DERBYSHIRE County Council

Information Security Document

Privacy Impact Assessment

ICT-P3755 Email to SMS Solution

Version 1.0

Version History			
Version	**Date**	**Detail**	**Author**
[redacted]			

Privacy impact assessment screening questions

Will the project involve the collection of new information about individuals?
No.

Will the project compel individuals to provide information about themselves?
No

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
No

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
No

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.
No

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
Incoming SMS sent to specific keywords may result in the council departments offering business as usual services to sender. Decisions made by business as usual services may be communicated to individuals or 'mailing groups' via emails that the Solution converts to SMS for delivery to mobile phones

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
As the system will allow citizens to send text messages to the council and there is now way to prevent them sending any type of information, there is a possibility that this could occur. It does not appear to have been an issue with the current solution.

Will the project require you to contact individuals in ways that they may find intrusive?
No. Communication will be in response to a request from a member of the public for information or work related SMS may be sent to staff

Privacy impact assessment

The information flows

Outgoing Message:

1. DCC staff or software package send email to +44number.Derbyshire.textmail.org. Email content and retention defined by DCC policies.
2. Email goes to Fujitsu email server and is sent to Solution email sever.
3. Solution email server passes to Solution where it is converted to an SMS. A phrase/word e.g. Snow is added to the SMS to replace the originating email address and a copy saved in the reporting system.
4. The email is then sent to the recipients' phone number.
5. DCC staff take appropriate action based on the email content before deleting the message from the system. DCC has no control over what happens to messages sent to private phone numbers, however staff with access to SMS facility are well trained in Data Protection and non-disclosure of personal and or sensitive information and do not include this in outgoing emails.

Incoming Emails:

1. SMS to 86555 with no key word at the beginning of the message
    a. Sender sends message to 86555
    b. SMS received at Solution
    c. Solution checks for key word and when none found, converts the SMS into an email and sends the email to contact.centre@derbyshire.gov.uk
    d. Call Derbyshire staff with access to contact centre mailbox, review emails and forward to the appropriate team or individual mail box, before deleting the message.
    e. The team or individual process the incoming email according to their departmental processes. Where no person information is included, they phone the sender and follow due process from there. Where personal information is enclosed, the email is logged within the departments appropriate business software.
2. SMS to 86555 where first characters in the message are equal to an assigned key word.
    a. Message sent to 86555 with key word, e.g. Snow
    b. SMS received at Solution
    c. Solution checks if SMS to Short Code contains known key word.
    d. Solution processes according to key word and either
        i. Places SMS in key word box within Solution where it can be viewed with Staff members having user rights to access that box. SMS remain in the box until they are automatically deleted after 12 months.
        ii. Looks up the email address associated with the key word, converts the SMS to an email and forwards to the associated email address. Staff members having access to the email box, review the message and process according to their departmental standard procedures for the topic of the contents.
3. The Solution retains a copy of incoming and outgoing messages including the date and time of the message, originator, recipient and the message

itself for audit and verification purposes. This data can be accessed by staff with the appropriate user level of access.

Consultation requirements

Departmental staff will review their processes for handing incoming and outgoing SMS to ensure they fall in line with DCC other policies as part of the G-cloud scoping document review.
Departmental staff will review this document for accuracy of information.
Project team to review logs of incoming calls to identify type of information submitted.
The possible inclusion of personal data in incoming SMS to be added to the risk register.
The lack of control over content of incoming data will be added to the project risk register.

Limitation of staff with access to contact.centre@derbyshire.gov.uk to those who need it to be able to carry out their role.

Privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Personal information could be included within SMS sent to DCC			

Privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Members of the public may submit private and/or confidential/sensitive information about themselves or	Audit Services and ICT Security team will provide details of, and evaluate the responses to,	Risk is reduced once coming under DCC control, but the risk of inappropriate	The risk is lower than that of information added by member of the public to Twitter

others in the body of an SMS message. The messages will be stored on the solution providers systems which are outside the direct control of DCC	specific requirements for the solution supplier to meet in order to minimise the risk of the SMS being compromised whilst retained on the solution provider's servers. DCC will conduct due diligence during the procurement exercise to ensure that the Solution provides adequate security in the storage and transmission of these message as soon as they become DCCs responsibility	content in an SMS from a member of the public has to be accepted.	or Facebook where it would be instantly in the public domain. The business as usual processes will ensure that any personal, private or confidential information forwarded to them is dealt with appropriately.

Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
As above	As above	[redacted]

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

Contact point for future privacy concerns

Linking the PIA to the data protection principles

.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project? Yes

How will you tell individuals about the use of their personal data? N/A

Do you need to amend your privacy notices? N/A

Have you established which conditions for processing apply? Yes

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? N/A

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8? No

Have you identified the social need and aims of the project? The project will allow members of the public greater choice of how they contact, particularly where they do not own a smart phone or internet coverage is limited.

Are your actions a proportionate response to the social need? Yes

Principle 2

Personal data shall be obtained only for one or more specified 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? N/A

Have you identified potential new purposes as the scope of the project expands? N/A any new uses to the Solution will undergo their own PIA

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? Yes

Which personal data could you not use, without compromising the needs of the project? None

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/A

How are you ensuring that personal data obtained from individuals or other organisations is accurate? N/A – dealt with outside the project

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing? Message details sent to departments will be subject to the data retention period of that department. Copies of message saved on the solution for audit and verification purposes will be retained for 12 months.

Are you procuring software that will allow you to delete information in line with your retention periods?
It is intended that the Solution will do this automatically.

Principle 6

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

Will the systems you are putting in place allow you to respond to subject access requests more easily? N/A – any information from that requires retention will be stored on departmental systems.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose? N/A

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?
ISO27001 certification will be a requirement, as will Govt Cloud Security

What training and instructions are necessary to ensure that staff know how to operate a new system securely?
None specifically for the solution. Instructions for the sending any emails by DCC staff are detailed in the Information Safe Haven Guidance.

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?
No

If you will be making transfers, how will you ensure that the data is adequately protected?
Solution will be TLS v1.2 compliant