This policy remains fit for purpose apart from the date.

Halstead Town Council

Risk management policy

Risk policy purpose

This policy is a formal acknowledgement that the Council is committed to maintaining a strong risk management framework. The aim is to ensure that the Council makes every effort to manage risk appropriately by maximising potential opportunities whilst minimising the adverse effects of risks. It should be used to support the internal control systems of the Council, enabling the Council to respond to operational, strategic and financial risks regardless of whether they are internally or externally driven.

Risk policy objective

To confirm and communicate the Council's commitment to risk management, to establish a consistent framework and protocol for determining appetite to and for managing risk, to assign accountability to management and staff for risk within their control and provide a structured process for risk to be considered, reported and acted upon throughout the organisation.

Risk policy statement

The members and officers believe that sound risk management is integral to both good management and good governance practice. Risk management should form an integral part of the Council's decision-making and be incorporated within strategic and operational planning. Risk assessment will be conducted on all new activities and projects to ensure they are in line with the Council's objectives and mission. Any risks or opportunities arising will be identified, analysed and reported at an appropriate level. All staff will be provided with adequate training on risk management and their role and responsibilities in implementing this. The Council will regularly review and monitor the effectiveness of its risk management framework and update it as considered appropriate. Reports will be made to the Council of continuing and emerging high concern risks and those where priority action is needed to effect better control. Individual error and incident reports will be required from individual staff where a reportable event is identified. Such incidents which are considered to pose a significant threat to the Council, financial or otherwise, will be escalated in accordance with the crisis management plan. The risk of falling short of these standards is mitigated as far as possible by ensuring that appropriate policies and working practices are adopted in each of these key areas and that staff are adequately experienced and trained to manage this. Where necessary, external advice is sought to supplement internal expertise.

Organisational roles

Councillors

The role of the Council is to ensure that a culture of risk management is embedded in all activities and working practices. It is also to set the level of risk appetite for the organisation as a whole and in specific circumstances. It should also communicate its approach to risk and set standards of conduct expected of staff. It should ensure that risk management is included in the development of business plans, budgets and when considering strategic decisions. It should approve major decisions affecting the Council's risk profile or exposure.

Clerk

The clerk should ensure that less fundamental risks are being actively managed and controlled. They should also regularly review the Council's approach to risk management and approve any changes to this and ensure that risk management policy is implemented throughout the organisation. They should anticipate and consider emerging risks and keep under review the assessed level of likelihood and impact of existing key risks. They should provide regular and timely information to the councillors on the status of risks and their mitigation and implement adequate corrective action in responding to significant risks. They should learn from previous mistakes and ensure that crisis management plans are sufficiently robust to cope with high level risk. This policy supplements risk assessment carried out to ensure that individuals act in particular circumstances in order to minimise the risk of fraud, error, accident or infection. These limits cover amongst other things - control over bank payments and receipts, authorisation of and processing of expenditure and approval required at particular levels of decision making. In addition, the Council expects to meet minimum standards required by legislation and best practice in operational areas covering the following: • IT and data protection in line with GDPR • Governance • HR • Financial accounting and reporting • Health and safety •

Key risk areas

- Strategic – HTC could put itself at risk by making changes to its organisational structure which were not well thought through, by being unaware of changes to the law, by not monitoring the economic situation, or by taking action which might damage its reputation
- Operational – the risks in this area are linked to errors made by people, using the wrong process, the wrong system, or being affected by external events
- Financial - these are the risks which would arise if bad decisions were made on budgeting and expenditure, cash flow or loans
- Health and Safety – failure to identify risks – HTC has a separate Health & Safety policy
- Data Protection – there are many risks associated with collection and storage of data, which could be caused by human error, or outside interference – HTC has a separate Data Protection policy

Sarah Greatorex Reviewed February 2025 Next review date February 2026