

## **Topcliffe Parish Council Risk Management Policy**

Adopted: 12th May 2025

Reviewed: 7th May 2026

Review Date: 31st May 2027

### **1. Introduction**

Topcliffe Parish Council adopts this Risk Management Policy in accordance with the *Governance and Accountability for Local Councils – Practitioners’ Guide (JPAG)* and the *Health and Safety at Work Act 1974*.

The purpose of this policy is to set out how the Council will identify, evaluate, manage, and review risks affecting its operations, assets, finances, people and reputation.

This policy covers:

- The Council’s approach to risk management
- Objectives of risk management
- Types of risk
- Roles and responsibilities
- The risk management process
- Monitoring and review arrangements

The Council aims to embed risk management into its culture by:

- Integrating risk considerations into decision-making
- Ensuring risks are owned and managed at appropriate levels
- Following best practice and meeting audit expectations

### **2. Policy Statement**

The Council recognises its responsibility to manage risks effectively to protect:

- employees, volunteers, and councillors
- public funds and physical assets
- the delivery of services to the community
- the Council’s reputation and legal compliance

Some risks cannot be eliminated entirely, but the Council will adopt a structured and proportionate approach to managing them. Risk management is an integral part of the Council’s governance and operational processes.

### **3. Objectives of Risk Management**

The objectives of this policy are to:

- Identify, evaluate, and manage risks at both strategic and operational levels
- Protect physical assets and promote public and employee safety
- Embed risk awareness into day-to-day working arrangements
- Support effective and safe delivery of services
- Ensure risks and opportunities are considered in budgeting and business planning
- Enable informed decision-making
- Learn from past incidents, audits, and near-misses
- Promote good corporate governance
- Ensure Members and staff understand their responsibilities

#### **4. Types of Risk**

The Council will consider risks in the following categories:

- Financial – loss of money, fraud, budget overspend
- Security – theft, embezzlement, unauthorised access
- Property – damage, vandalism, maintenance failures
- Legal – non-compliance, litigation
- IT & Data – system failure, cyber security, GDPR breaches
- Reputational – complaints, negative publicity
- People – loss of key staff, councillor turnover, lone working
- Operational – service disruption, contractor failure
- Environmental – flooding, severe weather, tree safety

#### **5. Roles and Responsibilities**

Full Council

- Holds overall responsibility for risk management
- Approves the Risk Management Policy and annual Risk Register
- Considers risk implications when making decisions
- Reviews risk management reports and AGAR internal control statements

Parish Clerk / RFO

- Lead officer for risk management
- Maintains the Risk Register and ensures risks are recorded and updated
- Identifies new and emerging risks
- Ensures legal and financial implications are considered
- Manages insurance arrangements
- Advises Council on compliance and governance

Councillors

- Consider risks when debating and approving decisions
- Report new risks or concerns to the Clerk
- Support a culture of risk awareness

Employees / Contractors

- Report new risks or failures of control measures
- Follow safe working practices
- Assist in identifying operational risks

Internal Audit

- Provides independent assurance that risk management systems are in place
- Reviews internal controls and reports findings to Council

## 6. Risk Management Process

### Step 1: Identify Risks

Risks may be identified through inspections, day-to-day operations, new projects, changes in legislation, or reports from staff, councillors, or the public.

All identified risks must be recorded on a risk assessment form and added to the Risk Register.

### Step 2: Evaluate Risks

Each risk is assessed using a simple matrix:

- Likelihood: unlikely (1), possible (2), likely (3)
- Impact: negligible (1), moderate (2), severe (3)

Risk score = likelihood × impact

Risk levels:

- Red (7–9) – high/very high: immediate action and notification to Chair
- Amber (4–6) – medium: timely action required
- Green (1–3) – low: monitor and review

### Step 3: Mitigate Risks

The Clerk will identify existing controls and assess whether they are adequate. Controls may include:

- policies and procedures
- insurance
- training
- inspections and maintenance
- segregation of duties
- data backups

### Step 4: Determine Further Action

Options include:

- **Terminate** – stop the activity
- **Transfer** – insure or outsource
- **Treat** – introduce additional controls
- **Tolerate** – accept the risk but monitor

Where additional controls require non-budgeted expenditure over £500, this will be reported to Council (as stated in your document: “Where the implementation of additional controls incurs non-budgeted costs of £500 or over...”).

### Step 5: Allocate Responsibility

Each risk is assigned to the Clerk or another responsible person for monitoring and implementation of controls.

## Step 6: Maintain the Risk Register

All completed risk assessments are reviewed by the Chair before being added to the Risk Register.

Risks may be grouped into categories such as:

- Financial (F)
- Property (P)
- Legal (L)
- Open Spaces (OS)
- IT (IT)
- Reputational (R)
- Events (E)
- Staffing (ST)

## 7. Monitoring and Review

- The Council will review the Risk Register **annually** as part of the AGAR process.
- A standing agenda item on risk management will appear **quarterly**.
- The policy will be reviewed **annually** or sooner if required.
- Internal audit findings will be used to improve risk management.

## 8. Business Continuity

The Council will maintain basic continuity arrangements, including:

- secure digital backups
- emergency contact lists
- delegation arrangements for urgent decisions
- alternative meeting arrangements in case of disruption

## 9. Cyber Security

The Council will:

- use strong passwords and two-factor authentication
- maintain antivirus and software updates
- back up data securely
- follow GDPR principles
- report data breaches promptly