Data Protection Impact Assessment (DPIA)

Project Name:	End User Services Contract Retender
Project Manager or Sponsor (PM):	Bernie Harrison (PM) / Sarah Cullen (PS)
Name of person completing the DPIA if different to (PM):	
Service Team and Department:	CDS
Relevant Director and Executive Director:	Paul Golland Elaine Jackson
Service Area Cost Code:	NA
Information Management Champion(s) for service area:	
Date DPIA received by the IMT:	
Date approved by DPO:	
Date approved by IMT :	

1 Project Scope

Projects overview

The End User Services contract is due to end in March 2024. The tender process needs to commence to ensure continuation of service post March 24.
This contract encompasses the services listed below.

- Remote Service Desk (Telephony, Chat & Web channels).
- ITSM tool (Service Now) management.
- Software license management (Snow).
- SIAM (Service Integrator).
- Onsite Deskside team.
- Device build and management – including application packaging and deployment.
- AOVPN.
- Citrix Cloud.
- SSL certificates - Monitoring and management of internal and external certificate expiry dates and implementation of internal SSL certificates.
- Monitoring and managing services at the OS and application layer.
- Active Directory and Azure AD - Monitoring and managing.
- PKI - Group certificate in Azure.
- Office 365 – Monitoring and managing.
- Asset Management.
- Microsoft Store Management.

Potential impact

The Supplier is not processing personal data related to customers, residents and other suppliers of the Council, the Supplier will be involved with processing the data of council employees such as name and contact details in line with carrying out their responsibilities of the contract.

It is not anticipated that the procurement of a new supplier(s) will have a detrimental impact on any of the groups that share protected characteristics, as there are no changes to current Council policies or procedures planned. Nor will there be instances of the new supplier processing personal information on the Council's behalf. This procurement is to ensure a continuation of services and support to the ICT End User Services.

Key Stakeholder

Chief Digital Officer	Paul Golland
Head of Service (Sponsor)	Sarah Cullen
Programme Manager	Paul Cohen
Project Manager	Bernie Harrison
Business Analyst	Richard Wyatt-Jones
Technical Architectural Manager	Jon Mellor
Enterprise Architect	Pravin Varsani
Digital Security Manager	Owen Smith
Service Delivery Managers	Jon Raby & Steve Jones
Finance Manager	Terry Gillam (interim)
Contracts Manager	Fahid Ahmad
Finance & Contracts Analyst	Terry Gillam
Procurement Manager	Gerard Gough
Procurement Officer	TBC - Procurement Team
CDS Management Team	Communicate to this team - via Core Tech Board
Staff and 3rd Party Suppliers/Vendors with access to Croydon's IT systems	

2 Data Description

Answer the questions below so that there is a clear understanding about how the information will be used, who will use it etc. Remember that it's personal information (i.e. information about individuals) that you need to be concerned with. If you do not have answers to all the questions at this time, simply record what you do know.

Whose information is being used? - *Are there additional concerns that need to be considered due to individuals sensitive/ complex circumstances? i.e. vulnerable person*	There will be NO processing of personal, sensitive, or special category information in relation to the council's residents, customers and other suppliers. The supplier will be responsible for the maintenance, management and monitoring of the systems listed in section 1. This does not involve looking at or reviewing personal data. The Service Desk will triage and raise a ticket that will go to themselves or other suppliers, so the supplier will be involved in a low level of processing of personal information of **employees** such as name and contact details as required to carry out their responsibilities to the contract. There may also be personal info contained in the context of the tickets raised by the Service Desk to setup or support a specific user. Once again, this user would be an employee of LBC and not residents or clients. **Employees** name and contact details are also held securely within the Microsoft Active Directory services.
What information is being used? - *Consider the nature of this information E.g. Child's social care file*	There will be NO use of personal information to support the supplier in carrying out their responsibilities to maintain, manage and monitor the in-scope systems. There may also be personal info in the context of the tickets raised.

Does it include special category or criminal offence date?	No
Can an individual be identified easily from the information?	Yes, potentially. There will be personal info in the context of the tickets raised e.g., a person's name (employee) and contact details. There is also similar data within the Active Directory system.
What is the potential impact on privacy of this information? - *What are the risks/ impact to an individual if this information was lost, stolen or manipulated?* - *E.g. could it be sold?*	There is a very low risk of impact on any individuals because the supplier will only be accessing contact details to carry out their responsibilities of the contract.
Will this change the manner in which we handle, use or protect this information? *e.g. should it be encrypted?*	No

3 Consultation process

Consider how to consult with relevant stakeholders.

When did you consult individuals?	No consultation with individuals conducted because the supplier will not be accessing or using any personal information for residents or customers. Will only be working with Council staff in carrying out their responsibilities, setting up new users and telephone/email communication. Therefore, the supplier will know staff names and contact details and in some cases home address is known where equipment needs to be delivered/collected.
How did you consult individuals?	NA
If not explain why it is not appropriate.	There is an exceptionally low risk of impact on any individuals because the supplier will not be accessing or using any personal information.
Who else within the organisation have you consulted with?	CDS Technical Architects CDS Digital Security Manager
Do you need to speak with your processor to assist?	**No**
Do you plan to consult information security	Have consulted and will work with the CDS

experts or any other experts?	Digital Security Manager on the procurement of the supplier.

4 Assessment of necessity and proportionality of data usage

What is your lawful basis for processing?	There will be NO processing of personal information. There are standard contractual clauses - UK GDPR.
Is consent being relied upon to share the information? Has explicit consent been obtained? Are data subjects able to opt out from giving consent?	NA
Does the processing actually achieve your purpose?	NA
How will the information be collected? Verbally, forms, intranet, interview, 3rd party, anonymous)	NA
Is there another way to achieve the same outcome?	NA
How will the information be used? *e.g. to write a report*	NA
Do the individuals know and understand how their information will be used? If there are changes to their information does the privacy notice need to be amended?	NA
How will it be stored, kept up to date and disposed of when no longer required? *e.g. stored in locked cabinet/securely shredded*	NA
How will you ensure data quality and data minimisation?	NA
Who will have access to the information within LBC? - *Include approximate number of users*	NA
Are there new or significant changes to the way we manage, use, handle or collect this information? - *Include any identified concerns for the individuals, would these changes heighten risks involved*	NA
Will individuals within an existing database be subject to new or changed handling? - *If yes amendments need to be made to the privacy notice and these individuals need to be informed.*	NA
What are the internal arrangements for processing	NA

this information? *e.g. number of staff who will have access*	
How will the information be updated? *e.g. monthly check*	NA
Does the project involve the exchange of information outside of the UK and are there set standards for how the information will be treated? How will you safeguard international transfers?	NA
How will you prevent function creep?	NA

5 Assessment of the risks to the rights and freedoms of data subjects

You must describe the source of risk and the nature of potential impact upon individuals and identify any additional measures to mitigate those risks.

5a Security

Who will be responsible for the control for this information?	Paul Golland
How will the access to this information be controlled?	There will be no accessing of personal information.
Is the data correctly managed to reduce the risk of collateral intrusion to the data subject?	NA
Are there adequate provisions in place to protect the information? If so what are they? *e.g. Process, security*	NA

5b Sharing

Who is the information shared with, why are we sharing the information with this organisation?	NA
What purpose does the information we are sharing have to the third party? - *Ensure that we only share relevant information and not excessively*	NA
Who will have access to the information, externally? - *Include approximate number of users* - *Describe any sharing arrangements and what the level of access is. It may help to produce a diagram to show the data flows.*	NA
How will it be transmitted to third parties and when? How often?	NA
Is there a data sharing agreement in place?	This will be put in place as part of the

	contract agreement process.
At what stage will the information be transferred?	NA

5c Identified Risks and assessment:

You should take into account the sensitivity of the information and potential harm that inappropriate disclosure or use of the information could cause to any individuals concerned. You should also consider the reputational loss to the Council and the potential for financial penalties being imposed by the ICO.

To assess the level of risk you must consider both the **likelihood** and the **severity** of any impact on individuals. A high risk could result from either a high probability of some harm or a lower possibility of serious harm.

The severity impact level and likelihood should be scored on a scale of 1 to 10 with 1 being low severity and 10 high. The two scores should be **added** together. The RAG status is derived from the following scale:

Score:

- 15 to 20 = Red (High)
- 8 to 14 = Amber (Medium)
- Below 8 = Green (Low)

To be completed by Project Sponsor

Risk Identified	Severity of Impact	Likelihood of harm	Overall RAG rating
To focus on info that is shared before consent – is dob/ anon details of the family/ sw/mgr/lawyer/ reasons for eligibility			

6 Identify measures put in place to reduce risk.

You must now identify additional measures you could take to reduce or eliminate any risk identified as medium or high risk in step 5.

To be completed by the Project Sponsor

Risk Identified	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated / reduced / accepted	Low / medium / high	Yes / No

Sign off and Record sheet

Item	Name/date	Notes
Measures approved by: Residual risks approved by:		Integrate actions back into project plan, with date and responsibility for completion. **If accepting any residual high risk must consult ICO before going ahead**.
DPO advice provided:		**Summary of DPO advice:** *(DPO should advise on compliance, measures to mitigate risk and whether processing should proceed)*
Consultation responses reviewed by:		If your decision departs from individuals views you must explain your reasons.
DPIA to be keep under review by:		

If you require further guidance to complete this DPIA please contact:

Information Management Team (IMT)
Ext: 47777
Email: information.management@croydon.gov.uk

Data Protection Officer
Email: DPO@croydon.gov.uk