

Hacheston Parish Council Financial Risk Assessment

Topic	Risk Identified	Risk Level H/M/L	Management of Risk	Staff action
Precept	Not submitted	L	Full Minute – RFO follow up	Diary
	Not paid by DC	L	Confirm receipt	Diary
	Adequacy of precept	H	Conduct a review of spending at each full Council meeting	Agenda
Other Income	Cash handling	M	Cash handling is avoided, but where necessary appropriate controls are in place	Annual review of documented controls
	Cash banking	M	Clerk to bank cheques promptly and conduct regular checks of bank statements. Produce bank reconciliations for every full Council meeting.	Examining Officer to verify reconciliations at meetings.
Grants	Claims procedure	M	Clerk/RFO check as required	Diary
	Receipt of grant when due	M	Clerk/RFO check as required	Diary

Salaries	Wrong salary/hours/rate paid	M	SALC carry out Payroll, at Council's agreed rate as per clerk's contract.	Clerk and Council to check SALC's payroll sheet before paying clerk.
	Council not meeting legislative requirements re workplace pensions	M	Confirm that Pensions Regulator's requirements being met. As payroll officials, SALC should advise of obligations in this regard.	Keep confirmatory letter Pensions Regulator on file
Payments	Goods not supplied to Council	M	Follow up on all orders	Approval check
	Invoice incorrectly calculated or recorded	M	Check arithmetic on invoices and perform bank reconciliations on regular basis	Member to verify
	Cheque payable is incorrect or made to wrong party	M	List of Payments agreed by Council and signed by 2 signatories. Cheque counterfoils initialled and compared to invoice/voucher. Payments are listed in Council's Minutes. Online payments authorised by two mandates.	Approval check at meetings
Online Banking			The clerk will access internet banking sites directly and not via a search engine. The clerk only has ability to view the accounts and transfer money, not to make any payments or withdrawals.	Bank reconciliations are checked at meetings Another Councillor also has online banking access to view the accounts at any point.

Election Costs	Invoice at local authority's agreed rate	L	RFO check and consider budgeting for contested election over several years	RFO verify
VAT	VAT analysis	M	All VAT to be separated in Receipts and Payments sheet	RFO verify
	Claimed within time limits	M	Clerk to submit at least annually and report back to council at full meeting, including confirming receipt of reclaimed VAT.	RFO verify

Reserves – General	Adequacy	L	Consider at Budget setting & monitor balances at each full Council meeting	RFO opinion.
Reserves – Earmarked	Adequacy	L	Consider at Budget and review of final accounts	Council to review regularly
Assets	Loss, Damage etc	M	Annual inspection, update insurance and asset registers as necessary. Compare insurance schedules with Asset Register	Agenda
	Risk or damage to third party property or individuals	M	Review adequacy of Public Liability Insurance	Diary
Staff	Loss of Clerk	L	Hours, health, stress, training, long term sick, early departure – risk monitored and managed as appropriate	Clerk to raise concerns with Council as appropriate. Consider conducting an annual appraisal.
	Fraud by staff/members	L	Fidelity Guarantee value appropriately set. Accounting is transparent and always available for Councillors to view.	Council to review annually or more frequently if concerns.
Legal Powers	Illegal activity or payment	H	Councillors and staff receive relevant training as to their legal powers	Diary
Financial Records	Inadequate records	L	RFO/clerk check regularly + internal audit review	Figures checked at meetings & signed by Examining Officer
Minutes	Accurate and legal	L	Review at following meeting	Agenda
Members' interests	Conflict of interest	M	Declarations of interest to be Minuted and any conflict addressed as appropriate	Agenda
Council records-electronic	Loss through: fire, theft, corruption of PC , Data falls into the hands of a third party,	L	Council's electronic records are stored on the Clerks computer. Back-ups of the files are taken at regular intervals and stored on a USB in a metal filing cabinet. Computer is password protected. Wipe the hard drives from computers, laptops and printers or destroy them before disposing of the device.	Existing procedure adequate

Data Protection	Financial loss following a data breach as a result of prosecution or fines, GDPR/PECR breach	M	<p>The Parish Council is registered with the Information Commissioner's Office and has a Data Protection Policy. Data breaches to be reported to the Council and ICO within 72 hours.</p> <p>Ensure that the council has liability cover which specifically covers prosecutions resulting from a data breach</p> <p>Use blind copy (bcc) to send group emails to people outside the council</p> <p>Use encryption for emails that contain personal information</p> <p>Delete emails from members of public when query has been dealt with and there is no need to keep it</p> <p>Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publically</p> <p>Password protect personal and sensitive information folders and databases.</p>	<p>Check registration and annual renewal. Data Protection Policy to be reviewed annually.</p> <p>Annually</p> <p>Regularly</p> <p>Councillors to ensure their own PC/tablets/laptops are password protected.</p>

Signed

.....
Chair

.....
Date