DERBYSHIRE County Council

Information Security Document

Privacy Impact Assessment Committee Management System

Version 0.7

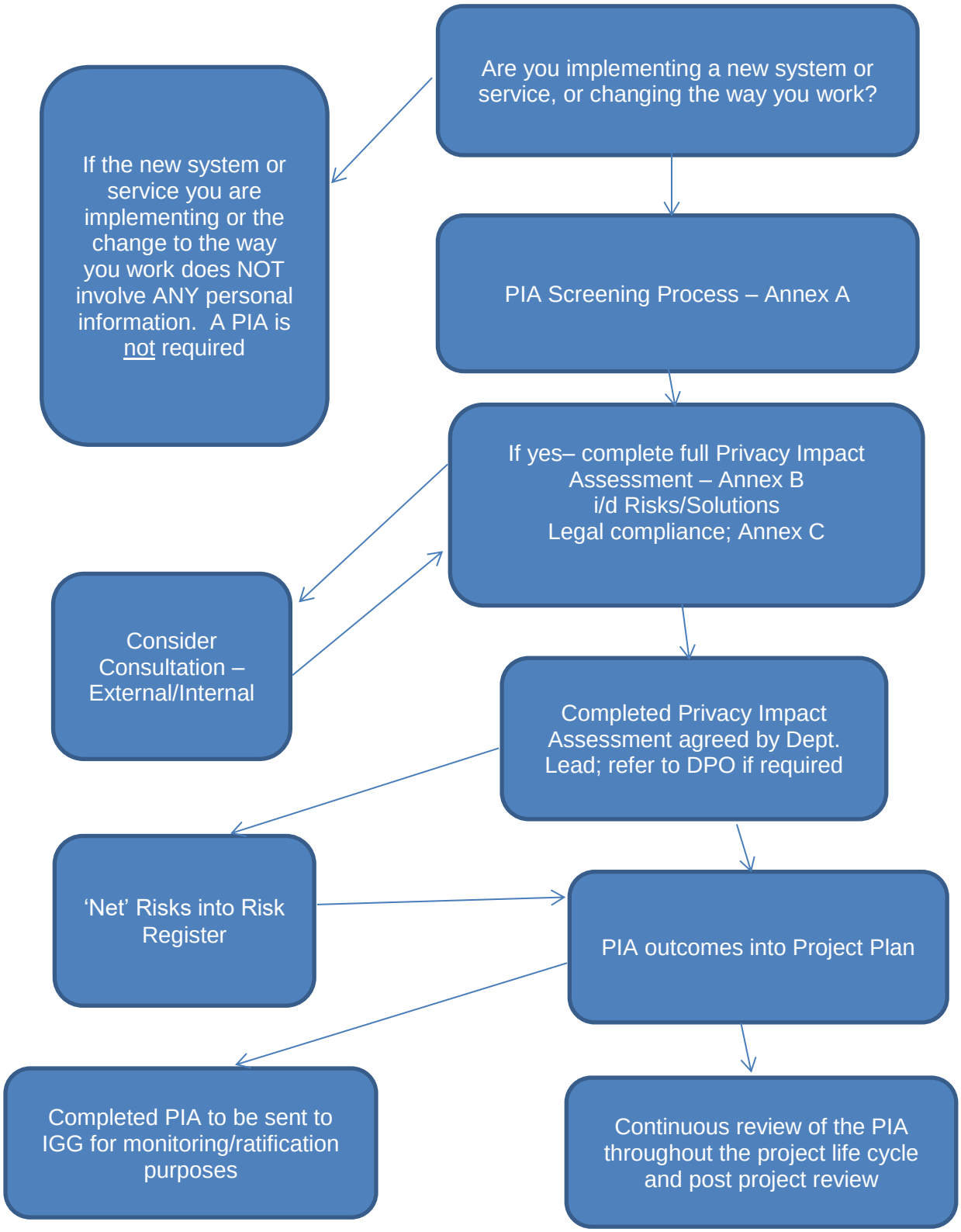
Version History			
Version	**Date**	**Detail**	**Author**
0.1	21/03/2018	Initial Draft	
0.2	28/03/2018	Review by	
0.3	05/04/2018	Review by	
0.4	17/04/2018	Added flow and further risks	
0.5	22/05/2018	Minor amendments to wording and added scores	
0.6	06/06/2018	Amendment made following review by	
0.7	06/06/2018	Reviewed by	

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.18.1.1	Identification of applicable legislation and contractual requirements
A.18.1.3	Protection of records
A.18.1.4	Privacy and Protection of personally identifiable information

Note: this policy will be revised to take account of the General Data Protection Regulations effective May 2018

Appendix 1

PRIVACY IMPACT ASSESSMENT PROCESS CHART



Appendix 2

Annex A - PIA Screening Questions

Question	Y/N	Additional Comments (optional)
Will the project involve the collection of new information about individuals?	N	No new information will be collected about individuals within the system itself. The system will be used as a database for forward plans, agenda items, meetings, reports for Democratic Services.
Will the project compel individuals to provide information about themselves?	N	The system does not require any personal data to be held within it, however sensitive data may be included in an exempt report. Individuals will not be required to give any personal information. Information may be contained with the Cabinet Reports, however this will be within the content of the report.
Will information about individuals be disclosed to third party organisations or people?	N	No personal information relating to individuals will be disclosed to any 3rd party organisations. However, the system will be hosted externally and procured using G-Cloud 9 so the system supplier will be hosting the data in their data centre which may be not their own. It's the information in the Council reports that may contain sensitive information especially if they are exempt reports and these will be hosted by the supplier.
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	Information will be collated and used as it is currently. The system will be used to collate and distribute Cabinet Reports/Cabinet member Reports, provide a public facing website so individuals can get the latest information on Cabinet dates, agendas and key decisions. Each Councillor could potentially have their own webpage with information about them, but this information is already in the public domain.
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 will be being used for this project. Members will be able to get to the information using tablets and other devices if needed. No technology will be used that might be perceived as intrusive. The system itself will be web based and permissions to access the system will be set accordingly.
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	N	The Committee Management System itself will not result in making decisions or taking action against individuals. But again, it may be that an exempt Cabinet Report could contain this type of information but this will be the content of the report written within DCC and not the system holding or creating this information.

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.	Y	The project and system procured should not raise any privacy concerns. Although the system will be hosted externally, security measures will be in place and due diligence will be undertaken with the highest scoring tenderer to cover any security or Audit concerns. Topics may be included in Cabinet Reports that people may consider to be private but this is content within a report created by DCC and not a privacy concern with the system itself. However, as there could potentially be sensitive information contained in an exempt Cabinet report for example, which is being hosted by the supplier, if there was a data breech then a privacy concern could be raised. This information could potentially be harmful to an individual or damaging to the Council.
Will the project require you to contact individuals in ways that they may find intrusive?	N	The project will not require individuals to be contacted that they may find intrusive. Members of the public and Councillors will have the opportunity to sign up to alerts and emails if they wish to get latest information on Cabinet dates, agendas etc., the same information that is currently available on the Councils website. They will also have the ability to unsubscribe from any mailing lists they sign up to.
Will the data be held in relation to children or vulnerable adults?	Y	There is the potential for data to be held in relation to children or vulnerable adults or any demographic. Documentation in the form of committee reports and committee minutes may hold confidential and/or personal information. This information included in the report would be classed as exempt.

Annex B Step 1 – Requirement for PIA – issues to be addressed

Project Aim and Objectives

Democratic Services are currently reliant upon manual processes for the administration, framework and decision making process. Currently, committee paper bundles are photocopied for around 50 individuals and once photocopied, Democratic Services staff manually sort and band the bundles ready for distribution. The committee papers are then added to the Council's website via Democratic Services staff using the web content management system, Tridian. If the paper is exempt then this is published to a secure part of the site. These bundles are then created as an electronic copy and emailed to elected members.
The department recognises the need to modernise the existing arrangements to enable a more effective and efficient way of working and also bring about further transparency to the Council's decision making process. Democratic Services are therefore looking to procure a committee management system to streamline these various tasks involved in the democratic process (production of agendas, publication of papers on the website, electronic sets of papers, decision digests, key decisions etc.).

Benefits to the organisation, to individuals and to other parties

The Council is looking to procure a new Committee Management Solution to be utilised by Democratic services to modernise and streamline current processes and bring about greater transparency to the democratic process and key decisions made by the Council. This should help avoid any duplication, manual processes that are already in place and in term potentially make saving in staff time and resources.
The Council also wishes to move forward in its aspirations for paperless meetings by utilising software and mobile technology to automatically create agendas, meeting minutes, key decisions and distribute these to Members mobile devices. Using this approach to achieve paperless meetings will lead to cost savings in staff time, stationary and postage costs.
There will also be benefits to the public experience as the documents that will be published on the Council's website for viewing will be displayed in a more customer friendly layout with more information readily available containing options for searching on previous committees and looking for future committees through a calendar style layout.

Links to any relevant project documentation

Outline Business Need - Committee Management System
https://edrmlive/livelink/llisapi.dll/properties/84636137

Options Appraisal - Committee Management System.docx
https://edrmlive/livelink/llisapi.dll/properties/84624629

Outline Specification - Committee Management System.docx
https://edrmlive/livelink/llisapi.dll/properties/84636250

PROCUREMENT OF A COMMITTEE MANAGEMENT SYSTEM - Included Paul Peat comments 16 March.docx
https://edrmlive/livelink/llisapi.dll/properties/85243861

Summary of Identified Need for PIA (can draw on answers to the screening questions).

Although only two of the screening questions answered 'Yes' (detailed below) it is felt that there is still a requirement to complete a PIA due to potentially sensitive/restricted information contained in a Committee Report being hosted externally.

- Will the project result in you making decisions or taking action against 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.

- Will the data be held in relation to children or vulnerable adults?

On the 11th October 2016, cabinet approved the use of the Crown Commercial Services, G-Cloud Framework ('the Framework') to procure low value/low risk externally hosted solutions.

Annex B Step 2 – Information Flows

To Include:

- Description of collection, use, retention and deletion of personal data
- 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

A Committee Management System will allow Members, Council Officers and the public, controlled and secure access to published information such as Committee Meeting agendas, key decisions, forward plans and a calendar of up-coming meeting, giving user's details on a wide variety of topics. The Committee Management System will also be able to collect information such as, members or Councillor's political affiliations, attendance at council meetings and register of interests.

The solution will allow all interested parties to review, comment and interact directly on plans and decisions. By subscribing to e-mail notification services, members of the public can participate and respond to forthcoming consultations and decisions.

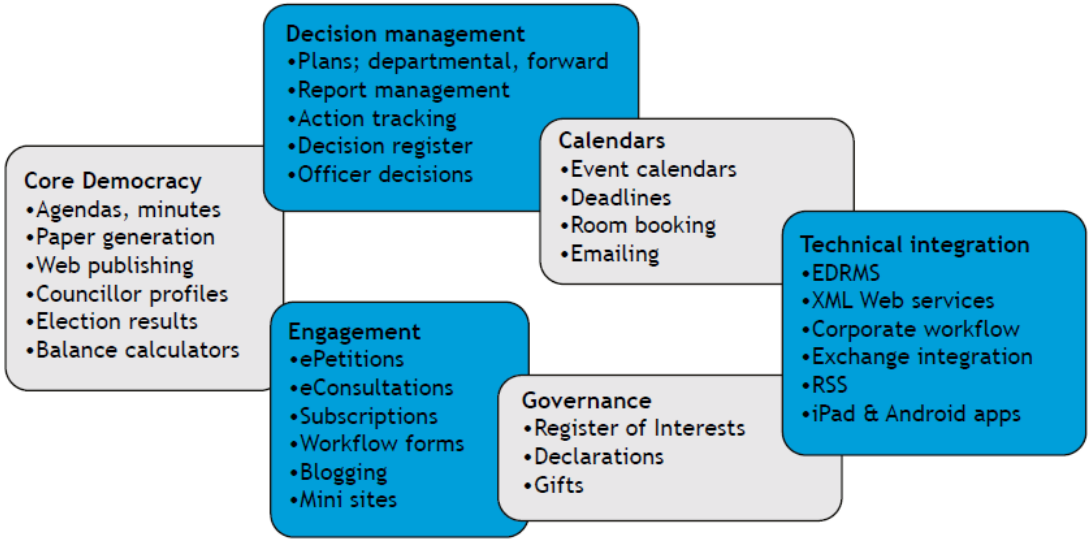
The solution can record every (selected) committee year on year, to form a historical archive of the Council's decisions and published information. Online facilities allow public access to all details from past meetings, as well as daily updates of future meetings.

Data will be retained in line with the Councils Data Retention Policy.

Reports and agendas will be assembled within the solution by Democratic Services staff, including the creation of front sheets and subsequent minutes. Late reports can also be added. From these induvial set of reports and documents, automatically generated document packs can be produced as a single PDF that includes a front sheet of agenda items, running page numbers and headers. Restrictions can also be applied to the document pack for restricted documents and exempt items. These document packs can then be emailed and made available online for members and the public (dependent on restrictions) to view. Members will also have the opportunity to use a mobile app (if purchased) to gain access to the document packs from their own devices to allow them to make notes and annotate the reports if required.

People who will be affected by this project will be Democratic Services staff who will be responsible for the creation of the document packs and pulling together the agendas, reports and minutes and ensure that these are made available online for both council officers and members of the public. Council Members who will be receiving the document packs in preparation for Committee meetings either by an

email link to the pack or via the mobile app. Members of the public who will be able to gain access to the committee agendas and reports via the website or again accessible via a mobile app.



Annex B Step 2 – Consultation Requirements

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

- Stakeholders to be consulted
- Method of consultation

A project team has been established that includes individuals from the Business (Democratic Services), Commissioning, Projects, Web development team and Audit and Security. The team will feed into the PIA and the requirements for the project.
As this will be a G-Cloud procurement, the project team will be responsible for managing the risks throughout the procurement and implementation phase of the project. The team will undertake a shortlisting exercise using G-Cloud to ensure that suppliers that will go through to the evaluation stage will meet the requirements of the Council both in terms of security and audit. Once the highest scoring tenderer has been identified a further due diligence process will be undertaken which will include a supplier demonstration to the project team.
Communication will be done via face to face project team meetings and email. The group will ensure regular communication is achieved to progress the project forward and the project manager will produce regular Highlight Reports of progress. All procurement communication with the supplier will be done via the Commissioning lead so an audit trail is maintained.

Part B Steps 3 to 5 – 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
Sensitive information contained in exempt Cabinet Report will be hosted by the Cloud Supplier. There is a potential risk of a data breech	Information contained with exempt reports could contain information relating to section 36 (conduct of public affairs), section 41 (information obtained in confidence), section 40 (personal information) and section 43 (commercial	12	Using the G-Cloud 9 framework, the suppliers listed have already been vetted and must show a level of security and governance in order to be on the framework	8	Treat/Control	Yes	

	interests) under the FOI exemptions.						
Human error – when using the system an exempt report may be publishe d to the public by mistake causing damagin g informati on either to the Council or an individua l to be in the public domain	If data is published to the web that contains sensitive or personal information including financial information for the Council this will incur ICO fines and also damage the Councils reputation.	12	Ensure that relevant system training is undertaken and that staff are aware of the importance of data protection and privacy issues. Ensure that a checking and screening process is in place and sign off has been sought before anything is published online.	6	Treat/Control	Yes	

Inappropriate retention of the data	The supplier will be required to hold information in line with the Councils retention policies and required to delete the data that is no longer required. If this is not done that data may be held in the report about an individual without their knowledge or consent. This would be in breach of the GDPR regulations.	6	Data sharing instructions set out timescales for the retention and destruction of data and conform to the data protection principles that data must not be kept for longer than necessary. The supplier will be required to retain data as per the Councils retention policies and destroy the data that is no longer required.	4	Treat/Control	Yes	
Passive data breech involving	As a result of a force majeure data may be lost	2	Cloud providers usually implement several capabilities to	1	Tolerate/Accept	Yes	

data breech due to natural (fire/earthquakes, flood) and/or man-made (terrorism) disasters.	or be subject to a data breach. This would be out of the Suppliers or the Councils control, however there could be mitigations put in place within the contract to reduce any foreseeable losses and to take reasonable steps to prevent or limit the loss.		Reduce the risk of data loss. This could be the use of separate data centres around the UK or the EU or having a robust disaster recovery programme				

Step five: 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
Data Breach Human Error Inappropriate Retention Passive Data Breach		

Step six: 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
Integrate PIA outcomes back into the project plan Update and monitor PIA throughout the project	Aug 2018 On-going	Project Manager

Contact point for future privacy concerns
Date of ratification by IGG

Annex C

Linking the PIA to the data protection 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 DPA or other relevant legislation, for example the Human Rights Act.

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?

Do you need to amend your privacy notices? NO

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? NO

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? YES

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? YES

Have you identified potential new purposes as the scope of the project expands? NO

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?

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? YES

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

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?

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

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? YES

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? YES

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

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?

If you will be making transfers, how will you ensure that the data is adequately protected?

Conditions for processing under the Data Protection Act can be found at;

https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/