Privacy Impact Assessment

Social Media Management Tool

Privacy Impact Assessment – Screening Questions

Question	Y/N	Additional Comments (please give reasons for either a 'yes' or' no 'answer here
Is there a requirement under GDPR to carry out a PIA? NB if there is a legal requirement to carry out a PIA there is no requirement to complete the remaining questions.	N	There is no legal requirement to complete a PIA under GDPR.
Will the project involve the collection of new information about individuals?	Y	The social media management tool will collect new information in a public domain
Will the project compel individuals to provide information about themselves?	Y	The product will give individuals to provide information about themselves in a public and private domain.
Will information about individuals be disclosed to third party organisations or people?	Y	A third party organisations will have access to the information about individuals.
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	The process will continue to remain the same.
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	N	No new technology is being used. A procurement project to replace an existing solution.
Will the project result in you making decisions or taking action against	Y	Individuals will use the solution to provide feedback, complaints, queries that will need to be actioned.

individuals in ways that can have a significant impact on them?		
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, health or information concerning an individual's sex life or sexual orientation or other information that people would consider to be private.	N	There is no expectation that information of this level will be collected about an individual.
Will the project require you to contact individuals in ways that they may find intrusive?	N	Any communication using the product will be started by the individual.
Will the data be held in relation to children or vulnerable adults?	Y	There is the potential that information regarding children or vulnerable adults. This will be limited to full name.

Privacy Impact Assessment

Step 1 – Requirement for PIA – issues to be addressed

To Include:

- Project Aim and Objectives
- Benefits to the organisation, to individuals and to other parties of personal data
- Links to any relevant project documentation
- Summary of Identified Need for PIA (can draw on answers to the screening questions).

A procurement project is underway to replace the councils Social Media Management Tool. The existing contract is with a solution called Crowd Control, but this may be replaced by a new solution.

The council has over 100 social media accounts (Facebook, Twitter, LinkedIn, YouTube) which are owned by departments throughout the council and all managed through a Social Media Management Tool (currently Crowd Control). This helps the Digital and Web Development Team and Communications Team to oversee all the accounts to monitor performance, public communication and risk. The tool also enables posting content and messaging, analytics and reporting, user administration and account management for all council social media sites.

The aims of the project are to procure a new Social Media Management Tool and implement it by the end of November 2018. This will means that the Digital and Web Development Team can continue to monitor all social media activity and accounts throughout the council to meet and enforce the Social Media Policy. The tool reduces the risk of the council having over 100 social media accounts, as it allows them all to be monitored in one place.

The Social Media Management Tool may collect personal data in a public and private domain through the use of existing social media channels such as Facebook, Twitter and LinkedIn. All communication through the councils social media accounts will be hosted in the Social Media Management Tool including names of users, any personal information they may send to us to help resolve a query. This could be in a private message, or in a public post.

The main benefit of the social media management tool is that it allows the council to manage the risk of having over 100 social media accounts, by allowing the Digital Team to monitor all interactions in one place. It also allows for better management of user permissions and access to accounts.

All project documentation is saved here - https://edrmlive/livelink/llisapi.dll?func=ll&objId=87954763&objAction=browse

Step 2 – Information Flows/Nature of processing

To Include:

- Description of collection, use, retention and deletion of personal data- is any sharing of data involved?
- Explanation of data flows – diagram or description detailing: controllers and processors, storage location and storage method, personal data fields collected, individual/team/organisational access to personal data(audit trail), security measures for storage and transfer of data
- Number of individuals likely to be affected by the project-do they include children or other vulnerable groups?
- A flow diagram is likely to be helpful here.
- Does the data include special category or criminal offence data?

All incoming data/messages will come through the social media channels (such as Facebook, Twitter or LinkedIn) either through the public domain, with users posting to the public, or through the private domain, with users posting through private messages. These messages/conversations/data will all be held in the social media management tool for council employees to respond to queries etc.

There will be no outgoing data sent from the council using the social media management tool.

As users are willingly posting their messages to the public there is no GDPR related issues, and they will have to sign up to the terms and conditions of the social media site (Facebook, Twitter etc). This may be different for private messages, which will be treated differently.

As users are freely posting whatever messages they want, this does however present them the opportunity to post personal data either about themselves or about other people. This is something that cannot be prevented by any tool. If a user does post this in the public domain then they could be breaking the terms and conditions of the social media sites. However, it is more likely that these messages may be posted in private (121) messages. For instance a user might provide some personal details to make an enquiry about a council service via a Twitter direct message. This data would then be accessible in the social media management tool.

Any data that is provided by a user will be in relation to a council service and will be needed to complete a tasks/enquiry. For instance someone could be reporting a pothole through a Twitter direct message and provide their email address for feedback on when the pothole has been repaired. Any personal data would be provided by the choice of the users and not requested.

All incoming data to the social media management tool will follow the Digital Communications retention schedule- https://edrmlive/livelink/llisapi.dll/properties/86816716

Step 2 – Consultation Requirements

Identify whether internal and/or external consultation is required to address privacy risks

- Stakeholders to be consulted
- Method of consultation

Stakeholders consulted and involved from the inception of the project through the initial development of procurement specifications, through to the ongoing implementation include ICT services, ICT Security Tea, Procurement, Audit, Legal Services and representatives from departments throughout the council who currently use the existing social media management tool.

The Security Team will be consulted on the classification of any potential data.

As part of the Project Governance process, the Project Board consisting of the above stakeholders have identified and monitored risks through the project risk register.

Throughout the project key requirements will be made at every stage of procurement and implementation to ensure the solution is technically robust, protects any data and complies with the Council's existing standards e.g. ISO 27001 and Data Protection Act.

No further specific consultation will be required with departments who use the tool in relation to any privacy risks. They will however be consulted on the new Digital Communications retention schedule and their expectations around social media data.

Part B Steps 3 to 4 – Identify Privacy Risks, Solutions and Approval

Privacy Risk	Risk to Individuals & organisation	Risk initial score	Action Identified	Target Score (after applying actions)	Risk Control Plan (Treat/Control/Tolerate/Accept/Terminate/Transfer)	Evaluation: is the final impact on individuals and the organisation after implementing each solution a justified, compliant and proportionate response to the aims of the project?	Approved By
Personal information could be included within public and private social media message sent to DCC	Personal data could be stored in the solution	10	There is no way to prevent this type of incoming message, the likelihood of it happening is unlikely. All messages need to meet the retention schedules and disposal procedure as outlined in the Digital Communications retention schedule.	4	Control/Tolerate	Yes	
Inappropriate retention of date	Risk to the organisation of storing data longer	3	Ensure Digital Communication Retention schedule is adhered to.	2	Treat	Yes	

	than expected/agreed		Review data on a weekly basis to ensure that it has not exceeded retention period.				

Step four: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Implementation of Digital Communication Retention Schedule	November 2018	

Contact point for future privacy concerns
Date of consideration by IGG

Linking the PIA to the GDPR principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully

There must be lawful basis for processing the personal data as follows;

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) 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.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

- Have you identified the purpose of the project and which lawful basis applies? | Y
- Is the processing of the data necessary in terms of GDPR? | Y
- How will you tell individuals about the use of their personal data?

Terms and conditions of use of social media websites and solution.

- Do you need to amend your privacy notices? | N
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? |
- If special categories of personal data have been identified have the requirements of GDPR been met? | Y

As the Council subject to the Human Rights Act, you also will where privacy risk are especially high need to consider:

- Will your actions interfere with the right to privacy under Article 8? N
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data? Y
- Have you identified potential new purposes as the scope of the project expands? N
- Does your Privacy Notice cover all potential users? Y

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the quality of the information good enough for the purposes it is used? Y
- Which personal data could you not use, without compromising the needs of the project?

Personal data is only provided by users and not requested. So the solution could be used without personal data

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary? N
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

- What retention periods are suitable for the personal data you will be processing?

Retention periods for the solution will follow the Digital Communication Retention schedule

- Are you procuring software that will allow you to delete information in line with your retention periods? | Y

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under GDPR.

- Will the systems you are putting in place allow you to respond to subject access requests more easily? | Y
- Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten). | Y
- If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose? | Y

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Do any new systems provide protection against the security risks you have identified? | Y
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Training on the functionality of the system

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA? | N
- If you will be making transfers, how will you ensure that the data is adequately protected?