Internal Audit 2022/23

Interim Report

The internal audit of Frodsham Town Council is carried out by undertaking the following tests as specified in the AGAR Annual Return for Local Councils in England:

- Checking that books of account have been properly kept throughout the year
- Checking a sample of payments to ensure that the Council's financial regulations have been met, payments are supported by invoices, expenditure is approved, and VAT is correctly accounted for
- Reviewing the Council's risk assessment and ensuring that adequate arrangements are in place to manage all identified risks
- Verifying that the annual precept request is the result of a proper budgetary process; that budget progress has been regularly monitored and that the council's reserves are appropriate
- Checking income records to ensure that the correct price has been charged, income has been received, recorded and promptly banked and VAT is correctly accounted for
- Reviewing petty cash records to ensure payments are supported by receipts, expenditure is approved and VAT is correctly accounted for
- Checking that salaries to employees have been paid in accordance with Council approvals and that PAYE and NI requirements have been properly applied
- Checking the accuracy of the asset and investments registers
- Testing the accuracy and timeliness of periodic and year-end bank account reconciliation(s)
- Year end testing on the accuracy and completeness of the financial statements

The interim internal audit provides evidence to support the annual internal audit conclusion in the AGAR Annual Return for larger councils.

Conclusion
On the basis of the internal audit work carried out, in our view the council's system of internal controls is in place, adequate for the purpose intended and effective, subject to the issues reported in the action plan overleaf.

As part of the internal audit work for the next financial year we will follow up all recommendations included in the action plan.

JDH Business Services Limited

ACTION PLAN

	ISSUE	RECOMMENDATION	FOLLOW UP
1	The Council have been the victim of a supplier fraud in 2022/23. The incident has been reported to the Police and Action Fraud and is currently under investigation. The fraud appears to have occurred following a hacking of the Clerk's email account and the setup of rules diverting emails from a supplier to the RSS feeds folder. This resulted in the original emails from the supplier not being viewed by the Clerk. Emails were then sent to the Clerk from a fraudulent email address with doctored invoices showing the details of the fraudster's bank account, notifying the Council that the bank account details had changed. A handwritten note on the invoice paid states the clerk queried the account number but does not state whether this was queried by telephone or email and the source of the contact information used. The IT provider has changed the passwords on the account following notification of the fraud. We have not been informed whether examination of the Clerk's laptop has taken place in order to identify how the email account was hacked and whether the laptop is free of malware or viruses	*Changes to supplier bank details must be followed up with a phone call using* ***current*** *contact information rather than those on an email or invoice purported to be from the supplier with new bank account details.* *The Council must ensure the IT provider is asked to review the clerk's laptop and ensure it is rendered free of malware or viruses, to try and identify how the council email account was hacked, and to ensure cybersecurity controls are sufficient to prevent this form of hack recurring.* *The Council must follow up with the bank to ascertain whether the amount can be recovered and how the payment was made, considering supplier verification procedures in place.* *The risk assessment must cover the risk of supplier fraud as previously recommended.*	

	ISSUE	RECOMMENDATION	FOLLOW UP
	that may have been the source of the security breech. The Council have notified their banking provider of the fraud and have also requested information from them on how the payment was verified by confirmation of payee banking procedures, and whether the amount can be recovered. At the time of the interim audit, the Council had not received a response from the bank. The Council has not yet reviewed their annual risk assessment for 2022/23. It is important that the Council review the controls in place over supplier fraud to help prevent an incident such as this recurring, as we previously recommended.		
2	The fraudulent payment referred to in issue 1 has been posted in the ledger as expenditure made to the original supplier and VAT has been accounted for relating to this payment. The amount due to the bona fide supplier has not yet been paid.	*The Council can only reclaim VAT on the payment of the bona fide supplier invoice. Therefore, the council must now ensure that when the payment is made to the actual supplier that VAT is not reclaimed twice.*	
3	A review of the most recent budget report identified that the following ledger codes appear with the description 'not in use': • Centre 100 account code:1890 • Centre 100 account code:4430	*The Rialtas ledger must be updated to ensure that the ledger codes have descriptions that relate to real budgets the council has approved.*	

	ISSUE	RECOMMENDATION	FOLLOW UP
	• Centre 100 account code:4515 • Centre 135 account code:4515		