hosted storage; lockable filing cabinets.* *Please identify exactly where the information will be held on the world wide web. Distinguish between 1) servers and databases hosted entirely on council premises, 2) servers and databases in external or third-party data centres, and 3) cloud-hosted services, servers and databases. If you are not sure, mark this as a risk,*	Data is attached to the relevant claim record on the bespoke insurance system. Only the insurance team have access to the system, accessed by password.

	Question	Guidance	Response
		and ensure that you find out as part of the procurement process.	
15.	Who will have access to the data, and how will you ensure that access is restricted to essential users?	*Please specify teams, roles and include external organisations. In some cases, this may be named officers.* *Data must be protected to prevent unauthorised or unlawful processing.* *Please identify exactly where the information will be held on the world wide web. Distinguish between 1) servers and databases hosted entirely on council premises, 2) servers and databases in external or third-party data centres, and 3) cloud-hosted services, servers and databases. Please make sure you understand and document who will have access to the council's data. If you are not sure at this stage, mark this as a risk and be sure you find out as part of the procurement or sharing process.*	Essential users only i.e. the claim handlers.
16.	How will you ensure that the data will be retained as per the Data / Document Retention Policy and Schedule?	*Explain how will data be retained and then deleted. Who will be responsible for deleting material – the council? Your contractor?* *Contractors and Partners:* *Ensure you have an exit strategy built it to any contractual or information sharing agreements so that you know exactly what will happen to the council's data at the end of the*	Data is retained in line with the Council guidance. It is retained on file as required to deal with the claim.

	Question	Guidance	Response
		project/contract or information sharing arrangement	

DPIA Change Control				
Version	Date	Nature of change	Person responsible	Role

PART THREE

Section 1. Guidance on how to complete section 2:

1. Use your knowledge of the project/procurement/ initiative, the controls that already exist, and any other contributory factors, to identify all known information (data privacy) risks.

- consider the impact of the risk on the individual whose data is processed (data subject)
- consider the risk to the council should there be an issue of non-compliance
- We have provided pre-populated guidance in the 'Privacy Risk' column as a starting point to help you identify the risks. These are based on the data protection principles under GDPR and DPA 2018 but you're not limited to the pre-populated details – you should tailor these to the risks specific to your project/procurement/initiative and you can add more than one risk under each principle
- It is important you capture what actions you will take to reduce any identified risks to the processing of personal data. Always think of the worst case scenario and then work back on what measures could be put in place at any point in the processing (start, middle or on-going) to either prevent or reduce high risk.
- If there is nothing that can be done to mitigate high risk the council is obliged to consider consulting the Information Commissioner's Office [ICO] **before** proceeding with implementing the project. Please consult the council's DPO if this is the case.

2. Use the tables for 'Description of likelihood ratings' and 'Description of impact ratings' to objectively score the respective impact and likelihood ratings of each identified risk
3. Record your scores in the relevant column
4. Multiply the respective scores for impact and likelihood to arrive at a risk rating score for each identified risk.
5. Document the risk rating score in the appropriate column
6. Identify the controls/measures/actions you need to put in place for each risk and document them in the Mitigations column to correspond to the risk they are designed to address
7. At the end, sum up the total scores in each column and find the average of the scores for each i.e. add up all scores and divide by the number of entries for each column.
8. Once your DPIA is complete please send to the IM team or if you work in ASC/ChS/PH ensure you also send a copy to with the IG/Caldicott Support Manager to discuss. Where you have answered "no" to all the screening questions, we still advise you contact the IM team to confirm your score.
9. A record of your DPIA and score will be registered on the council's DPIA register managed by the council's Data Protection Officer [DPO] and IM Team

Understanding Risk

This section follows up on the answers you've provided in sections 1 and 2 of the DPIA.

In this section you need to assess the information (data privacy) risks that relate to the intended processing of personal data. In doing so you need to identify and assess how the possible misuse of personal data could lead to significant impacts on:

- Individuals (data subjects such as our service users, residents, staff etc.) - because their rights under data protection law are breached e.g. someone accesses their data who shouldn't. Or our poor record keeping means we are unable to find their information when they ask for it.
- The service/the council - because our processing doesn't comply with the law – e.g. we sent out a spreadsheet containing a 150 names and other information about clients to the wrong email address. This is a data breach which is potentially reportable to the ICO and could result in a fine.
-

So, we must identify the risks and what we can do to mitigate them ***before*** any personal data is used. To assist, set out below are some key risk management definitions

- A **risk** is something that may occur
- An **issue** is something that has occurred
- In calculating risk, there are two components you need to consider: *Risk = Likelihood * Impact*:
  - the **likelihood** of a risk materialising to become an issue (something that has happened = probability)
  - the **impact** that will be felt if the risk were to occur

Finally, to avoid or limit the impact, we need to think about what actions (**mitigations**) we can take to manage or plan for the future.

- A **mitigation** is a control, measure, action we can take to either stop/reduce the likelihood of the risk occurring or reduce the impact if the risk does occur (i.e. if the risk becomes an issue).

Below, there are descriptions (and their meanings) for scoring the respective Likelihood (probability) and Impact ratings – these are based on the council's Likelihood and Impact tables. Use these tables to give a rating to the likelihood and impact elements of each risk you identify

Using Likelihood and Impact Rating to Assess Data Privacy Risk

RISK FORMULA: RISK = LIKELIHOOD * IMPACT (please see section 1 Guidance on How to Complete this section)

DESCRIPTION OF IMPACT RATINGS

Impact	Descriptions
1. Very Low	•Insignificant impact to the individual or the Council •Unauthorised access to, loss or damage to ordinary personal data of up to 10 living individuals, cost impact £0 to £25,000
2. Low	•Minor impact to the individual, service or the Council •Localised decrease in perception within service area – limited local media attention, short term recovery •Unauthorised access to, loss or damage to ordinary personal data of 11-999 individuals, cost impact £25,001 to £100,000
3. Medium	•Moderate impact to the individual, service or the Council •Decrease in perception of public standing at local level – media attention highlights failure and is front page news, short to medium term recovery •Unauthorised access to, loss or damage to sensitive data of 11-999 individuals, cost impact £100,001 to £400,000
4. High	•Major impact to the individual, service or the Council, •Decrease in perception of public standing at regional level – regional media coverage, medium term recovery from incident •Unauthorised access to, loss or damage of sensitive data to over 1000 individuals, cost £400,001 to £800,000
5. Very High	•Catastrophic impact to the individual or service or the Council. For instance, Life or Death situation, shut down in service for more than 3 days – for example inability to access social care systems

DESCRIPTION OF LIKELIHOOD RATINGS

Descriptor	Likelihood Guide	Mitigations
1. **Improbable, extremely unlikely**	Virtually impossible to occur 0 to 5% chance of occurrence.	You will be required in section 4 to outline any mitigating measures that can been taken as part of the project to help justify the score given. Note: This risk may be subject to moderation following the review by the Information Management Team
2. **Remote possibility**	Very unlikely to occur 6 to 20% chance of occurrence	
3. **Occasional**	Likely to occur 21 to 50% chance of occurrence	
4. **Probable**	More likely to occur than not 51% to 80% chance of occurrence	
5. **Likely**	Almost certain to occur 81% to 100% chance of occurrence	

Section 2: Undertaking Privacy Risk Assessment: Identify all Possible Risks (Likelihood and Impact) Arising from your proposed use of the Data				
Privacy Risks	**Like-li-hood (l)**	**Impact (i)**	**Risk rating (i x l)**	**Mitigation action and other things you need to consider**
Lawfulness, Fairness, And Transparency • The data subjects (service users, customers, employees) **have not been notified (agreed/aware) to** their personal and special categories/criminal offence data being processed for the purposes of this project/procurement/initiative. If notification rather than consent, the legal basis for processing must be stated. • **We don't have a legal basis** (lawful basis for processing personal data and additional conditions for processing special categories and criminal offences data) for our proposed processing. Our proposals are not driven by statute or official requirements. It is something we would like to do, but are not obligated to undertake by law or official duty – if we are, the Public Task/Public Interest Lawful Basis should suffice ***Please note:*** *Under the GDPR* ***Consent*** *is a Lawful Basis for processing personal data in its own right. However local authorities are encouraged not to rely on it as their primary lawful basis. This is because the powers invested in local authorities are driven by statute and regulation. This means we can nearly always rely on these to justify why we undertake the processing of personal data. For example, the council cannot rely on Consent to process Council Tax Data.* *The interpretation of* ***Consent*** *within the context of performing our Public Task/Public Interest duties means that we should always endeavour to directly inform service users about how their data will be processed, what guarantees they can expect, and their rights under the GDPR - including the right to withdraw consent where there are no statutory impediments to do so*	**1** **N/a**	**1** **N/a**	**1** **N/a**	*Action* *[Insert established or planned activities, controls or measures – ask yourself these questions:* **Data is provided by claimant/their solicitor to make a claim against the Council** **Privacy notice issues** **Password access Controlled system to record claim data** ***Tell/ Notify*** *How will individuals be told about the use of their personal data*? **Privacy notice issued** *Do you need to create or amend your privacy/fair processing notices?* **No** ***Purpose/Reasons why you need personal data*** *Does your project clearly state its purpose for using this information?* **To deal with a claim received from a claimant** ***Lawful Basis*** *Have you identified your legal basis for the processing of personal data?* **Yes** ***Please note****:* *Will your intended processing fall outside of a statutory or official duty i.e. the Public Task/Public Interest? If yes, consider the Legitimate Interests Lawful Basis. Please refer to the council's Legitimate Interest Policy and Assessment Tool when using this as your reason for the lawful processing of personal data. For example, the collection of email addresses for the purpose of undertaking some surveys or informing recipients about council events and services.* ***In general, individuals*** *who provide their contact details for informational purposes only can exercise their right to withdraw*

				their consent to participate. How will you manage this right to withdraw personal details from your contacts database? There are up to 6 Lawful Basis Categories within the GDPR. ***Please consult the IM Team or DPO if you are not sure which to apply to your project***
Purpose Limitation • The personal and special categories/criminal offence data sets to be handled **aren't collected for specified**, **explicit**, and **legitimate purposes**. • The personal and special categories/criminal offence data sets to be handled will **be processed in a manner that is incompatible with those purposes**. • Any future uses of the data will not be in line with the original specified purposes, and/or data subjects will not be informed of the new purposes.	**1**	**2**	**2**	***Action*** *[Insert established or planned activities, controls or measures – ask yourself these questions:* **Personal data collected – name. address , DOB.** **special categories/criminal data is not collected** **Only data needed for the claimant to pursue their claim is collected** *Is there any information you do not need access to? Are you collecting only the information you need? Are you collecting information for one purpose but then using it for another? What arrangements are being made to ensure that new suppliers are only provided with/collect sufficient and relevant data to provide the service? E.g. will the process and template be specified so that the suppliers know what information to collect and make sure that they only collect the same, necessary information each time?]*
Data Minimisation • The personal and special categories/criminal offence data to be handled are **not adequate, relevant and limited** for the purposes of task in hand.	**1**	**1**	**1**	***Action*** *[Insert established or planned activities, controls or measures – ask yourself these questions:* **Adequate system in place, minimal data collected to support the claim** *Is there any information you do not need access to? Are you collecting only the information you need? Could you anonymise or psuedonymise the data for parts or all parts of the processing?]* **Only data required for the claimant to pursue their claim is collected**
Accuracy • The personal and special categories/criminal offence data to be handled contains **inaccuracies** that will skew the accuracy of decisions taken.	**1**	**1**	**1**	*Action* *[Insert established or planned activities, controls or measures – ask yourself these questions:*

				The claimant or their solicitor provide the data to the Council. The Council does not gather this from other sources *How do you know the information you plan to use is accurate? How do you plan to maintain its accuracy? If the suppliers will have access to information that is already held, what arrangements are being made to ensure that the data passed to new or existing suppliers is accurate and up-to-date?* *What ongoing data quality measures are planned (for both data provided to the suppliers by the council and for data collected by the suppliers on the council's behalf)?* *What processes will be put in place to flag and correct inaccuracies that are identified/reported?* *Will testing be carried out to check the systems/processes work as expected?]*
Storage Limitation • The personal and special categories/criminal offence data handled is **retained** for longer than is necessary for the purposes for which it is processed.	**1**	**2**	**2**	***Action*** *[Insert established or planned activities, controls or measures – ask yourself these questions:* **Secure password system bespoke for insurance data.** **Only insurance team have access.** **No special /criminal data held.** *What retention periods will be applied to the information before destruction? How will the information be destroyed at the end of the retention period? Do you have robust exit strategies captured in your contracts or information sharing agreements to cover what must happen if the contract or your agreement runs to the end of the contract date or if it needs to be terminated early?*
Integrity and Confidentiality (Security) • Personal and special categories/criminal offence data is processed in a manner that is not secure - there is not an appropriate level of technical and organisation measures taken to protect the data against **unauthorised** or **unlawful**	**1**	**2**	**2**	***Action*** *[Insert established or planned activities, controls or measures – ask yourself these questions:* **See above, system is secure claims are self handled in-house by the Council. Rolling programmed to be in place to destroy data after 10 years where applicable.**

processing and against **accidental loss**, **destruction** or **damage**. • Assessments of suppliers and/or partners' security arrangements have not been undertaken. • Appropriate Information Sharing Agreements or compliance monitoring checklists have not been put in place or agreed to enable continuous monitoring of compliance controls				*In all activities relating to the project or initiative, have you employed necessary measures - both technical and organisational – in the personal data you will be processing? Have you identified how you will protect information (soft and hard copy) when being moved/transferred/migrated? Have you considered what controls you will put in place to prevent unauthorised access/modification/disclosure? e.g. organisational measures such as training of staff, Disclosure Barring Service (or other) checks of staff, processes and policies; technical measures such as encryption; user-based access controls? Has the supplier completed the Information Security Questionnaire ISQ) and has been reviewed by the Information Security Team – what level of assurance do they provide?]* The bidders are global insurance companies subject to strict DP rules, procedures, governance and legislation requirements. *The bidders confirm their data processing process within their tender response. Completion of the ISQ can be arranged if required.*
Accountability • We are unable to demonstrate compliance with the data protection principles for the processing of the Personal and special categories/criminal offence data: a. Lawful, fair and transparent b. Purpose limitation c. Data minimisation d. Accuracy e. Storage limitation f. Security	1	1	1	***Action*** *[Insert established or planned activities, controls or measures – ask yourself these questions:* **Data collected direct from the individual or provided by their solicitor. Only data required is collected to allow their claim to be progressed.** **The data is as required by insurance law needed to make an insurance claim.** **System password secure, access limited to insurance team only** *Can you demonstrate how the processing will comply with the data protection principles – things that help us to demonstrate compliance include: contracts with appropriate data protection and processing clauses in them, information sharing agreements, fair processing notices, completing a DPIA,*

				capturing processing details in the council's information asset register, having documented processes/ templates which set-out how the information will be handled]
International Transfers • Personal and special categories/criminal offence data is processed outside of the UK without appropriate safeguards in place.	**N/a**	**n/a**	**n/a**	*Action* *[Insert established or planned activities, controls or measures – ask yourself these questions:* *Where will the data be processed? Does the contract cover acceptable data processing locations and potential changes to processing location if locations change to outside of the EEA?]* *Do you know every location where the council's data will be held, accessed and maintained? This include hosted solutions. Is this covered off in your contract?* *Are you able to exercise direct control over the data, or are you going to rely on a supplier? What assurances have you got from them? Are these adequate – did you do a test run for a data breach, data complaint or data subject asking for a copy of their data and an explanation about where their data is held?]*
Data Subject Rights • The processing of personal and special categories/criminal offence data is processed in a manner that does not comply with the rights of data subjects: 1. the right to be **informed** 2. the right of **access** 3. the right to **rectification** 4. the right to **erasure** 5. the right to **restrict processing** 6. the right to **data portability**	**1**	**1**	**1**	*Action* *[Insert established or planned activities, controls or measures – ask yourself these questions:* *How will this information be quickly accessed/blocked in a timely response to a subject access request, court order or litigation hold? Do your contracts with suppliers include clauses obliging them to assist the council with responding to data subject rights requests?]*

7. the right to **object** 8. Rights in relation to **automated decision-making and profiling**				
Overall Risk Exposure Score	**1**	**2**	**11**	

Section 3 – Risk Assessment and Information Management/Information Security Review
You should enter your Overall Risk Exposure Score against the appropriate Initial Score and Risk Level Box. Remember this is achieved by multiplying the impact and likelihood rates to arrive at a risk rating score for each identified risk. Add these up and then populate the initial score box. Send the DPIA to IM team for discussion and final approval.

Initial Score and Risk level			**Score**
Low –	1- 10	Project can proceed	
Medium	11 – 15	Recommended Minor Actions Required. IM and Project to Agree Timescales	11
High	16+	Recommend Significant Actions required before proceeding	

IM/IS Comments provided by: [Enter IMT Officer Name and Date] IM Officer will enter comments below

IM/IS Recommended Actions

	IM/IS Recommended Action9	Date Implemented
1	Clarification of Data Retention for Claims (initial) and fulfilled	
2	Global Insurance companies. Confirmation of where the processing will take place is needed	
3	Clarification on Lawful Basis – you have to have one! Is it Contract, Legitimate Interests, Are Councils required under law to have public liability insurance	

Final Agreed Project Risk Rating (Tick relevant box)	
Risk level	**Agreed Outcome: Closed. Open and under Review**
Low 1-10 - Project can proceed	
Medium 11-15 – Recommend minor actions are required before proceeding	
High 16+ - Recommend significant actions required before proceeding	
Please Note: All Recommended Actions will be documented on the Review section of the online DPIA register and monitored against agreed timescales. If some/all of the recommendations are not accepted this must also be captured in the Review section	

Sign off Level – Recommendation

Guidance Note on DPIA Sign Off

DPIAs should be signed off by the Information Asset Owner (IAO) for the information that will be processed.

The IAO needs to be satisfied with the level of information risk that the service area is taking
.
The IAO should be at Director or Head of Service level (the IAO role should only be devolved below that level with Director/Head of Service agreement and we would advise that this delegation is documented as part of the department's processes)

If there is more than one IAO (i.e. information will be used from more than one service area) then if all the information sits within one department the senior officer that has responsibility for the entire department may sign the DPIA off.

Where the information that will be processed comes from across the organisation then the SIRO (Senior Information Risk Owner) should sign the DPIA. However, they should only do so once the relevant Information Asset Owners have reviewed the DPIA and confirmed that they are happy for the SIRO to sign the DPIA off (the departments are still responsible for risks to their information).

If any recommendations and/or mitigations are not accepted, then this must be documented, and the signatory must capture this

This DPIA must be signed off by either IAO or SIRO whichever is appropriate (as outlined above):

Tick Box	Level
	Information Asset Owner
	Senior Information Risk Owner

Section 4. Signatories

Guidance Note – 4

If any of the captured mitigations and IM recommended actions will not be implemented, then the signatory must capture this here and by signing they confirm they accept the additional risk posed by this.

I am satisfied that this DPIA is an accurate summary of the intended processing of personal data, the related risks and the mitigations that will be adopted.

Signature of Information Asset Owner

_____

Signature of Senior Information Risk

_____

Print Name and Role of signatory

_____

Date……

_____