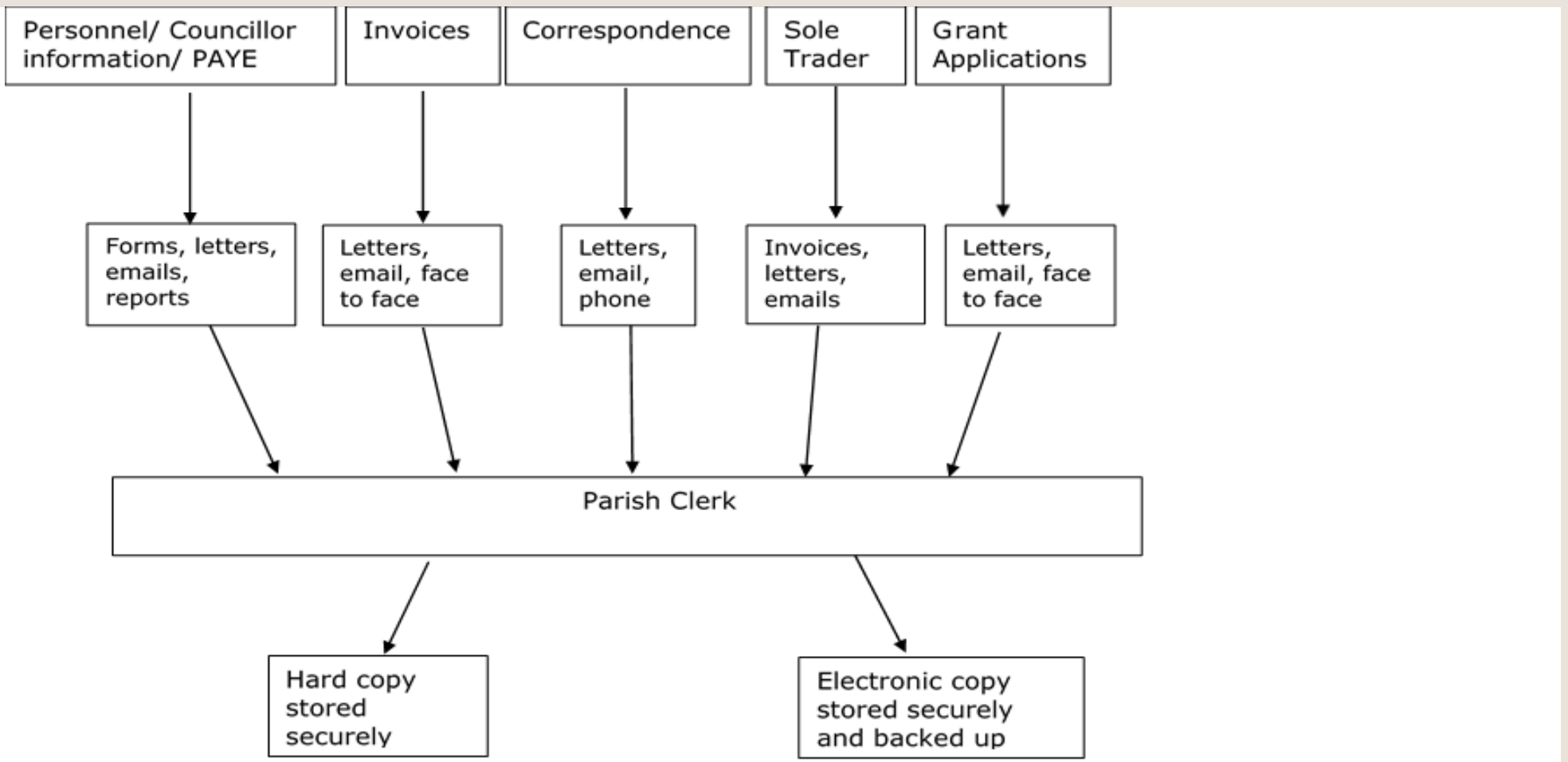
Great Ness And Little Ness Parish Council Data Protection Impact Assessment

Step one: Identify the need for a DPIA

The following is a list of data this parish council processes and controls to run the council:

- Employees' information including personnel and payroll information
- Records of current councillors' information
- Invoices
- Sole traders
- General correspondence, mostly email.
- Donations (grant) - groups.

Step two: Describe the information flows



Step three: Identify the privacy and related risks

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Holding unnecessary and out of date personal information. • Personal information on current and previous Clerk and other applications for the post. • Bank mandates. Councillor bank passwords. • Previous councillor's declarations. • Bank details on invoices for sole trader • Correspondence held by councillors where personal data is stored. • Archive Filing in village hall.	Data subjects at increased risk of their data being breached	Does not comply with the main principles of GDPR	Damage to reputation and possible fine if breach occurs.
Storage of personal data in an insecure location.	Could lead to unauthorised access	GDPR states all data should be kept securely.	Damage to reputation and possible fine if breach occurs

	of personal information.		
Lack of secondary security measures for documents held on computer	Could lead to unauthorised access of personal information.	GDPR states all data should be kept securely.	Damage to reputation and possible fine if breach occurs.
Lack of retention policy	Data may be kept for longer than needed and therefore increase risk of breach.	GDPR states data controllers must have a clear, transparent retention policy.	Damage to reputation and possible fine if breach occurs.
Lack of privacy policy	Without a privacy policy data subjects will not know or accept how their data is being processed.	GDPR states data controllers must have a clear, transparent privacy policy	Damage to reputation and possible fine if breach occurs.
Lack of cookie policy	Without a cookie policy the data subject does not know how their data is being processed	GDPR states data controllers must be transparent in their data processing	Damage to reputation and possible fine if breach occurs.

Step four: Identify privacy solutions

Risk	Solution(s)	Result: is the risk eliminated, reduced, or accepted?	Evaluation:
Holding outdated data	Destroy any outdated documents in accordance with retention policy	Eliminate	Shredding outdated data is an essential part of compliance.
Storage of Personal data in an insecure location.	All hard copy documents containing personal data should be held in secure storage. These include personnel records. Councillor details not in the public domain. Grant applications. Documentation containing personal information in archive filing in the village hall. Where possible personal information should be redacted. This would include, NI numbers on pay slips and bank details of sole traders.	Reduce	This solution is an effectively way to reduce the risk.
Lack of secondary security measures for documents with personal data	Use password protect on electronic documents and secure by encryption.	Reduce	Very effective way to secure files and ensure compliance

Lack of retention policy	Implement a retention policy. This will help prove transparency.	Eliminate	Solution is a justified way of ensuring compliance.
Lack of privacy policy.	Privacy policies should become part of the fabric of processing data. Privacy Policies must form part of all processes containing personal data.	Eliminate	Solution is a justified way of ensuring compliance.
Lack of Cookie policy	Cookie policy to detail cookies used and what they do. Must have opt in facility.	Eliminate	Solution is a justified way of ensuring compliance.

Step five: Sign off and record the PIA outcomes

Risk	Approved solution	Approved by signature
Holding outdated data	Destroy any outdated documents in accordance with retention policy	Clerk: Chairman
Storage of personal data in secure location	Store hard copy documents in a secure cabinet. Redact all unnecessary information	Clerk: Chairman:
Lack of secondary security measures for documents with personal data.	Use password protect and encryption on documents containing data.	Clerk: Chairman:
Lack of retention policy	Introduce retention policy.	Clerk: Chairman:
Lack of privacy policy	Introduce privacy policies where necessary.	Clerk: Chairman:
Lack of Cookie policy	Incorporate opt in cookie policy on website	Clerk: Chairman:

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

Action to be taken	Date for completion of actions	Responsibility for action
Destroy any outdated documents in accordance with retention policy		Clerk
Secure storage of personal data.		Clerk

Redaction where necessary		
Use password protect and encrypt.		Clerk
Updated retention policy with data audit, this will now be implemented.		Clerk
Updated privacy policy with data audit, this will now be implemented.		Clerk
Cookie policy		Clerk

Contact point for future privacy concerns
Peter Malley: peter@dmpayrollservices.co.uk