

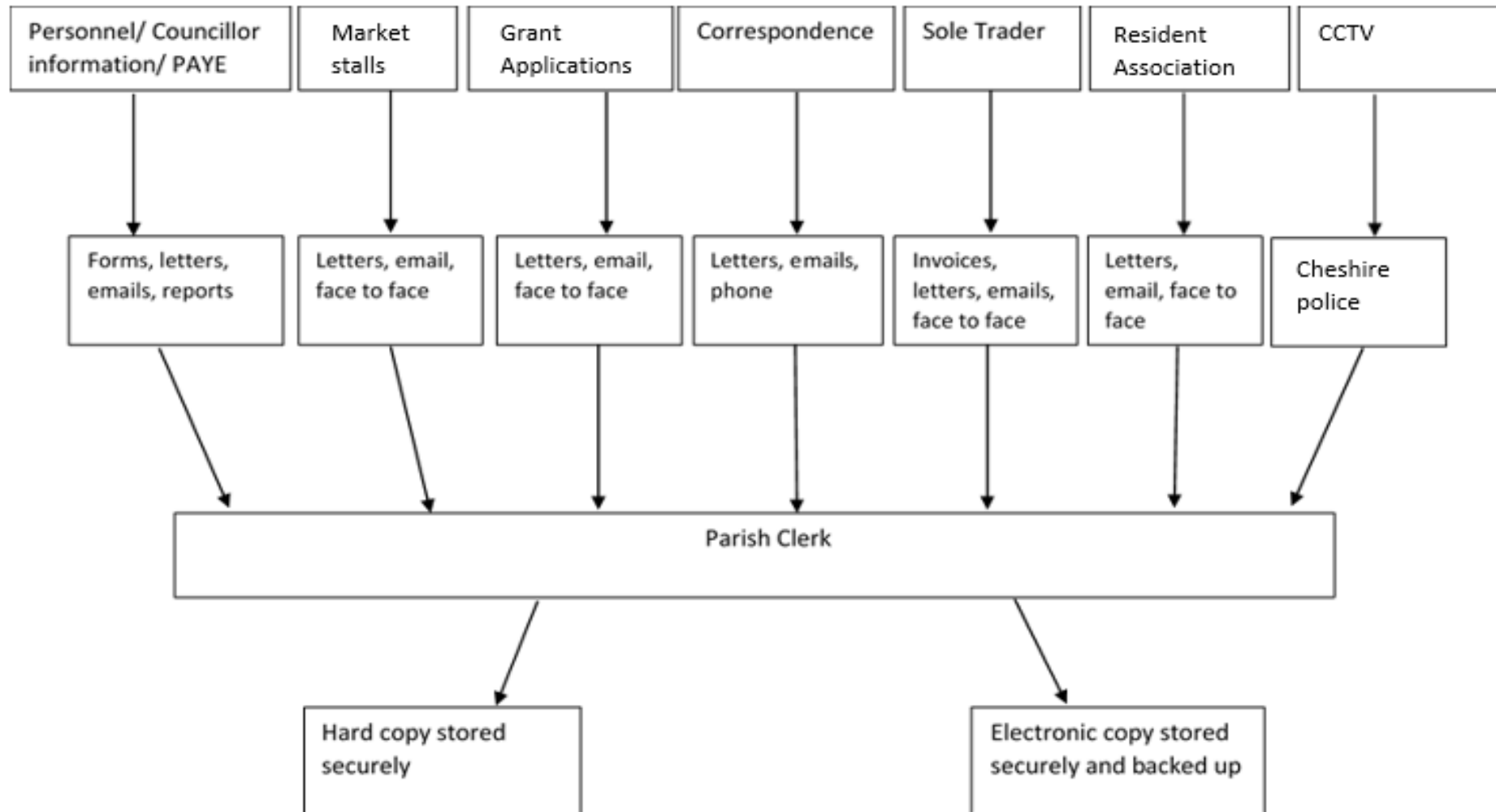
Handforth Parish Council Data Protection Impact Assessment

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.
- Market stalls- Christmas.
- Grant application
- Residents association group.
- CCTV

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
<p>Holding Personal data where there is no legitimate right for it to be held or stored. This includes:</p> <ul style="list-style-type: none"> • Previous clerk's and applicant's details • Proof of eligibility • Planning applications 	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.
Holding full copies of documents which contains personal information.	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.
Documents containing personal data must be kept secure.	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 secondary security measures for data held electronically.	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.
Councillors using personal email for council use.	No assurance that data is secure.	GDPR states all data should be kept securely.	Damage to reputation and possible fine if breach occurs.
Back up more frequently and ensure its stored securely.	Could lead to loss of data if not done.	The backup must be stored securely to prevent risk of loss.	Damage to reputation and possible fine if breach occurs.

Lack of digital shredder	Data will not be destroyed electronically and, therefore increasing the risk.	GDPR states only minimal data should be held.	Damage to reputation and possible fine if breach occurs.
Lack of consent to hold councillor's and clerk's details on website.	Clerk and councillor's information is easily found and could be exploited.	GDPR states gaining explicit consent from data subjects is essential.	Damage to reputation and possible fine if breach occurs.
Update CCTV policy	Ensure data subjects are fully protected	A CCTV policy is essential to reduce risk and ensure compliance.	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 how their data is processed	GDPR states data controllers must have a clear, transparent privacy policy	Damage to reputation and possible fine if breach occurs.
To consult with DPO for any future processes	To ensure the risk to the individual is as minimal as possible.	To ensure the future processes are compliant with GDPR	Damage to reputation and possible fine if breach occurs.

Step four: Identify privacy solutions

Risk	Solution(s)	Result: eliminated, reduced, or accepted?	Evaluation:
<p>Holding Personal data where there is no legitimate right for it to be held or stored. This includes:</p> <ul style="list-style-type: none"> • Previous clerk's and applicant's details • Proof of eligibility • Planning applications 	<p>Destroy any outdated documents in accordance with retention policy</p>	<p>Eliminate</p>	<p>Destroying outdated and unnecessary data is an essential part of compliance.</p>
<p>Holding full copies of documents which contains personal information.</p>	<p>Redact personal details off the following documents whilst they are being held in accordance to retention policy:</p> <ul style="list-style-type: none"> • Signature off declaration of interest copy. • Bank details off sole trader invoices • Signature off grant applications 	<p>Reduce</p>	<p>This solution is an effective way to reduce the risk.</p>
<p>Documents containing personal data must be kept secure.</p>	<p>Keep documents holding personal information secure.</p>	<p>Reduce</p>	<p>Effective way to secure files and ensure compliance</p>

Lack of secondary security measures for data held electronically.	Use password protect on electronic documents and encrypt personal data	Reduce	Effective way to secure files and ensure compliance
Councillors using personal email for council use.	DPO has advised councillors to have their own councillor specific email	Reduce	Solution is protecting councillors from have their personal being searched following an access request.
Back up more frequently and ensure its stored securely.	When not in use remove hard drive and store in a secure location. Back up daily.	Reduce	Effective way of reducing risk.
Lack of digital shredder	Download digital shredder, destroy any documents in accordance to retention policy	Reduce	Destroying outdated and unnecessary data is an essential part of compliance.
Lack of consent to hold councillor's and clerk's details on website.	Ask councillors for consent to have personal details in the public domain. Clerk also needs to give consent.	Eliminate	Explicit consent is an essential part of compliance.
Update CCTV policy	CCTV policy must adhere to all relevant law and legal process, these include: <ul style="list-style-type: none"> • Justified reason for use • Signage displaying its use • Trained staff to use recording equipment, to be 	Eliminate	Solution is a justified way of ensuring compliance.

	<p>responsible for the storage and dissemination of the data.</p> <ul style="list-style-type: none"> Equipment that can isolate other data subjects if an information request is made 		
Lack of retention policy	Introduce retention policy.	Eliminate	Solution is a justified way of ensuring compliance.
Lack of privacy policy	<p>Introduce privacy policy. To be used in all data processes and be available on your website. This includes:</p> <ul style="list-style-type: none"> Market stall list Grant applications Correspondence 	Eliminate	Solution is a justified way of ensuring compliance.
To consult with DPO for any future processes	To consult with DPO for any future processes.	Reduce	Gaining professional advice will guide council to conform to GDPR.

Step five: Sign off and record the PIA outcomes

Risk	Approved solution	Approved by signature
<p>Holding Personal data where there is no legitimate right for it to be held or stored. This includes:</p> <ul style="list-style-type: none"> • Previous clerk's and applicant's details • Proof of eligibility • Planning applications 	<p>Destroy any outdated documents in accordance with retention policy</p>	<p>Clerk: Chairman:</p>
<p>Holding full copies of documents which contains personal information.</p>	<p>Redact personal details off the following documents whilst they are being held in accordance to retention policy:</p> <ul style="list-style-type: none"> • Signature off declaration of interest copy. • Bank details off sole trader invoices • Signature off grant applications 	<p>Clerk: Chairman:</p>
<p>Documents containing personal data must be kept secure.</p>	<p>Keep documents holding personal information secure.</p>	<p>Clerk: Chairman:</p>
<p>Lack of secondary security measures for data held electronically.</p>	<p>Use password protect on electronic documents and encrypt personal data</p>	<p>Clerk: Chairman:</p>
<p>Councillors using personal email for council use.</p>	<p>DPO has advised councillors to have their own councillor specific email</p>	<p>Clerk: Chairman:</p>
<p>Back up more frequently and ensure its stored securely.</p>	<p>When not in use remove hard drive and store in a secure location. Back up daily.</p>	<p>Clerk: Chairman:</p>
<p>Lack of digital shredder</p>	<p>Download digital shredder, destroy any documents in accordance to retention policy</p>	<p>Clerk: Chairman:</p>
<p>Lack of consent to hold councillor's and clerk's details on website.</p>	<p>Ask councillors for consent to have personal details in the public domain. Clerk also needs to give consent.</p>	<p>Clerk: Chairman:</p>

Update CCTV policy	<p>CCTV policy must adhere to all relevant law and legal process, these include:</p> <ul style="list-style-type: none"> • Justified reason for use • Signage displaying its use • Trained staff to use recording equipment, to be responsible for the storage and dissemination of the data. • Equipment that can isolate other data subjects if an information request is made 	<p>Clerk:</p> <p>Chairman:</p>
Lack of retention policy	Introduce retention policy.	<p>Clerk:</p> <p>Chairman:</p>
Lack of privacy policy	<p>Introduce privacy policy. To be used in all data processes and be available on your website. This includes:</p> <ul style="list-style-type: none"> • Market stall list • Grant applications • Correspondence 	<p>Clerk:</p> <p>Chairman:</p>
To consult with DPO for any future processes	To consult with DPO for any future processes.	<p>Clerk:</p> <p>Chairman:</p>

Step six: Integrate the DPIA 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
<p>Redact personal details off the following documents whilst they are being held in accordance to retention policy:</p> <ul style="list-style-type: none"> • Signature off declaration of interest copy. 		Clerk

<ul style="list-style-type: none"> • Bank details off sole trader invoices • Signature off grant applications 		
Keep documents holding personal information secure.		Clerk
Use password protect on electronic documents and encrypt personal data		Clerk
DPO has advised councillors to have their own councillor specific email		Clerk
When not in use remove hard drive and store in a secure location. Back up daily.		Clerk
Download digital shredder, destroy any documents in accordance to retention policy		Clerk
Ask councillors for consent to have personal details in the public domain. Clerk also needs to give consent.		Clerk
<p>CCTV policy must adhere to all relevant law and legal process, these include:</p> <ul style="list-style-type: none"> • Justified reason for use • Signage displaying its use • Trained staff to use recording equipment, to be responsible for the storage and dissemination of the data. • Equipment that can isolate other data subjects if an information request is made 		Clerk
Introduce retention policy.		Clerk
<p>Introduce privacy policy. To be used in all data processes and be available on your website. This includes:</p> <ul style="list-style-type: none"> • Market stall list 		Clerk

- Grant applications
- Correspondence

To consult with DPO for any future processes.

Clerk

Contact point for future privacy concerns

Ben Malley: ben@dmpayrollservices.co.uk