Minutes of the Performance Review Committee meeting held on Monday 27 April 2026, in Suite 2, Taverham Village Hall, commencing at 7.50pm when there were present:

Mrs C Karimi-Ghovanlou in the Chair

Mrs B Clarke Mrs J Latchford

Mr N Dack Mr T Yousefian

Also present: Clerk

Apologies for absence: None

To receive Declarations of Interest: None

The Minutes of the Meetings held on 17 November 2025 were confirmed and signed by the Chairman.

The following Council policies were reviewed recommendations made:
Standing Orders – No change
Financial Regulations – No change
Grant Awarding Policy – **Recommendation:** Change to considering applications twice per year. The grants budget would be spilt evenly between the two rounds with any unallocated funds from the first round being carried forward to the second round.
Biodiversity Policy – A report calling for the cessation of the Council use of herbicides and pesticides was received and given consideration while the policy was being reviewed. Councillors commented that some members of the public would consider that the village would look untidy if the use of herbicide was stopped, while others considered that the dead patches where areas had been treated were unsightly. **Recommendation:** No change to the policy until 2028 as changes will be needed to existing contract specifications.

The draft Committees' Terms of Reference were received, and it was **recommended** that the Council adopts the documents with no changes.

The draft GDPR policy was considered and the Committee **recommended** that the Council adopts the policy with no amendments

The General Privacy Notice was discussed and the Committee **recommended** that the Council adopts the notice without changes.

The Staff, Councillor and Role Holder Privacy Notice was reviewed and the Committee **recommended** that the notice be adopted with no changes.

The meeting closed at 8.37pm

Signed…… Dated……

Taverham Parish Council CCTV Policy

1. Purpose of This Policy

This policy sets out how Taverham Parish Council manages and operates Closed Circuit Television (CCTV) systems installed at:

- **Hinks Meadow Hall (external cameras)** – used for security of the hall, its grounds, and users of the facility.
- **Thorpe Marriott Green Play Area (external cameras)** – used to deter and prevent vandalism, criminal damage, and anti-social behaviour.

The Council is committed to ensuring that all CCTV usage complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and guidance issued by the Information Commissioner's Office (ICO).

2. Objectives of CCTV Use

The Council uses CCTV for the following purposes:

- To protect Council property, including buildings, equipment, and outdoor assets.
- To deter crime, including vandalism, theft, and anti-social behaviour.
- To assist in identifying individuals involved in criminal activity where appropriate.
- To enhance the safety of hall users, staff, contractors, and visitors at Hinks Meadow Hall.
- To support the Council's duty of care in maintaining safe public spaces.

CCTV will **not** be used for any form of routine monitoring of staff, councillors, or legitimate users of Council facilities.

3. Lawful Basis for Processing

CCTV footage is processed under Article 6(1)(e) UK GDPR (public task) where the Council is carrying out its public functions and responsibilities. Where appropriate, processing may also be undertaken under Article 6(1)(f) UK GDPR (legitimate interests) for the protection of Council property, facilities, and community assets.

4. Locations of CCTV Systems

4.1 Hinks Meadow Hall

External cameras are positioned to monitor:

- Entrances and exits
- Car park and external pathways
- Grounds surrounding the hall

The purpose is security and protection of the premises.

4.2 Thorpe Marriott Green Play Area

External cameras are positioned to monitor:

- Play equipment
- The skatepark
- Seating and gathering areas
- Access points to the play area

The purpose is prevention of vandalism and anti-social behaviour.

Cameras are **not** positioned to intrude on private residential property.

5. Management and Operation

- Taverham Parish Council is the Data Controller for both CCTV systems.
- The Clerk is responsible for day-to-day management, including access control, data handling, and compliance.
- Only authorised personnel may access CCTV recordings.
- All authorised personnel will receive appropriate training.

6. Signage
Clear and visible signage will be displayed at both sites stating:

- CCTV is in operation
- The purpose of the CCTV
- Contact details for Taverham Parish Council as the Data Controller

Signage will comply with ICO requirements.

7. Data Storage and Retention

- CCTV footage will normally be retained for a maximum of 30 days in accordance with the Council's Data Retention Schedule unless required for an ongoing investigation.
- Footage required for police or insurance investigations may be retained longer, but only for the duration of the investigation.
- After the retention period, footage will be automatically overwritten or securely deleted.

8. Access to Footage
Access to CCTV footage will be strictly controlled:

- **Internal access**: Only authorised staff (typically the Clerk or designated officers) may view footage.
- **External access**: Footage may be shared with:
  - Norfolk Constabulary
  - Insurance providers
  - Legal representatives
  - Individuals making a valid Subject Access Request (SAR), where lawful and appropriate
  - External CCTV maintenance engineers and support providers may be granted access for system maintenance, troubleshooting, repairs, and software updates. Such access is controlled, logged where possible, and subject to confidentiality and data protection requirements.

All access requests will be logged.

9. Subject Access Requests (SARs)
Individuals may request access to footage in which they appear. The Council will:

- Respond within one calendar month
- Provide footage only where the identity of other individuals is protected or redacted
- Refuse requests where disclosure would prejudice crime prevention or ongoing investigations

Requests must be made in writing to the Clerk.

10. Disclosure to Law Enforcement
Footage may be disclosed to Norfolk Constabulary when:

- A crime has occurred
- A crime is suspected
- The police request footage for investigation

All disclosures will be documented.

11. Data Security
The Council will ensure:

- Secure storage of all recordings
- Password-protected access
- Regular system maintenance
- Appropriate technical and organisational measures to prevent unauthorised access, alteration, or deletion
- Any suspected unauthorised access, disclosure, loss, or compromise of CCTV footage will be handled in accordance with the Council's Data Breach Procedure.

12. System Maintenance
The Council will ensure that:

- CCTV equipment is maintained in good working order
- Faults are logged and addressed promptly
- Cameras remain correctly positioned and focused
- Systems are reviewed periodically to ensure they remain necessary and proportionate

13. Review of CCTV Use
The Council will review this policy and the operation of CCTV systems **annually**, considering:

- Whether the systems remain necessary and proportionate
- Any changes in legislation
- Any issues raised by the public, police, or insurers
- Any incidents that required footage retrieval

14. Complaints
Complaints about the Council's use of CCTV should be submitted in writing to the Clerk. If unresolved, individuals may escalate concerns to the **Information Commissioner's Office (ICO)**.

15. Policy Approval and Review
This policy was adopted by Taverham Parish Council on: **[insert date]**
Next review due: **[insert date]**

Taverham Parish Council
GDPR Policy

1. Introduction
The Parish Council is committed to protecting the personal data it holds and ensuring it is used lawfully, fairly, and transparently. This policy explains how the Council complies with:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018**
- The **Freedom of Information Act 2000** (where relevant)
- The **Local Government Act 1972** (record-keeping and publication duties)
- The **Local Audit and Accountability Act 2014** (transparency and inspection rights)
- The **Transparency Code for Smaller Authorities**

This policy applies to all councillors, employees, contractors, and volunteers who handle personal data on behalf of the Council.
The Parish Council is the **Data Controller**, as defined in Article 4(7) UK GDPR.

2. What is Personal Data?
Personal data is defined in Article 4(1) UK GDPR as any information relating to an identifiable living person. Examples include:

- Names, addresses, email addresses, phone numbers
- Photographs or CCTV images
- Bank details or payment information
- Opinions or comments linked to an identifiable person
- Information about complaints, service requests, or correspondence
- Employment or volunteer information

Some personal data is classed as **special category data** under Article 9 UK GDPR (e.g., health information, political opinions). The Council only collects this where absolutely necessary and with appropriate safeguards.

3. How the Council Collects Personal Data
The Council collects personal data when individuals:

- Contact the Council by email, phone, letter, or online
- Complete forms, surveys, booking requests, or applications
- Attend Council events or use Council facilities
- Apply for a job, contract, or volunteer role
- Provide information to councillors in their official capacity
- Submit comments on planning applications or consultations
- Personal data may also be collected through Council-operated CCTV systems where this is necessary for security, crime prevention, public safety, or protection of Council assets.

We may also receive information from third parties, such as:

- Other local authorities
- Contractors working on our behalf
- Public bodies (e.g., Electoral Services under the Representation of the People Regulations)

The Council always aims to collect the minimum amount of data needed to carry out its statutory functions.

4. How the Council Uses Personal Data
The Council uses personal data to fulfil its statutory duties and functions under:

- The **Local Government Act 1972**
- The **Localism Act 2011**
- The **Local Government Finance Act 1992**

DRAFT

- The **Local Audit and Accountability Act 2014**
- The **Transparency Code for Smaller Authorities**

This includes:

- Responding to enquiries and providing services
- Managing bookings, facilities, and events
- Administering finances, contracts, and payments
- Meeting legal and statutory obligations
- Communicating Council decisions and public information
- Managing staff, councillors, and volunteers
- Supporting community engagement and consultations
- Maintaining records of Council business, including minutes and agendas

The Council does **not** use personal data for marketing and never sells personal information.

5. Lawful Basis for Processing

Under Article 6 UK GDPR, the Council processes personal data under one or more lawful bases:

- **Public task** – performing the Council's official functions (Article 6(1)(e))
- **Legal obligation** – complying with the law (Article 6(1)(c))
- **Contract** – delivering a service or agreement (Article 6(1)(b))
- **Consent** – where the individual has clearly agreed (Article 6(1)(a))
- **Legitimate interests** – only where appropriate and minimal (Article 6(1)(f))

Where special category data is processed, the Council relies on Article 9(2)(b), (g), or (a) depending on the context.

Where consent is used, individuals may withdraw it at any time.

6. Data Minimisation and Retention

The Council follows the principles in Article 5(1)(c) and (e) UK GDPR:

- Only collecting data that is necessary
- Keeping it accurate and up to date
- Retaining it only for as long as needed

Retention periods are set out in the Council's **Data Retention Schedule**, informed by:

- The **Local Government Act 1972** (permanent retention of minutes)
- The **Local Audit and Accountability Act 2014**
- The **Transparency Code**
- Best practice guidance for local authorities

7. Data Security

The Council takes appropriate technical and organisational measures to keep data secure, in line with Article 32 UK GDPR.

Digital security

- Password-protected devices and accounts
- Two-factor authentication where available
- Secure cloud storage or encrypted drives
- Regular backups
- Avoiding personal email accounts for Council business

Paper records

- Locked cabinets or secure storage
- Shredding or secure disposal of confidential waste

Access control

- Only those who need the information can access it
- Councillors only access data relevant to their role or casework

8. Sharing Personal Data

The Council may share personal data with:

- Local authorities or government bodies
- Contractors or service providers working on behalf of the Council
- Auditors, insurers, or regulators
- Law enforcement (where required under legislation)
- Funding bodies or grant providers

Data is only shared when necessary and always in a secure and lawful way.
The Council does **not** transfer personal data outside the UK unless appropriate safeguards are in place, in accordance with Chapter V UK GDPR.

9. Rights of Individuals

Under Articles 12–23 UK GDPR, individuals have the right to:

- Be informed
- Access their personal data
- Request correction
- Request deletion (where appropriate)
- Restrict or object to processing
- Request data portability (where applicable)

Requests should be made to the Clerk. The Council will respond within one month unless the request is complex.

10. Data Breach Procedure

In accordance with Articles 33 and 34 UK GDPR, the Council will:

- Record all breaches
- Assess the risk to individuals
- Notify the ICO within 72 hours where required
- Inform affected individuals where there is a high risk of harm

A full step-by-step breach procedure is included in this policy.

11. Training and Awareness

The Council ensures councillors and staff receive appropriate data protection training, in line with the accountability principle in Article 5(2) UK GDPR.

12. Roles and Responsibilities

- **The Parish Council** is the Data Controller (Article 4(7)).
- **The Clerk** manages day-to-day data protection and acts as the main contact for data requests and breaches.
- **Councillors and staff** must follow this policy and handle personal data responsibly.
- **Contractors** must comply with UK GDPR when handling data on behalf of the Council.

13. Review of Policy

This policy will be reviewed annually or sooner if legislation or Council practices change, in line with the accountability requirements of Article 24 UK GDPR.

Date of adoption: May 2026

DRAFT

TAVERHAM PARISH COUNCIL
GENERAL PRIVACY NOTICE

1. What is personal data?

"Personal data" means any information relating to an identified or identifiable living individual. This includes information such as names, addresses, photographs, identification numbers, online identifiers, or any data that can be linked with other information to identify a person.

The processing of personal data is governed by UK data-protection legislation, including:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018**
- The **Privacy and Electronic Communications Regulations (PECR)**
- Relevant updates introduced by the **Data (Use and Access) Act 2025**

2. Who are we?

This Privacy Notice is provided by Taverham Parish Council, which is the data controller for the personal data we process.

Other data controllers we work with

We may work with, or share data with:

- Other local authorities
- Community groups
- Charities and voluntary organisations
- Contractors and service providers
- Credit reference agencies
- Not-for-profit organisations

Where we jointly determine the purposes and means of processing, we act as joint controllers. Where each party processes data for its own purposes, each acts as an independent controller.

3. What personal data do we process?

We may process some or all of the following categories of personal data:

- Names, titles, aliases, photographs
- Contact details (addresses, telephone numbers, email addresses)
- Demographic information (gender, age, marital status, nationality)
- Employment, education or qualification details
- Family information, dependants
- Financial information (bank details, payment information, grant applications)
- Information relating to council services you use
- CCTV images and recordings collected through Council-operated CCTV systems for crime prevention, public safety, protection of Council property, prevention of vandalism and antisocial behaviour, and safeguarding users of Council facilities.

Special category data and criminal offence data

Where necessary and lawful, we may process:

- Health information
- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Biometric or genetic data
- Sexual orientation
- Criminal convictions or allegations

We only process this data where permitted under UK GDPR, including:

- With your explicit consent
- Where required by law
- Where necessary for reasons of substantial public interest
- Where needed to protect vital interests

- Where the information has been made public by you

4. How and why we use your personal data
We use your personal data to:
- Deliver public services and statutory functions
- Confirm your identity
- Contact you by post, email, telephone or social media
- Maintain our accounts and records
- Prevent and detect fraud or crime. The use of CCTV protects Council property, promote public safety, deter crime and support investigations
- Carry out safeguarding duties
- Manage facilities, events and community services
- Process financial transactions
- Seek your views and feedback
- Notify you of changes to services
- Carry out research and statistical analysis to improve services

5. Legal bases for processing
As a public authority, we primarily process personal data because it is:
- **Necessary for performing a task carried out in the public interest** or
- **Necessary for exercising our official authority**

We may also process data where:
- It is necessary to comply with a **legal obligation**
- It is necessary for the performance of a **contract**
- You have given **consent** (e.g., for optional communications)
- It is necessary for **legitimate interests** (where applicable and not overridden by your rights)

Special category data is processed only where a UK GDPR Article 9 condition applies.

6. Sharing your personal data
We may share your data with:
- Other public authorities
- Contractors and service providers acting on our behalf
- Partner organisations involved in joint projects
- Law-enforcement bodies where required - CCTV footage may be disclosed to police, insurers, legal representatives and CCTV maintenance providers where lawful and necessary.

All third parties must comply with UK data-protection law and implement appropriate security measures.

7. International transfers
If we transfer personal data outside the UK, we will ensure appropriate safeguards are in place, such as:
- A UK **adequacy regulation**
- The **International Data Transfer Agreement (IDTA)**
- The **UK Addendum to the EU Standard Contractual Clauses**

Some information published on our website (e.g., newsletters) may be accessible from overseas.

8. How long we keep your data
We retain personal data only for as long as necessary for the purposes for which it was collected, in line with:
- Statutory retention requirements
- Limitation periods for legal claims
- Best-practice guidance for local authorities

- CCTV recordings are normally retained for up to 30 days unless required for an ongoing investigation or legal purpose.

Some records may be kept permanently where required for archiving or historical purposes.

9. Your rights

You have the following rights under UK GDPR:

- **Right of access** – to request copies of your personal data
- **Right to rectification** – to correct inaccurate or incomplete data
- **Right to erasure** – in certain circumstances
- **Right to restrict processing**
- **Right to object** to processing carried out in the public interest
- **Right to data portability** (where applicable)
- **Right to withdraw consent** at any time (where consent is the basis for processing)
- **Right to complain** to the Information Commissioner's Office (ICO)

We may need to verify your identity before responding to a request.
Individuals may make a Subject Access Request for CCTV footage in which they appear.
Requests will be handled in accordance with UK GDPR and the Council's CCTV Policy.

10. Further processing

If we intend to use your personal data for a new purpose not covered by this notice, we will issue a new privacy notice before processing begins and seek consent where required.

11. Changes to this notice

We keep this Privacy Notice under regular review.
This version was last updated in **May 2026**.

12. Contact details

For questions, concerns, or to exercise your rights, please contact:
The Data Controller
Taverham Parish Council
Taverham Village Hall
Sandy Lane
Taverham
Norwich
NR8 6JR
Email: clerk@taverhamparishcouncil.org.uk

Taverham Parish Council

Financial Risk Assessment and Management Policy

Definition of Risk Management. Risk is the threat that an event or action will adversely affect an organisations ability to achieve its objectives or successfully execute its strategies. Risk Management is the process by which risks are identified, evaluated and controlled. It is a key element of the framework of governance together with community focus, structures and processes, standards of conduct and service delivery arrangements.

This document has been produced to enable Taverham Parish Council to assess the risks that it faces and satisfy itself that it has taken adequate steps to minimise them. The Council is aware that although some risks can never be eliminated fully, it has in place a strategy that provides a structured, systematic and focused approach to managing risk, which:

- Identifies the key risks facing the council
- Identifies what the risk may be
- Identifies the level of risk
- Evaluates the management and control of the risk and records findings
- Regularly review, assess and revise procedures if/when required.

MANAGEMENT				
Subject	**Risk Identified**	**H/M/L**	**Management / Control of Risk**	**Review / Assess / Revise**
Business Continuity	Council not able to continue business due to unexpected or tragic circumstance.	L	Files automatically backed up in the cloud. Finance system is remotely based. Temp staff may need to be recruited in long term absence or resignation of Clerk/RFO. Loss of office accommodation/loss of internet connection	Existing procedure adequate. Additional funds included in wages budget. Staff can work from home.
Meeting Location	Health and Safety	L	Venue is managed by Taverham Village Hall Committee and is independent from Taverham Parish Council and Health and Safety is managed by the Committee. Fire equipment and exits are in place.	Existing location and procedures suitable.

MANAGEMENT				
Subject	**Risk Identified**	**H/M/L**	**Management / Control of Risk**	**Review / Assess / Revise**
Meeting Location	Adequacy Building Closure	L L	The premises and the facilities are considered to be adequate for the Clerk, Councillors and Public who attend from Health and Safety and comfort aspects. Seek alternative venue.	Existing location and procedures suitable.
Council Records (Paper)	Loss through theft, fire or damage.	M	Taverham Parish Council records are stored at the Council Office based at Taverham Village Hall. Records include historical correspondence, minute books and copies, leases for land or property, records such as personnel, insurance, salaries etc. Recent documents are in a metal filing cabinet (not fireproof) and older historical records (not minute books) in the Warden's store at Taverham Village Hall.	Scan deeds and historical minutes, store originals at Norfolk County Council Archives – Ongoing
Council Electronic Records	Loss through damage, fire, corruption or theft of computer. Unauthorised access	L M	Microsoft 365 has been installed, this is an efficient back-up system which allows remote access. Anti-virus in place and kept current. Office laptops are password protected. Tablet used by PATCH Administrator, password protected.	Existing procedure adequate.
Cyber Security and Data Protection	Loss of data, unauthorised access to Council systems, cyber attack, phishing, ransomware, data breach or loss of personal information.	M	Microsoft 365 utilised for email and document storage. Council laptops and devices are password protected. Anti-virus and security software maintained and updated. Access to systems restricted to authorised users. Personal data processed in accordance with the Council's Data Protection Policy and privacy requirements. Staff undertake relevant training and security awareness measures.	Review annually. Monitor cyber security arrangements, access permissions and training requirements. Ensure software and security updates are applied regularly.
Electronic Systems and Cloud Services	Loss of access to Council records, systems or email services due to software failure, supplier outage or cyber incident.	M	Council records stored electronically with cloud-based resilience and recovery arrangements. Critical financial information is held within secure accounting systems.	Review business continuity arrangements annually and following any significant system changes.

FINANCE				
Subject	**Risk Identified**	**H/M/L**	**Management / Control of risk**	**Review / Assess / Revise**
Precept	Adequacy of precept	L	The Council reviews the Precept requirement annually at the January meeting and reviews the presented budget update information for the next financial year. With this information the Council then agrees the amounts set for the specific budget headings for the following year, the total of which is resolved to be the precept amount to be requested from Broadland District Council. This figure is submitted by the RFO in writing to Broadland District Council. The Council receive the monies in April and October. The Budget is monitored on a monthly basis.	Existing procedure adequate.
Precept	Adequacy of precept			Existing procedure adequate.
Insurance	Adequacy	L	An annual review is undertaken, prior to the time of the policy renewal, of all insurance arrangements.	Review provision and compliance annually.
	Cost / Compliance	L	Asset Register is updated and assessed at same time.	Asset Register is maintained.
	Fidelity Guarantee	L	Employers Liability, Public Liability and Fidelity Guarantee (statutory requirements) in place.	
Banking	Inadequate checks	L	Financial Regulations in place. Monthly bank reconciliation and payments list presented to members. All banking records available to view in office.	Financial regulations reviewed annually. Continue internal audit checks on a monthly basis.
Cash	Loss through theft or dishonesty	L	Taverham Parish Council has £150 petty cash in the office. Transactions are made by cheque or online.	Existing procedure adequate.
		L	Taverham Parish Council receives few cash payments for room hire. All monies are receipted, recorded and banked. Internal checks are in place and subject to internal audit quarterly. Regular hirers are now encouraged to use electronic payment methods.	Existing procedure adequate.
		L	The Council's insurance policy has a Fidelity Guarantee - £1,000,000.	Ensure Fidelity Insurance is adequate.

FINANCE				
Subject	**Risk Identified**	**H/M/L**	**Management / Control of risk**	**Review / Assess / Revise**
Financial controls and records	Inadequate checks	L	Two signatories on cheques. All payments resolved and minuted. s137 payments identified separately on accounts system and minuted at time of approval. There is a full programme of monthly internal checks.	Existing procedure adequate.
Freedom of Information Act	Policy provision	L	Policy in place and clear guidance online for submission of Freedom of Information requests.	Existing procedure adequate. Monitor and report any impacts of requests made under the FOI Act.
Personnel	Personnel Health and Safety	L L L	Designated reserves for employment costs are planned into budgets. Includes recruitment costs, SSP provision, new training. Significant financial controls and monthly monitoring in place. Taverham Parish Council has various policies outlining behaviour and procedures, along with a Training policy and budget including Health and Safety. Training budget to ensure CPD, membership of SLCC, current reference books, regular attendance at NALC and other events. Annual appraisal process.	Existing procedure adequate. Continue existing planning, monthly monitoring and reporting. Monitor working conditions, safety requirements and insurance regularly. Check recruitment procedures to ensure references and background checks take place. The Parish Council has sufficient reserves to enable training for the CiLCA qualification in the event of the Clerk resigning.
Election Costs	Unbudgeted election cost	L/M	Risk is higher in an election year. When an election is due the ~~Clerk~~ RFO will obtain an estimate of costs from the District Council for a full election and an uncontested election. There are no measures which can be adopted to minimise the risk of	Existing procedure adequate

FINANCE				
Subject	**Risk Identified**	**H/M/L**	**Management / Control of risk**	**Review / Assess / Revise**
			having a contested election as this is a democratic process and should not be stifled. The Council could consider creating an ear-marked reserve and setting money aside annually towards election costs.	Ear-marked reserve to be considered.
VAT	Reclaiming / charging	L	Taverham Parish Council has Financial Regulations that sets out the requirements.	Existing procedure adequate.
AGAR	Failure to comply with statutory AGAR requirements, publication requirements or submission deadlines.	L	The Annual Governance and Accountability Return (AGAR) is prepared by the Responsible Financial Officer (RFO) and presented to the Council for consideration and approval within the statutory timescales. The Internal Auditor undertakes an annual review of the Council's systems of internal control and financial records and provides an independent report. The AGAR and supporting documentation are then submitted to the External Auditor in accordance with the requirements of the Accounts and Audit Regulations and current AGAR guidance.	Appropriate procedures are in place to ensure compliance with publication and submission deadlines.

ASSETS				
Subject	**Risk Identified**	**H/M/L**	**Management / Control of Risk**	**Review / Assess / Revise**
Play Area & Equipment	Public injury	L	Weekly recorded check of area and equipment. Twice yearly Play Area Inspections by The Play Inspection Company – remedial actions taken when identified. Public liability insurance in place.	Existing procedure adequate. Reviewed annually.
Street Lighting	Public injury Outage / damage	L L	Public liability insurance in place. Maintenance contractor in place. Electrical testing every six years and structural testing every 20/25 years.	Reviewed annually. Maintenance contract under a four-year contract.

ASSETS				
Subject	**Risk Identified**	**H/M/L**	**Management / Control of Risk**	**Review / Assess / Revise**
Street Furniture / Dog Waste Bin / Litter Bin	Public injury Damage / destruction	L L L	Public liability insurance in place. Units sourced from suppliers of street furniture, ensuring compliant materials and designed with public safety in mind. Designated funds in budgets for repairs and replacement.	Reviewed annually. Existing procedure adequate.
Notice boards	Public injury Damage / destruction	L L	Public liability insurance in place. Taverham Parish Council has six noticeboards sited around the parish. These are inspected regularly by the Warden and any repairs/maintenance requirements are brought to the attention of the Taverham Parish Council.	Reviewed annually. Existing procedure adequate.
Village signs	Public injury	L	Public liability in place.	Reviewed annually.
Office Equipment	Staff/councillor injury Loss / damage	L L	Training provided for new users. Employers' liability insurance in place and insurance in place, depending on asset value.	Existing procedure adequate. Reviewed annually.

LIABILITY				
Subject	**Risk identified**	**H/M/L**	**Management / control of risk**	**Review / assess / revise**
Legal Powers	Illegal activity / payments	L	Decisions and payments made only within the powers of the Parish Council. Procedures clearly outlined in Standing Orders and Financial Regulations.	Existing procedure adequate.

LIABILITY				
Subject	**Risk identified**	**H/M/L**	**Management / control of risk**	**Review / assess / revise**
Minutes / Agendas / Statutory documents	Accuracy / legality Non-compliance with statutory requirements.	L L	Minutes and agendas are produced in the prescribed method and adhere to legal requirements. Minutes are approved and signed at next meeting. Minutes and agendas are displayed according to legal requirements. Business conducted at Council meetings managed by the Chair.	Existing procedure adequate. Ensure all councillors are adequately trained. Members to adhere to Code of Conduct.
Public Liability	Risk to third party, property or individuals	L	Insurance in place, £10 million any one event. Risk assessments regularly carried out to comply with requirements.	Review annually. Existing procedure adequate.
Employer Liability	Non-compliance with employment law	L	Employer's liability insurance in place. Clerk updates current knowledge through ACAS, SLCC, HMRC, etc Councillors receive Good Employer Guide on appointment.	Review annually. Existing procedure adequate.
Legal Liability	Legality of activities	L	Official's Indemnity incorporated into Employers Liability - £10 million any one event inclusive of costs.	Existing procedure adequate.
Members interests	Conflict of interest	L	Councillors have a duty to declare any interests at the start of the meeting. Councillors are asked to declare all interests (pecuniary and non-pecuniary) in agenda items at every Council meeting/Committee meeting to ensure transparency.	Existing procedure adequate. Members take responsibility to update their Register.

Adopted: 8th December 2025

Minute ref: 175/25

Next Review: November 2026

TAVERHAM PARISH COUNCIL – Internal Audit Checklist (2027/28)

Item	Date Checked and Signature
Insurance in place – Employer and Public Liability insurance	
Asset register up to date	
Large purchases added to insurance schedule	
Petty Cash payments match receipts and petty cashbook	
Payslips checked against approved salaries and PAYE/NI/Pension payments match pay slip totals	
HMdow receipts match booking forms	
Sickness Chart	
Bank statements/electronic payments checked against computer entries	
VAT Return Submitted	
Approval List/electronic payments match invoices	
Invoices match quotes/orders	
Bank Reconciliations – checked and signed by non-bank signatory	