Belton Parish Council

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	Belton Parish Council
Subject/title of DPO	Parish Clerk and RFO
Name of controller contact /DPO (delete as appropriate)	Clare Boyall

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
This Data Protection Impact Assessment (DPIA) is designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible as well as demonstrating compliance with GDPR in order to avoid sanctions. It will also inspire confidence in the public by improving communication about Data Protection Issues, and makes sure users are not at risk of their data protection rights being violated.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Processing means taking any action with someone's Personal Data e.g. Name, Address, Photographs, Medical Information. This begins when a data controller starts making a record of information about someone and continues until you no longer need the information and it's been securely destroyed. If you hold information on someone, it counts as processing even if you don't do anything else with it. Other types of data processing include actions such as organising and restructuring the way you save the data, making changes to it e.g. Updating someone's address or record and sharing it or passing it to others. (Taken from The Information Commissioner's Office (ICO) under section for Advice to small organisations.

Councillor contact details including name, address, telephone numbers and email addresses stored on the council's laptop. These details are added and deleted as part of the election and resignation process.

Staff name, address and contact details are stored on the council's laptop.

Members of the public names and email addresses who contact the Parish Council. These are only kept for as long as necessary and then deleted. These details are only shared with Councillors if the member of the public has given consent.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Name and address email and phone numbers of the councillors plus Parish Clerk are stored on a single laptop. The Parish Clerk manages access through the administration of the Microsoft account and IT provider. There are no special categories or criminal offence data stored of the Parish Councillors. Details of other members of the public are stored during correspondence and are deleted when query has been completed. Details updated or deleted as appropriate following elections or resignations. Area is within three miles from the parish boundary but on occasion enquiries are received from members of the public outside of this geographical area but are treated in the same way as any other correspondence and only kept until the query has been completed.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Councillors are elected onto the Parish Council. When elected they are given the option on whether they wish their contact details to be displayed on the website. The Council has a Code of Conduct adopted and provided to all Cllrs when they join the council. A copy is also available on the council's website. Children are not involved in the Parish Council. The Clerk works from a single laptop provided by the council for work purposes only. This is password protected and backed up. Only the Clerk can gain access to the council's email account. Personal contact details of residents are not kept once an enquiry has been completed.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Councillor information is used to communicate with them for the normal business of the council. Residents contact the council with queries and expect an answer.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Residents contact the council from time to time with queries or requesting information. The vast majority of contact is by email to the council and rarely by letter. All correspondence is either deleted from emails or shredded when it is no longer relevant or the matter has been dealt with. At the present time the council does not ask for surveys or use questionnaires to seek residents views.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Data quality and data minimisation is ensured as only relevant information is collected from the Parish Councillors and retained only for as long as is necessary or for the period they stand as a Councillor, if they resign data is removed/deleted immediately. Financial information will be retained for the relevant period required. Data relating to other persons such as residents is not retained and any relevant information held in line with the Document Retention policy Personal information relating to staff is held for the purposes required by the employer.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Data breach of personal information for councillors, Clerk or members of the public.	Remote,	Minimal,	Low,

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Loss of councillors, staff or residents personal information	All data is password protected. Paper documentation is stored securely and only kept as long as it is relevant.	reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Parish Councils do not need a Data Protection Officer as they are not public authorities for the purpose of GDPR. ICO annual subscription in place.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA