Privacy Impact Assessment

All processing of personal data, whether staff or citizen related, must be subject to a privacy impact assessment (PIA). All data processing activity (including obtaining, recording, keeping, sharing, disclosing; erasing and destroying data) **MUST** comply with the Data Protection Act 2018 and GDPR. The Privacy Impact Assessment process helps managers identify how the collection and use of people's personal data may affect an individual's privacy and work out way to protect citizen's privacy at all times.

All PIA's will be reviewed by the DPO to ensure that they comply with current technical and information governance requirements.

All high risk PIA's will be reviewed by the Information Governance (IG) Steering Group. If high risks cannot be mitigated then either the project will be refused or further guidance will be sought from the ICO before processing is approved. The ICO can take up to three months to approve high risk processing.

The form should be completed* by the service but support can be provided by the Information Governance Team (6398). Please return the completed form to feedback@luton.gov.uk for approval.

This form should be completed for all new:

- IT systems
- data processing,
- LBC projects
- Governance Boards (decision making)

*One assessment should be completed for each system/process

Project type	Consultation and engagement platform	**Project name**	Delib Ltd Citizen space
Department	Communications	**System/Asset name**	Citizen space
Lead officer	Mark van Vastenhoven & Shaista Khan	**Service/Directorate**	Chief Executive
Telephone	01582 546567	**DPO**	Katy Bodycombe / Usman Iftikhar
Email	mark.vanvastenhoven@luton.gov.uk	**Telephone**	7335
Data subject type	Respondents to (public) consultations/engagements	**Email**	Katy.Bodycombe@luton.gov.uk
Planned start date	week commencing 6 January 2020		

1a: List all personal data that you will be collecting as part of this data processing?

Personal data is data that relates to a living individual who can be identified directly or indirectly from the data. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Examples of personal data are the name and address of an individual; email and phone number; a Council Tax reference number or an NHS number

The platform Citizen space is GDPR compliant. We understand that those that want to be regularly notified about new consultations are submitting their personal details for that purpose only, and are asked for their consent.

Standard public consultations are anonymous. Though depending on type of public consultation we occasionally gather 1,2, 3 and 4. 5 is rare, but can apply.

1. Name
2. Address
3. Email address
4. Postcode
5. Date of birth

1b: List all special category data that you will be collecting as part of this data processing?

Feedback from public consultations/engagements. These are anonymous in general though at times personal data are collated. Note that standard procedure is to ask demographics.
Depending whether and to what extent LC services require specified demographics for public consultations. These are categorised as:

- gender
- age
- race or ethnic origin
- religious beliefs or other beliefs of a similar nature
- disability
- special needs
- marital status
- employment status
- sexual orientation

2: Why are you collecting this data and how do you intend to use it?

- List each purpose.

1. Services that request a consultation/engagement activity do want to collect (some) personal data, so that particular questions and comments can be analysed upon individually
2. Postcodes and/or addresses are asked for in situations that understanding of geographical distribution is required
3. Demographics are usually gathered for services to obtain insight in background of respondents, in order to help ensure that policies are aimed at the right audiences. Which categories are asked depends on the nature of the services.
4. Email addresses are collected at times e.g. as part of a prize draw, as incentive to take part in consultations. Email addresses are also used to gain consent for interest areas that respondents would like to engage in future.

3a: Do you have a lawful basis for collecting/processing this data?

- List all relevant acts

No	☐		
Yes	X	Please list lawful basis for each processing activity	1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose. Regarding public consultations this only applies if Luton Council services particularly require personal data for their policies and procedures. 2. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). This with regards to legal duty to consult e.g. as laid out in specific Housing legislation and or regulations for Health, Education, and Highways. 3. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

3b: If you are relying on consent how do you plan to evidence this?

Will you obtain consent at the point of collection? By accessing the platform users agree with term and conditions		Yes	x	No	
How will you gain consent?	New consultation alerts will only be sent to subscribers who have given their consent (opted in) to receive information. Each consultation survey also includes a standard				
Have you attached a copy of your consent form with this PIA?		Yes		No	

4: If you are relying on consent have individuals been given the opportunity to refuse permission to use their data for this project?

No	☐	Why not?	
Yes	X	How will this impact their ability to access the service?	A data sharing agreement is in place with Delib as part of the service agreement. People have the option to answer anonymous

How will you inform individuals of the consequences of refusing permission? There is an opt in process for anyone who wants to access Citizen Space and for being kept	Yes	X	No	☐

5: Do you have a process for deleting data if an individual requests to be forgotten or restrict processing?

No	☐	Why not?	
Yes	X ☐	How?	Yes, if people do not want to be informed anymore about new consultations/engagements then we delete their personal data i.e. email address. In line with consultation procedure: Data check

6: will you carry out any automated decision-making or profiling of the data?

No	X		
Yes	☐	How?	

7: Are you planning to share this personal data with any other internal service?

- List each internal service and the reason for access.

No. Any data sharing is confidential and only accessible to that particular consultation. This relates to all internal LC services as potential commissioners of public consultations.

8a: Are you planning to share this personal data with any other external service?

- List each external service and the reason for access

Only on rare occasions on explicit request e.g. when working in partnership. (If working in partnership then third party need separate PIA). Third parties that Luton Council have worked with in the recent past: Central Bedfordshire Council, Police services, Fire services, NHS England. This also includes organisations liaised with the Council such as Luton Culture. Note that this list is not exhaustive .

8b: If you are planning to share this data with external services do you have an approved Information Sharing Agreement (ISA) in place?

- You will need to send a copy with this form

No		Why not?	
Yes	x	ISA Reference?	Mailchimp will be used for subscribers who will opt in. An Information Sharing Agreement is already in place between Luton Council and Mailchimp.

9: What are the benefits to the individual of their personal data being used for this project?

In general: making public consultations more meaningful for individuals

10: What are the organisational benefits of the individual's personal data being used for this project?

1. Learning about key audiences, at operational level
2. As part of Strategic Policy development
3. Allowing more and further engagement with and within the Luton community
4. Providing credibility and authenticity to the consultation

11: What are the potential negative impacts to the individual of their personal data being used?

1. Individuals may not want to be recognised as stakeholders

12: How will you make sure that the personal data you are using is kept accurate and up to date?

Who will have access to the system and how will that access be controlled? Give description of potential users and authorisation process. Include process used when users leave employment and how the account will be disabled

Data will be stored in the Citizen Space portal. Data is stored in ISO27001 accredited data centres located in the UK & owned by Rackspace. Rackspace is certified to ISO 27001:2013 & PCI DSS Level 1 – see https://www.rackspace.com/en-gb/compliance for a full list of certifications.

It will only be accessible to the main site admins within the consultation team and the service requesting the consultation. This is on a case by case basis – depending on purpose of the consultations/engagement. Access is via work email. Permission to access the portal will be immediately revoked when someone leaves employment with their email address being disabled. Site admins will monitor inactive users and grant limited time access to service for the consultation/ analysis only. Personal public data will be updated from time to time using mailchimp features for opt-ins and opt-outs; and will be updated every 6 months.

13: How will you ensure that all users have attended mandatory/follow up data protection training

LC staff are obliged to be trained regarding up to date data protection legislation

14: How long will you need to hold the personal data for?

Please check the data retention schedule matches with what you put here:

Six months is our standard in the consultation team

http://intranet/Departments/ChiefExecutive/TandT/BI/IG/Pages/retentionschedules.aspx

15: Is the corporate retention schedule up to date?

- Make sure you copy a link to the schedule here

No	☐	Why not?	For Data protection officer to advise/ Usman to check and advise
Yes	☐		

16: Does the process/system enable timely location and retrieval of personal data to meet Subject Access request requirements?

Describe retrieval process. If the process refers to another paper or electronic system then this process is also required, e.g. tracing of paper case notes by an electronic system:

No	☐	Why not?	For Data protection officer to advise
Yes	x	Retrieval process description:	This would be done as per the Data Sharing agreement which is part of the Delib service agreement.

17. Will any reports produced only contain anonymised or aggregated data?

Yes	x	How?	At times both, though anonymous is the default position
No	☐	Why not?	

18. How will you avoid causing unwarranted or substantial damage / distress to the individual when using their personal data for this project?

By clarifying that personal data will only be used for purposes as indicated, and not for any other reason e.g. promotion. This will be in accordance with the Data Sharing Agreement which is fully compliant to GDPR.

19. Who is the Information Asset Administrator?

Who will be responsible for the data quality (accuracy of the information) in the process/system? An internal member of staff must be named as the responsible person for maintaining the system/database and who will carry out data validation checks: Delib and LC services commissioning the consultations.

20. Has the information Asset Register been updated?

Yes	☐	How?	For Data protection officer to advise
No	☐	Why not?	

21. Who will have access to the system?

Only LC designated staff will have access to the system. Respondents do not log into the system at all. They get access to only public pages related to consultations. The consultation team consisting of two senior officers have full access to the system, while services will be given access as and when needed.

22. How will that access be controlled?

Only site admins can add/ delete and change roles attributed to users.

23. Will training on the use of the system be provided and a list of trained personnel maintained?

Yes, use of the system will be accessible to a degree within the organisation, with two senior consultation officers as controllers- Site admins. Training has been provided to key services who often engage with the public and carry out consultations with a view to slowly enable them to create their own online surveys. However the site admins will manage all public surveys. A list of internal LC staff users will be created and monitored, attributing roles with varying degrees of access- Department user/ Individual/ Analyst only.

24. How will the data be held / stored?

Data is stored in ISO27001 accredited data centres located in the UK & owned by Rackspace. Rackspace is certified to ISO 27001:2013 & PCI DSS Level 1 – see https://www.rackspace.com/en-gb/compliance for a full list of certifications.

25. How will you make sure that you are holding data for the appropriate length of time, and no longer?

This is in line with the council's policy as explained earlier.

26. Will you be transferring personal data to a country outside of the UK?

Yes	☐	Where/why?	
No	x		

27. How will you ensure that third parties will comply with data protection obligations?

Mailchimp will be used as a third party. A Data Sharing agreement is already in place with Luton Council.

Anyone who uses Citizen space agree with the term and conditions, including GDPR requirements

28. What technical security measures will be in place?

Citizen Space is a fully secure system: the platform is ISO:27001 certified and Cyber Essentials certified. Delib has been handling sensitive data since 2004, and is registered with the UK Information Commissioner's Office. Users will have an individual secure log in and they will have password protection.

29. How will personal data be transferred / shared between the agencies involved in this project?

Data in transit is encrypted in using either TLS 1.2 or SSHv2 using secure cipher suites.
Delib does not transfer data internally between microservices. All processing is self-contained.
Citizen Space is hosted on virtual servers on a single-tenancy basis, i.e. each customer organisation is assigned a dedicated virtual machine which is not shared with other customers. Both the application server stack and data store are hosted in the virtual machine, providing logical separation of data between customers organisations. Separation is enforced at the hypervisor level and each virtual machine has its own IP address.

30. What measures are in place to ensure only appropriate and authorised access to, and use of, personal data?

Luton council admin users are required to login using an email address and password (set by the user themselves). Site Administrators are responsible for adding users, and deciding which access privileges they have. Site administrators can also promote and demote users, and suspend and delete users.

31. How will technical and organisational security be monitored / audited?

Citizen Space is a fully secure system: the platform is ISO:27001 certified and Cyber Essentials certified. Delib has been handling sensitive data since 2004, and is registered with the UK Information Commissioner's Office.

32. who has access to the asset

Define as UNIT/TEAM, ALL COUNCIL , EXTERNAL BODY. Please give a brief description of who can access this data

Senior Officers of the Consultation team and Citizen Space Account Manager. Luton council admin users are required to login using an email address and password (set by the user themselves). Site Administrators are responsible for adding users, and deciding which access privileges they have. Site administrators can also promote and demote users, and suspend and delete users.

33. How will data be received and stored?

From perspective of Provider: Internal (Server on-site), Externally Hosted Server - Cloud, External (offsite storage), External (Cloud Storage), Shared Drive (internal Server), External Server

Specify the size of the full contents associated with this Information Asset. If IT system, specify size in GB, for Paper Records, specify amount of space required, No. of Storage boxes

On Citizen space Cloud storage. This completely depends on the volumes of responses to consultations. On average over a year this can be thousands.

From perspective of LC Consultation team: Data will be stored on Citizen Space and if extracted documents holding data will be in pdf and excel format. If need be these are kept on the council consultation area on the server. Access is only through council secure entry and secure passwords for senior consultation officers only.

34. How often is the asset updated?

Response from Delib: Citizen Space is updated a number of times a year to bring in new features and keep the software and infrastructure up to date (please see our release announcements list here for details of recent updates). Customers are notified in advance of new features and improvements: https://delib.zendesk.com/hc/en-us/sections/200816049-Citizen-Space-Release-Notes.

We also monitor routinely for any applicable security updates relevant to our infrastructure and software and will apply these as soon as they are available. It's difficult to put a number on these as they are identified and applied whenever they are relevant to our software and made available, and this may vary year to year.

35. What Impact will it have on the Organisation to deliver business if the asset is no longer accessible?

Moderate

36. What protective marking is on this data?

No Protective Marking, Unclassified, Marked Official, Marked - Official Sensitive , Marked - Official Confidential
Is there a Business Continuity plan in place and if so what are the details.

Not Applicable – This is an online public survey with no protective marking. All questions are for public.

37. Is there a Business Continuity plan in place and if so what are the details.

Provide high level info: If need be all data (including personal data) can be downloaded e.g.in Excel format by 'site admins'

Delib has a continuity plan for Information Systems, this is part of the service agreement.

There is an INTEGRATED BUSINESS IMPACT ANALYSIS (BIA) AND BUSINESS CONTINUITY PLAN (BCP) FOR Communications and Marketing (this is available on the team's section of the server)

38. Has the asset been published on the Public Information Asset register (IAR)?

Response from Delib: This is a question for yourselves as a council rather than us, as each organisation tends to have its own IAR in order to keep track of the assets it uses. I'm afraid we wouldn't know if anyone at Luton Council has added Citizen Space to your asset list already.

39. Can any of the asset details be published?

If so please describe here –
Response from Delib: Yes, you're welcome to list Citizen Space on your IAR. It would normally be listed as a consultation platform. An IAR is something that is completed by council staff rather than us, as it is your own asset register, but I've attached an example IAR template which the National Archives supply with some Citizen Space details completed, which I hope will help you if you want to add Citizen Space to your IAR. Some columns in this template I've left blank as these need to be answered in line with your own Council guidelines, but all the generic parts I've given you suggested wording. Of course, this IAR template may not match exactly with the column topics in your own, but it's likely to be similar and I hope it will help you to copy paste into the relevant sections of your own IAR if you do want to add the platform to it.

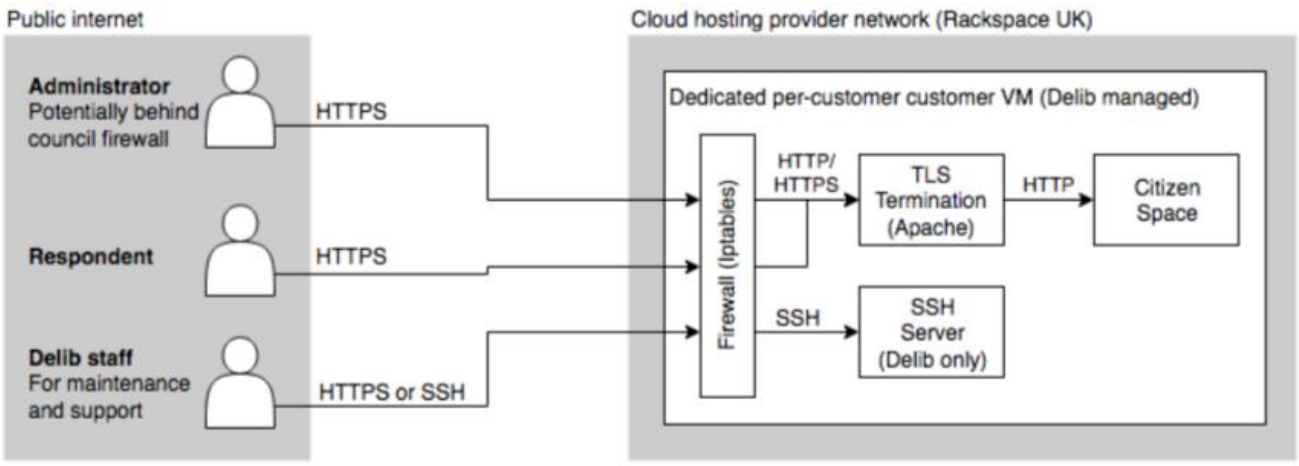
40. Describe the flows of data

Data flow diagrams provide a graphical representation of how information moves between processes in a system. This would normally be a diagram showing how the data flows from the customer or third party organisation into the council and then how the information flows into other IT systems and then back out of the organisation to third parties or the customer.

In the first instance it may be best to display the connections between system on an excel spreadsheet. The IG team will then work with the department to put this onto a diagram via visio.

This diagram must show all data controllers and processors, storage location and storage method, data fields collected, individual/team/organisational access to personal data, security measures for storage and transfer of data

All https traffic is TLS 1.2. The site is accessible from any supported web browser.



Information Governance Team's risk assessment of this project's overall compliance with GDPR and likelihood of non compliance	
Risk score	
Likelihood score	

Information Governance Team's conclusions regarding this project's overall compliance with GDPR

Information Governance Team's recommendations for changes / refinements to the project which are required to ensure compliance.

PIA reference number	

Approval

As lead officer, I confirm that the information recorded on this form is, to the best of my knowledge, an accurate and complete assessment of the potential privacy impacts of this project.

Name	Signature	Date

Please return your signed and dated form to:

Information Governance Team
Luton Council
feedback@luton.gov.uk

If you have any questions about the Privacy Impact Assessment process, or if you need any help completing this form, please contact us using the email address, above, or by telephoning the Information Governance on 018582 546398

Privacy Impact Assessment reviewed and approved by Luton's Data Protection Officer:

Name	Signature	Date