DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project. **You should only complete this full DPIA where you have been told that one is required by the Information Rights Team or the Data Protection Officer.** If you have not been asked to do a full DPIA please do the pre-screen first. Search on essentials for 'DPIA' and download the DPIA pre-screen.

A DPIA is a legal requirement therefore please complete the form in as much detail as you can so the council has the necessary assurances of data protection legal compliance. Avoid technical language and jargon, and assume little prior knowledge of your subject and project by readers.

Ethics screening: If you have been advised to proceed straight to a full DPIA please complete the ethics screening at the end of this document. If you have already completed a DPIA pre-screen then the ethics screening need not be duplicated.

Project Name	**Instagram – TieTheKnot Camden**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Corporate Services – Registration Phill Quickenden
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail. Explain any acronyms on first use.*	To maintain our Instagram social media account. Instagram is a social media platform that has become increasingly popular over the years, with over one billion users. This platform has become an essential tool for businesses looking to connect with their target audience and promote their brand. It is a visual platform that is centered around images and videos. We plan to upload regular updates – providing informative feedback to the community, advertising various developments with the Camden Registration Services.	

	We will do regular amendments to uploaded posts, ensuring social media followers are able to see current activities and promotions within Camden. For example, post relevant to marriage in various venues (pubs, hotels and the town hall etc.) can be updated within certain cycles. Using Instagram for Camden's business can drive brand awareness, boost sales, and build and track audience engagement. It's an excellent way to find customers within Camden - where they're already spending time. It can also provide valuable audience insights to use with all our marketing plan strategies. Overall, to help Camden promote business ventures and its social media presence.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	Soon as possible

Initial risk assessment: Screening questions are to do an initial risk assessment and highlight problems that need to be addressed. Answering "Yes" to any of the screening questions above represents a potential privacy/data protection/security risk factor.

If you have already completed a pre-screen, attach it to the DPIA, skip q1 and go to q2 otherwise please answer the questions below.

Q 1		Step 1: Initial Risk Assessment	Yes/No
1.1		Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	No
1.2		Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	No
1.3		Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	No
1.4		Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	No
1.5		Might the project cause data that was previously anonymous or pseudonymised (where a code is used instead of eg names) to become identifiable ?	No
1.6		Does the project involve multiple organisations, eg public sector agencies eg joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	Yes
1.7		Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	No

1.8		Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	No
1.9		Will data be combined, compared or matched from multiple sources?	Yes
1.10		Will you process biometric (finger print /facial recognition) or genetic data?	No
1.11		Will the personal data be processed out of the U.K? Eg any providers have out of UK servers?	Yes
1.12		Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	No
1.13		Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.14		Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	No
1.15		Will personal data be processed which could result in a risk of if there was a security breach?	No
1.16		Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

<table>
<tr><th colspan="11">Step 2: What personal data is being used?</th></tr>
<tr><td>2.1</td><td colspan="7">Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?</td><td colspan="3">New/Changed

New</td></tr>
<tr><td rowspan="5">2.2</td><td colspan="10">What data will be processed/shared/viewed?
Put a YES in the box as appropriate</td></tr>
<tr><td colspan="10"><u>Personal Data</u></td></tr>
<tr><td>Name</td><td><u>Yes</u></td><td>Date of Birth</td><td><u>No</u></td><td>Gender</td><td><u>Yes</u></td><td>National Insurance Number</td><td><u>no</u></td><td>Financial Information about the person</td><td><u>no</u></td></tr>
<tr><td>Address</td><td>no</td><td>Email address</td><td>No</td><td>Telephone number</td><td>No</td><td>NHS No</td><td>No</td><td>Other eg a reference number such as Mosaic ref</td><td>No</td></tr>
<tr><td colspan="3">Other data (Please state):</td><td colspan="7">Photographs</td></tr>
</table>

	Special Categories of Personal Data							
	Racial or ethnic origin	No	Fingerprints/ Biometrics	*No*	Religious or philosophical beliefs Political opinion			Only if obvious from clothing or headwear etc
	Trade Union membership	no	Physical or mental health or condition					Only if obvious from equipment: walking stick, wheelchair etc. Or more visible conditions
	Sexual life or sexual orientation	Only inferred from composition of couple	Housing records Social services records	No	Tax, benefit or pension records	No	Employee/HR records	No
	Other data *(Please state):*							
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	No						

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data - how is the data being used, how it is being handled, stored and transferred/shared? Please use plain English!**	We will upload the image to Instagram, adding any relevant text or captions, selecting the audience for the post, and choose any additional options such as location tagging or sharing to other platforms. When adding text, we might include a description of the image, a hashtag to categorize the post, and the first names of the couple and location of their ceremony.. Depending on the social media platform, we may have the option to choose who can see the post. This might include selecting specific individuals or groups or making the post public so that anyone on the platform can view it. For example: targeting audience by age, background and likes. Any information gained will be completed with market research, to ensure a satisfactory standard is upheld within legal frameworks. Any images will be stored on secure Camden devices (laptops etc.) as well as any social media presence operated by Camden.
3.2	**Explain in as much detail as possible why this is being done**	Using Instagram for Camden's business can drive brand awareness, boost sales, and build and track audience engagement. It is an excellent way to find customers within Camden - where they are already spending time. It can also provide valuable audience insights to use with all our marketing

			plan strategies. Overall, it will help Camden promote business ventures and its social media presence.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		Yes.
	External organisation or partner Name	**Controller or Processor?**	**Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection? Yes/No/In progress**
	Instagram	Joint controller	Yes
3.4.	**Please explain your process from start to finish. you can do this is a diagram if you wish, or a flow chart, or describe it. You can attach a document if that's easier.**		Please refer to point **3.1.**
3.5	**How will you handle data in your project, how will use store and share it. Please explain**		**Password protected; additional data will be stored on secure Camden work laptop. Work phone**

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify the Lawful Basis for processing personal data/special category /criminal data.** **If you don't know then please ask Data Protection Advice Team for advice (DPA@camden.gov.uk if you have no named Information Rights Officer advising)** **If not processing the category say N/A**		
	Personal data Article 6(1) UK GDPR condition Where couples are providing us the photographs directly: article 6(1)(a) consent. Where the photographs are provided by photographers article 6(1)(f) legitimate interest of Camden. As a commercial service this legal basis is available to us. A legitimate Interests Assessment has been undertaken.	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Where couples are providing us the photographs directly for any incidental special category data article 9(2)(a) explicit consent.	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Not applicable
4.2	**If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Data Protection Advice Team have advised this is appropriate**		
	Consent will be obtained from the couple where possible using our consent form. In some circumstances we may receive pictures from photographers, who have contracts with the couples, giving them the freedom to use their pictures as they wish. We will still seek consent from any couples the photographer provides pictures of if we can, but should we have no reply we will approach the photographer for a "collaboration". These posts are shared posts, where we are not explicitly posting the content, only sharing content posted by another Instagram user.		
4.3	**How will you ensure data quality and data minimisation- how will you ensure the data is accurate and you are only using the minimum data to achieve your aims?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below		

	To summarise, all information gathered will be clear and concise – irrelevant data will be discarded. This will be completed through a list of validation checks followed by cleaning any irrelevant information. For example, if we source images of a venue, the images will be collated, and the unused photographs discarded. The remaining images will be scrutinised and corrected, ensuring they are to contemporary standards. The images will then be stored in secure folders with access only given to parties who are involved in the process.	
4.4	**Have/ will individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Privacy Notice? Remember telling people is not the same as asking for consent	Yes
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**	
	Yes, a privacy notice.	
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject.	
	No	
4.7	**Data Retention Period - how long will the data be kept? What will happen to the data at the end of the project – deleted or kept? If you're using a processor what are the arrangements with them for data at the end of the project?**	
	5 years	

Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples include Mosaic, SharePoint, shared drives,*
	Instagram **Shared drive** **Camden Website**
5.2	**In what country is the data stored?**
	UK London Borough of Camden. Instagram Servers: Denmark, Ireland and Sweden.
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	Management - Business Development Manager, Registration Manager.
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Yes, by [redacted] through Camden provided work laptops and phones. If other parties need access they will have to liaise with [redacted]
5.5	**Is there an ability to audit access to the information?**
	Yes I will be keeping a record of the information in a single folder on our S-Drive
5.6	**What security and audit measures will there be to make sure that data is kept safe?**

	Password protected on work laptop and Instagram password
5.7	**Has the Information Security Team advised on the security measures? What were their comments?** **"I would advise to use a shared mailbox to register the account as well as set up 2FA to bolster security.** **Furthermore, the account should be accessed on a Camden corporate devices and not setup onto personal devices.** **Restricting amount of individuals and devices that have access to the social media account is also recommended"** **Kind regards,** **Sharief Ali-Khan**

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Facial recognition by 3rd parties. We will be using photos of couples, so there is a risk their faces could be picked up by facial recognition technology. Unlike many other forms of data, faces cannot be encrypted. Data breaches involving facial recognition data increase the potential for identity theft, stalking, and harassment because, unlike passwords and credit card information, faces cannot easily be changed.	Unlikely	High	Medium High
Cyberattack Cybercriminals may try to hack into Instagram accounts to steal personal information, such as usernames, passwords, and email addresses.	Unlikely	Medium	Medium

Phishing attacks Hackers may send phishing emails or messages to users, posing as Instagram, and asking for their login credentials. If users fall for this scam, they could unknowingly give their login credentials to the hackers.	Unlikely	Medium	Medium
Malware attacks Users may unknowingly download malware onto their devices, which could steal their login credentials or other personal information.	Unlikely	Medium	Medium
Privacy Intrusion We will sometimes use photographs without consent of the couple, when submitted by photographers who have the right to distribute said photographs, in line with our Legitimate Interests Assessment Form.	Unlikely	Low	Low
Data leaks Instagram collects a lot of personal information about its users, such as their name, age, location, interests, and more. is leaked or hacked, it could be used for identity theft, fraud, or other malicious purposes.	Unlikely	Medium	Unlikely/Medium

Step 7: Identify Measures to reduce risk				
Identify measures to reduce or eliminate risks identified in step 6. *Remember that risks need to be reduced to an acceptable level, and not all risks can be eliminated.* Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by /DPO* The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.				
Risk identified in step 6	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved?**
Facial recognition.	We can inform customers of the possibility. However, the pictures we share, will most commonly have been already shared by couples on their own Instagrams. All couples will consent to the use by use. Facial recognition by 3rd parties would not be under the control or the responsibility of the council.	Reduced	Low	Yes
Cyberattack	Strong passwords, limited number of people with log in access to account. Good password management. Using council devices. The risks of attack on Instagram remain but given the widespread use of this social media are considered proportionate to the processing	Reduced	Low	Yes

Malware attacks	Only use the Instagram on Camden work phones / laptops via Instagram website to mitigate malware attacks.	Reduced	Low	Yes
Privacy Intrusion	We will not directly share photographs from photographers, or house the photographs on Camden devices. Instead, we will only share photos from photographers – where we have no consent from couples – using Instagram's collaboration feature.	Reduced	Low	Yes
Data leaks:	Keep personal details away from any messages, and suggest that once direct message correspondence is initiated all correspondence is through our Camden emails.	Reduced	Low	Yes
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Low				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	No, Sarah Laws, Data Protection Manager
DPO advice	Approved, Andrew Maughan, DPO and Borough Solicitor, April 2023
Information Asset Owner acceptance of residual risks	Phill Quickenden
This DPIA will kept under review by: *(usually the author or the IAO)*	[redacted]

Version Control

Version	Reason	Date	Author(s)
1.0	New draft	29/3/23	[redacted] and Sarah Laws
2.0	New draft	23/04/2024	[redacted] and Sarah Laws

Appendix 1
Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely
Possible	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
Likely	Will reoccur on a regular basis, pointing to some failure in controls
Almost Certain	Willful act, systemic failure in controls

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level* • Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services

Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3 - risk level

Table 4: is the risk level acceptable?

	Score:		PROBABILITY				
			Rare	Unlikely	Possible	Likely	Almost Certain
IMPACT		Catastrophic	5	10	15	20	25
		Major	4	8	12	16	20
		Moderate	3	6	9	12	15
		Minor	2	4	6	8	10
		Negligible	1	2	3	4	5

Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
8-12 Medium / High Risk	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures
15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required

Appendix 2: Ethics screen.

Only complete this if you have skipped the DPIA pre-screen and proceeded straight to a full DPIA. If you did the ethics screen as part of the DPIA pre-screen ignore this section.

Ethical Assessment. In assessing ethics you need to take into account the benefits, proportionate use, possible biases and transparency of the impact of the proposed processing and analysis of personal data on individuals and groups. It is the responsibility of the Project Manager and Sponsor to assess the potential ethical impacts that the intended processing may pose. (These answers can be reused for questions dealing with the same issues in the Full DPIA if the outcome of this pre-screen requires you to do one) The Data Charter is here: Camden's Data Charter - Camden Council

1. *Effects on Residents*

a) *How does use of this data benefit our residents? (Is there evidence of this approach being likely to meet a public need?)*

- Providing content on civil marriages and civil partnerships. Residents will be able to view what is on offer within the borough. This includes information on intent to marry and where to get married.

b) What would be the harm in not processing this data?

- Potential customers going elsewhere, resulting in Camden losing revenue streams. No harm to the data subjects

2. Data Bias

a) How do you plan to identify errors and biases in data collection, analysis and algorithms? Once errors and biases have been identified in data collections, how will they be considered for any future policy or service which uses this work as an evidence base?

- Data Collection:
  Check for missing or incomplete data and ensure that data is representative of the population being studied. Ensure that data is collected in a consistent and standardized manner. Check for potential sources of bias, such as sampling bias or selection bias.
- Data Analysis:
  Check for outliers and data entry errors. Ensure that appropriate statistical methods are used for the type of data being analyzed. Check for potential sources of bias in the analysis, such as confounding variables or selection bias.
- Algorithms: Conduct a thorough review of the algorithm to identify potential sources of bias or error. Test the algorithm with different types of data to ensure that it performs consistently and accurately. Use a diverse team with varying perspectives to review the algorithm and identify potential biases or errors

- *Correct errors: Fix any mistakes in the data.*
- *Address biases: Fix any issues that might make the data unfair or inaccurate.*
- *Communicate findings: Tell everyone what the problems were and how we fixed them.*
- *Re-evaluate policies or services: Look at the data again to make sure that the policies or services are still the best options based on the corrected data.*

b) Who could be negatively affected by processing this data? (How can you show there is a fair balance between the rights of individuals and the interests of the community?

- *Get consent: Make sure people know how their data will be used.*

- *Protect privacy: Keep data secure and private.*
- *Analyze data fairly: Don't let biases or discrimination affect the analysis.*
- *Be transparent: Be clear about how data will be used and who can access it.*

By doing these things, we can protect people's rights and use data fairly for the benefit of the community.

3. *Limitations of Data*

a) *How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?*

- To make sure that only necessary data is processed for a project and no more than is necessary, we can take the following steps:
  Clearly define project goals.
  Identify only the necessary data.
  Minimize data collection.
  Regularly review data processing.

  By doing these things, we can minimize risks associated with data processing and ensure that data is used only for the intended purpose.

b) *How are you ensuring the data used is reliable? (**Data quality**)*

i) *What processes do you have in place to ensure maintenance of data accuracy? (**Data integrity**)*

- To maintain data accuracy and integrity, we can take the following steps:
  A) Validate data during collection.
  B) Regularly clean data to correct errors or inconsistencies.
  C) Implement quality control procedures to identify anomalies or outliers.
  D) Document data source, collection process, and any manipulations.
  E) Control access to data to prevent unauthorized modifications.
  F) Establish data governance policies and procedures.

c) *How have you clearly marked origins and destinations of data used to trace source of errors? (**Data lineage**) (Are all metadata and field names clearly understood)*

- To trace the source of errors, we can use data lineage techniques (pattern based etc) via excel:

Document metadata and label fields.
Use data mapping to identify the flow of data.
Implement version control to track changes made to the data.

These techniques help ensure that the origins and destinations of data are clear and errors can be traced easily and logged.

c) *How could the objectives of this project be completed without processing the data?*

- No, the whole project depends on use of the personal data