

St Austell Town Council



Finance and General Purposes Committee

To: All Members of the Finance and General Purposes Committee

(Councillors: Brown, Clemo, Cohen, Gray, Hamilton, Kimber, Lanxon, Marshall, Pearce, Preece, Rowse, Thompson, Whitehouse and Young).

Dear Councillor

You are summoned to attend a **Meeting of the Finance and General Purposes Committee** to be held in **Chi Austel, White River Place, St Austell, Cornwall, PL25 5AZ** on **Monday 16th February 2026 at 6pm.**

David Pooley
Town Clerk

10th February 2026

Tel: 01726 829859

E.mail: david.pooley@staustell-tc.gov.uk

Website: www.staustell-tc.gov.uk

AGENDA

- 1. Apologies for absence**
- 2. Declarations of Interest**

(Purpose: To receive declarations of disclosable pecuniary and other non-registerable interests in respect of items on this agenda).

This meeting has been advertised as a public meeting and as such could be filmed or recorded by broadcasters, the media or members of the public.

Please be aware that whilst every effort is taken to ensure that members of the public are not filmed, we cannot guarantee this, especially if you are speaking or taking an active role.

3. Dispensations

(Purpose: To receive requests for dispensations under the Code of Conduct).

4. Minutes of meeting held on 3rd November 2025

**Pages
1 - 6**

(Purpose: To agree that the minutes of the above meeting be signed as a correct record). (Attached).

5. Matters to Note

A verbal update from the Town Clerk on the actions taken since the last meeting. Note: No decision may be made under this agenda item.

6. Public participation (15 minutes maximum)

The Chairman will invite members of the public to address the meeting in relation to the business to be carried out at the meeting.

15 minutes will be allocated for public participation (this can be extended at the Chairman's discretion). Each person addressing the Council will be allocated a maximum of two minutes.

7. Insurance Renewal

**Pages
7 - 8**

(Purpose: To approve the renewal of the Council's insurance cover). (Report attached).

8. CCTV

**Pages
9 - 10**

(Purpose: To consider a report on the potential to add to the CCTV camera system). (Report attached).

9. Budget Monitoring Report

**Pages
11 - 18**

(Purpose: To review the Town Council's budget monitoring report for the period 1st April 2025 to the 31st January 2026). (Report attached).

10. Information Technology Policy

**Pages
19 - 34**

(Purpose: To review and approve a draft Information Technology Policy). (Attached).

This meeting has been advertised as a public meeting and as such could be filmed or recorded by broadcasters, the media or members of the public.

Please be aware that whilst every effort is taken to ensure that members of the public are not filmed, we cannot guarantee this, especially if you are speaking or taking an active role.

11. Risk Management

**Pages
35-44**

(Purpose: To review and update the Council's Risk Management Strategy and Register). (Attached).

12. Treasury Management

**Pages
45-53**

(Purpose: To provide Members with a breakdown of the Council's Treasury Management activity during the 2025/26 financial year and re-confirm the Council's Treasury Management Strategy). (Attached).

13. Library

(Purpose: To receive an update on the activities of St Austell Library). (Report to follow).

14. Dates of Next Meetings

(Purpose: To note the date of next meeting – 13th April 2026).

This meeting has been advertised as a public meeting and as such could be filmed or recorded by broadcasters, the media or members of the public.

Please be aware that whilst every effort is taken to ensure that members of the public are not filmed, we cannot guarantee this, especially if you are speaking or taking an active role.

MINUTES of a MEETING of the FINANCE AND GENERAL PURPOSES COMMITTEE held on MONDAY 3rd NOVEMBER 2025 in Chi Austel, White River Place, St Austell, Cornwall, PL25 5AZ at 6pm.

Present: Councillors: Brown, Clemo, Cohen, Gray, Hamilton, Lanxon, Marshall, Thompson, Whitehouse and Young

In attendance: David Pooley (Town Clerk) and Sara Gwilliams (Deputy Town Clerk).

Also in attendance: Councillor Pearce (TEAMS) and Councillor Taylor.

F/25/32) Apologies for absence

Apologies for absence were received from Councillors Kimber and Preece.

F/25/33) Declarations of Interest

Councillor Whitehouse declared an interest in agenda item 11 by virtue of his stepmother being on the St Austell Festival of Music and Speech Committee.

F/25/34) Dispensations

None.

F/25/35) Minutes of meeting held on 29th September 2025

It was **RESOLVED** that the minutes of the meeting held on 29th September 2025 be approved and signed as a correct record.

F/25/36) Matters to Note

The Clerk advised that further to minute number F/25/25, Cornwall Council has confirmed that their staff are expected to either pay for parking or find suitable parking in the town when visiting Chi Austel.

F/25/37) Public participation

There were no members of the public present.

F/25/38) Budget 2025/26 and 2026/27

The Clerk advised that following the informal budget/priorities meeting at the beginning of October, a draft budget for the 2026/27 financial year had been produced and highlighted the assumptions made within the draft:

- Provision for maternity leave cover
- Additional senior officer resource
- Deletion of the Regeneration Officer post at the end of March 2026
- Renewal of the lease of the Stable Block and the associated costs required within the Heads of Terms
- Continuation of CCTV/monitoring costs and security personnel
- £20,000 budget for events (reduced from £30,000)
- An increase from £8,000 to £10,000 for the Small Grants Scheme

- A £5,000 budget for the Youth Council when it has been set up
- An additional Grounds Maintenance Apprentice
- £50,000 for playground equipment repairs/maintenance
- £25,000 for a vehicle or mower replacement
- £25,000 for pump priming projects

In addition, the Clerk advised that Cornwall Council has not yet invoiced the Town Council for the contested election in May, but when it is received, it is likely to be in the region of £7,000. Cornwall Council is also expected to announce the pension contribution rate and council tax base in November which will adjust the draft budget slightly.

The Clerk advised that the budget and Council Tax is due to be set at the Town Council meeting on Monday 15th December 2025 and recommended that a Council Tax increase of in the region of 8.2% for the 2026/27 financial year would set a balanced budget, maintain services and provide some small growth. He clarified that a Council Tax increase of 8.2% equates to a 31p per week increase for a Band D property.

During discussion, mixed views were expressed with regard to the increase in Council Tax that should be levied. Overall, Members felt that although they would like the Town Council to have more resource, they were mindful of the impact Council Tax increases have on the electorate.

Arising from a question, the Clerk confirmed that the £80,000 underspend from the 2024/25 financial year and the £27,000 in saving in election costs has been placed into a reserve and in due course he will put a report to Members suggesting one or two projects that the money could be used for.

A view was expressed that a wheelchair swing should be installed in Poltair Park. The Clerk responded that the Operations Manager is looking at the refurbishment of the play park in Poltair Park and that 2-3 designs with various pieces of play equipment, including accessible equipment will be brought to Members in due course for consideration.

It was **RECOMMENDED** that subject to any reasonable adjustments required following announcements with regard to the Council Tax Base and the pension contribution rate, the Council:

1. Approves the revised draft budget for the 2026/27 financial year;
2. Approves a Council Tax increase of approximately 8.2% for a Band D property paying the full Council Tax charge.

F/25/39) Budget Monitoring Report

The Clerk explained the key variations in the report for the current financial year to 30th September 2025 and raised no concerns.

Members noted that the car park income is performing well against budget.

It was **RESOLVED** to note the report.

F/25/40) Standing Orders - Trusts

The Clerk explained that the Town Council as a whole is legally the trustee for one charitable trust and one trust which is not a registered charity, but the Standing Orders are silent on the minimum number of councillors required for meetings of these trusts.

He suggested that at least 1/3rd of the whole number of members of the council should be present and that this should be reflected in the Standing Orders.

It was **RECOMMENDED** that Standing Order 3U should be amended to read as follows:

No business may be transacted at a meeting unless at least one-third of the whole number of members of the council are present and in no case shall the quorum of a meeting be less than three. Where the Council is meeting in its capacity as a trustee for a formal trust this clause shall apply. See standing order 4d (vi) below for the quorum of a committee or sub-committee meeting.

F/25/41) Interim Internal Audit Report

The Clerk advised that the Interim Internal Audit Report for the year ended 31st March 2026 has been received with one recommendation regarding the reconciliation of contactless card payments for Priory Car Park.

The Clerk advised that he would contact the software provider to see if the amounts received into the Town Council's bank account can be independently verified.

It was **RESOLVED** to note the report.

F/25/42) Small Grants Scheme

It was **RESOLVED** to award a grant in the sum of £250 to the St Austell Festival of Music and Speech.

Councillor Whitehouse took no part in the voting on the above item

F/25/43) Licencing Reforms Programme (at the request of Councillor Brown)

Councillor Brown referred to his draft answers to the questions contained within the Government's consultation paper on "Licencing Reforms Programme – Call for Evidence"

During discussion, Members suggested that a reference to the general lack of awareness of the Government's public notice portal and the use of on-line newspapers should be included in the response to question 16.

It was **RESOLVED** to approve the draft response subject to the additions suggested above.

F/25/44) Town Councillor Vacancy – Poltair and Mount Charles Ward

The Town Clerk advised that following the resignation of Councillor Pears, a Notice of Vacancy for Poltair and Mount Charles Ward has been issued by Cornwall Council. If an election is not requested by Friday 7th November 2025, the vacancy is eligible to be filled by co-option.

The Clerk explained the Town Council's co-option procedure which invites interested parties to complete a short application form outlining why they would like to be a Town Councillor. The completed forms are validated, and the applicants are invited to attend a full Council meeting to perform a short presentation to Members. After the presentation by each candidate, each Member votes for their preferred candidate.

A view was expressed that a by-election coinciding with the Christmas holidays would be unfortunate.

It was **RESOLVED** to adopt the Town Council's co-option procedure if a formal election is not triggered and authorise the Town Clerk to advertise the vacancy within the Poltair and Mount Charles Ward at the earliest opportunity.

F/25/45) St Austell Library

The Deputy Town Clerk provided an update on the Library as follows:

Staffing

There are 2 full time staff, 6 part time staff and a vacancy of 24 hours has just been filled. Renewal DBS checks for each member of staff and the volunteers within the library are underway. The volunteers at the library are carrying out general library duties and administering the Home Library Service. The library is open 9am to 5pm Monday to Friday and 10am to 1pm on Saturday and continues to hold a number of core activities during the week including Sing and Shake (0-4 year olds), Story Time (0-4 year olds), reading and writing groups, whole school visits and Knit and Natter.

SALSA continue to hold events at the library with a number of activities for Christmas planned including a craft fair, wreath making, Father Christmas, reindeer and a mini-Christmas tree competition. A "friendship bench" for the library garden is also being purchased. The High Sheriff has been working with the grounds staff on a landscaping scheme in the front garden and an oak tree will be planted by the High Sheriff and Mayor on 10th November 2025.

Cornwall Council is still keen for the Town Council to take on the freehold of the building and discussions are due to resume again. The main issue to resolve before the transfer is the age and condition of the boiler.

F/25/46) To consider excluding the press and public

It was **RESOLVED** that under Section 1 (ii) of the Public Bodies (Admission to Meetings) Act 1960, the public and press be excluded from the meeting for the remainder of the business of the meeting in view of the confidential nature of the business to be transacted.

F/25/47) Office/Depot Lease Renewal

It was **RECOMMENDED** to:

1. Renew the lease as per the Heads of Terms, for 5 years with effect from 11th December 2025 with an annual break clause for the tenant;
2. Recharge telecommunications cost to Cornwall Council as outlined in the report in accordance with the existing lease dated 11th December 2018;
3. Explore independent options before a commitment is made to new premises on the Penwinnick Road site.

It was **RESOLVED** to return to open session.

F/25/48) Dates of next meeting

It was noted that the next meeting of the Finance and General Purposes Committee is due to take place on 16th February 2026.

The meeting closed at 7.32pm.

ST AUSTELL TOWN COUNCIL

FINANCE AND GENERAL PURPOSES COMMITTEE

16th FEBRUARY 2026

INSURANCE RENEWAL

1. PURPOSE OF REPORT

To agree to invoke a one year extension clause to the Council's current insurance policy.

2. LEGAL AND RISK MANAGEMENT ISSUES

The Council is required to have suitable risk management arrangements and insurances in place and to review these from time to time. The Council's current insurance policy has a clause within it which permits a one year extension.

3. RESOURCE ISSUES

As set out in this report.

4. EQUALITIES ISSUES

None.

5. ENVIRONMENT ISSUES

None directly.

6. RECOMMENDATIONS

It is recommended that the Committee:

1. Approves a one year extension to the existing insurance policy at a cost of £12,304.09.

Background

The Council went out to tender for insurance cover in 2023 and appointed Zurich Municipal based on price and experience for 3 years. The policy awarded provided a clause permitting a one year extension.

New reinstatement valuations have been sought for Priory toilets, Poltair Café and The House which reflect increased building costs. The new valuations are reflected in the quotations received.

The following options have been offered:

1 year extension £12,304.09

New 1 Year Policy £12,959.56

New 3 year Long term agreement £11,711.75

Before accepting a 3-year agreement it would be sensible to test the market as insurance costs fluctuate. To buy time to allow this it is recommended that the Council should accept the one year extension option and seek tenders for up to 3 years with effect from 1st April 2027.

DAVID POOLEY
TOWN CLERK

ST AUSTELL TOWN COUNCIL

FINANCE AND GENERAL PURPOSES COMMITTEE

16th FEBRUARY 2026

CCTV FUNDING

1. PURPOSE OF REPORT

To advise Members of the offer of a grant from the Office of the Police and Crime Commissioner for the expansion of the Council's CCTV camera system.

2. LEGAL AND RISK MANAGEMENT ISSUES

The funding offered can only be used for the expansion of the CCTV system. The area around Polkyth is deemed a high risk area with a youth club, a wellbeing centre under construction, the leisure centre and the Health Hub being developed and has been identified as a priority for further CCTV cameras.

The siting, control and use of CCTV cameras is highly-regulated and requires trained operatives and compliance with legislation governing surveillance and evidence gathering. Privacy impact assessments will be undertaken as part of camera placement.

3. RESOURCE ISSUES

A grant of £10,000 has been offered towards an investment of £21,700 for 3 additional fixed CCTV cameras and a redeployable or mobile CCTV camera.

4. EQUALITY ISSUES

CCTV cameras can provide a significant deterrent against crime and offer protection to vulnerable people.

5. ENVIRONMENTAL ISSUES

CCTV cameras only use small amounts of electricity and have a negligible impact on the environment. They aid the efficient and safe use of police and security resources.

6. RECOMMENDATIONS

It is recommended that the Clerk be authorised to consult organisations based in the Polkyth area and, subject to the outcome of this exercise, acquire CCTV cameras to a value of approximately £21,700.

Background

In October 2025, the Office of the Police and Crime Commissioner (OPCC) invited expressions of interest for grants up to £10,000 for the expansion of CCTV camera systems. The timescales for submitting a bid were tight so an application was completed for a grant towards the cost of 3 CCTV cameras for the Polkyth area and one redeployable or mobile CCTV camera.

The Polkyth area is not currently covered by the Council's CCTV system and has been identified as a high risk area with the leisure centre, The House youth centre and the proposed opening of a wellbeing centre and the Health Hub.

On the 23rd December 2025 the OPCC formally offered a grant of £10,000 towards the purchase of new CCTV cameras with an estimated cost of £21,700.

It is recommended that the Clerk be authorised to consult organisations based in the Polkyth area and, subject to the outcome of this exercise and there being no technical barriers to connecting further cameras to the existing system, acquire CCTV cameras to a value of approximately £21,700.

DAVID POOLEY
TOWN CLERK

ST AUSTELL TOWN COUNCIL

FINANCE AND GENERAL PURPOSES COMMITTEE

16th FEBRUARY 2026

BUDGET MONITORING REPORT

1. PURPOSE OF REPORT

To provide Members with an update on income and expenditure to the 31st January 2026 and a copy of the Council's latest bank reconciliation statements.

2. LEGAL AND RISK MANAGEMENT ISSUES

It is a legal requirement for the Town Council to set a budget annually and it is good practice to monitor that budget at regular intervals. The Town Clerk monitors budgets monthly and provides regular budget monitoring reports to the Finance and General Purposes Committee. It is part of the remit of the Finance and General Purposes Committee to monitor and manage budgets on behalf of the Town Council.

3. RESOURCE ISSUES

None outside of existing budgets.

4. EQUALITIES ISSUES

None.

5. ENVIRONMENTAL ISSUES

None.

6. RECOMMENDATIONS

It is recommended that Members note the attached budget monitoring reports and bank reconciliation statement.

The budget variance report for January 2026 and the financial year to the 31st January 2026 is attached for information. After allowing

for the Town Centre Revitalisation projects which are to be largely funded from grant monies the income and expenditure are within acceptable limits.

Significant variances are explained below:

- **Car Park income** – more income than anticipated
- **Interest income** – higher interest rates and balances
- **Other grants and contributions** – Shared Prosperity Fund and Town Vitality Fund grants
- **Other income** – insurance claims and sale of vehicle
- **Contract payments** – seasonal CCTV monitoring costs and new cameras
- **Election costs** – reduced recharge from Cornwall Council
- **Miscellaneous expenses** – Town centre projects largely grant funded
- **Other transport/plant expenses** – new vehicle.
- **Play equipment** – Projects not commenced
- **Rates** – likely to be slightly above budget
- **Salaries and Wages** – staff vacancies

DAVID POOLEY - TOWN CLERK

Budget Variance

St Austell Town Council

For the month ended 31 January 2026

	JAN 2026	JAN 2026	VARIANCE	VARIANCE %	APR 2025-JAN	APR 2025-JAN	VARIANCE	VARIANCE %
		OVERALL BUDGET			2026	2026 OVERALL BUDGET		
Trading Income								
Car Park Income	20,917.99	20,000.00	917.99 ↑	4.59% ↑	234,028.83	200,000.00	34,028.83 ↑	17.01% ↑
Interest Income	4,096.76	3,000.00	1,096.76 ↑	36.56% ↑	39,178.49	30,000.00	9,178.49 ↑	30.59% ↑
Library Income	522.83	467.00	55.83 ↑	11.96% ↑	5,745.65	4,670.00	1,075.65 ↑	23.03% ↑
Other Grants and Contributions	25.00	.	25.00 ↑	-	90,764.44	.	90,764.44 ↑	-
Other Income	39.61	202.00	(162.39) ↓	-80.39% ↓	32,189.93	2,020.00	30,169.93 ↑	1,493.56% ↑
Precept Payments	.	.	.	-	1,301,100.00	1,301,100.00	.	-
Public Convenience Charges	66.55	221.00	(154.45) ↓	-69.89% ↓	1,417.89	2,210.00	(792.11) ↓	-35.84% ↓
Rent Received	.	868.00	(868.00) ↓	-100.00% ↓	7,885.00	8,680.00	(795.00) ↓	-9.16% ↓
Total Trading Income	25,668.74	24,758.00	910.74	3.68%	1,712,310.23	1,548,680.00	163,630.23	10.57%
Gross Profit	25,668.74	24,758.00	910.74	3.68%	1,712,310.23	1,548,680.00	163,630.23	10.57%
Operating Expenses								
Books and Publications	.	.	.	-	148.50	150.00	(1.50) ↓	-1.00% ↓
Cleaning & Domestic Supplies	1,802.18	1,753.00	49.18 ↑	2.81% ↑	18,311.38	17,530.00	781.38 ↑	4.46% ↑
Contract Hire and Operating Leases	35.00	46.00	(11.00) ↓	-23.91% ↓	1,576.65	460.00	1,116.65 ↑	242.75% ↑
Contract Payments	6,466.66	14,085.00	(7,618.34) ↓	-54.09% ↓	149,905.57	140,850.00	9,055.57 ↑	6.43% ↑
Election Expenses	.	.	.	-	7,943.56	35,000.00	(27,056.44) ↓	-77.30% ↓

Budget Variance

	JAN 2026	JAN 2025 OVERALL BUDGET	VARIANCE	VARIANCE %	APR 2025-JAN 2026	APR 2025-JAN 2026 OVERALL BUDGET	VARIANCE	VARIANCE %
Electricity	4,336.27	1,642.00	2,694.27 ↑	164.08% ↑	13,025.75	16,420.00	(3,394.25) ↓	-20.67% ↓
Fuel	642.60	1,030.00	(387.40) ↓	-37.61% ↓	9,502.03	10,300.00	(797.97) ↓	-7.75% ↓
Gas	145.39	602.00	(456.61) ↓	-75.85% ↓	1,871.34	6,020.00	(4,148.66) ↓	-68.91% ↓
Grounds Maintenance Supplies	1,817.50	2,146.00	(328.50) ↓	-15.31% ↓	25,153.57	21,460.00	3,693.57 ↑	17.21% ↑
Insurances	-	-	-	-	12,156.99	11,920.00	236.99 ↑	1.99% ↑
IT / Communications	1,060.06	1,968.00	(907.94) ↓	-46.14% ↓	20,975.28	19,680.00	1,295.28 ↑	6.58% ↑
Mayors Allowances	-	62.00	(62.00) ↓	-100.00% ↓	100.00	620.00	(520.00) ↓	-83.87% ↓
Members Allowance	90.00	-	90.00 ↑	-	372.59	-	372.59 ↑	-
Miscellaneous Expenses	7,826.32	7,638.00	188.32 ↑	2.47% ↑	251,829.94	76,380.00	175,449.94 ↑	229.71% ↑
Miscellaneous Grants	7,500.00	6,160.00	1,340.00 ↑	21.75% ↑	57,804.00	61,600.00	(3,796.00) ↓	-6.16% ↓
Office Supplies	345.15	229.00	116.15 ↑	50.72% ↑	2,537.26	2,290.00	247.26 ↑	10.80% ↑
Other Transport/plant expenses	41.25	2,321.00	(2,279.75) ↓	-98.22% ↓	27,613.50	23,210.00	4,403.50 ↑	18.97% ↑
Play Equipment	-	4,167.00	(4,167.00) ↓	-100.00% ↓	7,231.71	41,670.00	(34,438.29) ↓	-82.65% ↓
Printing and Stationery	123.34	363.00	(239.66) ↓	-66.02% ↓	4,442.50	3,630.00	812.50 ↑	22.38% ↑
Protective Clothing	-	238.00	(238.00) ↓	-100.00% ↓	2,291.10	2,380.00	(88.90) ↓	-3.74% ↓
Publicity	225.00	158.00	67.00 ↑	42.41% ↑	1,903.72	1,580.00	323.72 ↑	20.49% ↑
Rates	5,394.00	3,799.00	1,595.00 ↑	41.98% ↑	54,444.10	37,990.00	16,454.10 ↑	43.31% ↑
Recruitment	-	108.00	(108.00) ↓	-100.00% ↓	105.85	1,080.00	(974.15) ↓	-90.20% ↓
Rent / Room Hire	972.67	850.00	122.67 ↑	14.43% ↑	4,160.00	8,500.00	(4,340.00) ↓	-51.06% ↓
Repairs / Maintenance Premises	2,586.29	3,580.00	(993.71) ↓	-27.76% ↓	34,069.48	35,800.00	(1,730.52) ↓	-4.83% ↓

14

ST AUSTELL TOWN COUNCIL

BANK RECONCILIATION AS AT:

31.1.26

	£	£
Business Current Account		56,631.60
Mayor's Charity Account		979.68
Business Direct Reserve Account		216,324.50
Treasury Deposit Account		203,361.02
Petty Cash		243.00
Library Float		100.00
Total in Bank		<u>477,639.80</u>

Total Unpresented Cheques		<u>0.00</u>
		477,639.80

Outstanding receipts		
Unprocessed DD		
		<u>0.00</u>
		477,639.80

Accounting System Bank Balance:

Opening Bank Balance		114,995.35
Expenditure to date		279,796.12
Income to date		316,061.57
		<u>477,639.80</u>

Accounting System Receipt not recorded

Accounting System Bank Balance	<u>477,639.80</u>	0.00 balanced
---------------------------------------	-------------------	------------------

Note:

Attach Accounting Statement and remember to adjust for the Outstanding Accounting System Entries after balancing.

Reconciliation Completed: Date: 2.2.26

Reviewed: Date: 2.2.26

ST AUSTELL TOWN COUNCIL

FINANCE AND GENERAL PURPOSES COMMITTEE

16th FEBRUARY 2026

INFORMATION TECHNOLOGY POLICY

1. PURPOSE OF REPORT

To consider and approve an Information Technology (IT) Policy.

2. LEGAL AND RISK MANAGEMENT ISSUES

It is a good practice to ensure that the Council maintains robust IT systems and procedures to safeguard data. The Council is subject to the Data Protection Act and the General Data Protection Regulation. Key staff have completed training in this legislation and the Council has Data Protection, Document Retention and Information Policies. Independent IT support services are employed to ensure the security of the Council's IT systems and data.

3. RESOURCE ISSUES

None outside of existing budgets.

4. EQUALITIES ISSUES

None.

5. ENVIRONMENTAL ISSUES

None.

6. RECOMMENDATIONS

It is recommended that Members note and approve the attached policy.

The National Association of Local Councils (NALC) has issued a draft Information Technology Policy which it recommends that all local councils adopt. The attached is based on the template provided. Members are asked to review and approve the attached policy.

The Town Council employs Objective IT Services to maintain its IT systems and undertake regular back-ups of data. Firewalls are maintained, data encryption is used and regular monitoring of security is undertaken on behalf of the Council.

The Town Council retains minimal personal data and complies with the Data Protection Act and the General Data Protection Regulation.

DAVID POOLEY - TOWN CLERK



St Austell Town Council

Information Technology Policy

Purpose of the IT Policy	2
Monitoring of IT use	2
Scope of this policy	2
Computer use	2
Equipment	3
Health and safety	6
Password and authentication policy	6
Monitoring	8
Remote working	9
Email	10
Use of the internet	10
Use of social media	11

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer use

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the Town Clerk). Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

1.1.2 All councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

1.1.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.1.5 All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

1.1.6 Equipment should not be dismantled or reassembled without seeking advice.

1.1.7 Staff and other authorised users are not to purchase any computer or mobile equipment (including software) unless previously authorised.

1.1.8 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Town Clerk.

1.1.9 The council has a number of wireless networks. Using a portable device to make personal Wi-Fi hot spots which bypass existing Wi-Fi is not allowed.

1.1.10 Any faults or necessary repairs must be reported to the Town Clerk.

Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

2.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disabled or removed.

2.1.5 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018. The Council will adopt MFA where possible.

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the Town Clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first £200 of the loss/damage.

2.1.7 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior written permission of the Town Clerk. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.8 Under no circumstances should any non public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.1.9 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Town Clerk.

2.2 Use of own devices

2.2.1 Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems during working hours, unless this has been authorised by the employee's line manager. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.

2.2.2 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's SharePoint account or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems will not normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2.3 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties must be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.4 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). For Workers or Contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

2.2.5 In cases of legal proceedings against the council, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

2.2.6 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.7 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a 6-digit pin or a strong password to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 3 failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 15 minutes;
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email);
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible;
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the Town Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.8 Personal data relating to councillors, staff, and other authorised users, associates, residents or external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.2.9 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

2.2.10 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

2.2.11 Councillors, staff, and other authorised users who open any attachments containing sensitive data should ensure that any cached copies are deleted immediately after use. The Town Clerk will provide assistance or training in doing this if needed. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

2.2.12 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

2.2.13 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow the Town Clerk access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.14 Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and safety

3.1.1 Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

3.1.2 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the council's health and safety policy.

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to their line manager.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Town Clerk.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The council recommends following the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of

verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: [NCSC Password Guidance](#)

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Town Clerk, in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass) or locked in a secure safe.

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorized passwords will be treated as a security incident.

4.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider is responsible for:

- Managing system/service credentials.

- Enforcing password policies. Auditing and monitoring password-related security practices.

Monitoring

5.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.1.5 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

5.1.6 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors and IT providers/staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.1.8 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

5.1.9 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.1.10 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

5.1.11 The council has software and systems in place that can monitor and record all internet usage. A daily log is kept of all activity, which details the names of all websites accessed, along with the date and time of access, by individual staff, and other authorised users. Records of internet use and sites visited will normally be retained for a period of six months.

5.1.12 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any

time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.1.13 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.14 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

Remote working

6.1.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home or at a premises or any other different venue), as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the device does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- all electronic files should be password protected and the data saved to the council's system/services when accessible;
- papers, files or computer equipment must not be left unattended at a premises unless arrangements have been made with a responsible person for them to be kept in a locked room or cabinet if they are to be left unattended at any time;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

6.1.2 Those issued with a 'dongle' to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of internet access can be very high. Dongles should therefore be used for essential council purposes only, especially if abroad.

6.1.3 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1.2 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the Town Clerk rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

7.1.5 Email messages sent on the council's account should be for council use only. Personal communications are permitted provided they do not encroach upon working time or interrupt council business in any way. Employees and other authorised users are asked to restrict their personal use to official lunch breaks or before or after working hours, and to use their personal email accounts, rather than council addresses.

Use of the Internet

8.1 Copyright

8.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Town Clerk if unsure about anything.

8.2 Trademarks, links and data protection

8.2.1 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the Town Clerk.

8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which is located on the Council's website.

8.3 Accuracy of information

8.3.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

Use of social media

9.1.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

9.1.2 Personal use of social networking/media and chat sites is not permitted during working hours.

9.1.3 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be

interpreted as being associated with the council, or if remarks about external stakeholders could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

9.1.4 To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

- Contacts from any of the council's databases should not be downloaded and connected with LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee who is developing a site or writing a blog that will mention the council, must inform the clerk that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff, and other authorised users to be respectful about the council and its current or potential employees, councillors, clerks, and authorised users and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the council. Additionally, photos, videos, or audio recordings must not be taken on council premises without explicit permission
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with external stakeholders should not take place on any social networking sites, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors, staff, and other authorised persons, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their

permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users, anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.

- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members' Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council or its councillors, staff, and other authorised users, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the Town Clerk or Mayor.
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff, or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

9.1.5 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

9.1.6 It is important to note that external stakeholders contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data including external stakeholders contact details from any personal device/equipment.

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use by staff may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

ST AUSTELL TOWN COUNCIL

FINANCE AND GENERAL PURPOSES COMMITTEE

16th FEBRUARY 2026

RISK MANAGEMENT

1. PURPOSE OF REPORT

To approve an updated Risk Management Strategy and Strategic Risk Register (e-mailed separately) which are required as part of the annual internal audit.

2. LEGAL AND RISK MANAGEMENT ISSUES

The Council is required as part of its governance arrangements to have suitable risk management processes in place and to review these processes from time to time. The nature and scale of risks experienced by the Town Council is changing as services and assets are devolved from Cornwall Council.

3. RESOURCE ISSUES

None outside of existing budgets.

4. EQUALITIES ISSUES

Equality Impact Assessments are undertaken as and when appropriate as part of the Council's Risk Management process.

5. ENVIRONMENT ISSUES

The Council has declared a Climate Emergency and has committed to improving its environmental impact.

6. RECOMMENDATIONS

It is recommended that the Committee:

1. Approves the updated Risk Management Strategy (Appendix 1) and Strategic Risk Register (e-mailed separately).

DAVID POOLEY
TOWN CLERK



ST AUSTELL TOWN COUNCIL

RISK MANAGEMENT STRATEGY

1. Introduction

1.1 This document forms the Council's Risk Management Strategy. It sets out:

- What is meant by risk management;
- Why the Council needs a risk management strategy;
- The philosophy of the Council's risk management;
- An overview of the methodology to be adopted and its links with existing processes;
- A summary of the implementation timetable;
- An outline of the associated roles of Elected Members and officers; and
- A summary of future monitoring and reporting lines for risk management.

1.2 The objectives of this strategy are to:

- Further develop risk management and raise its profile across the Council;
- Integrate risk management into the culture of the organisation;
- Embed risk management through the ownership and management of risk as part of all decision-making processes; and
- Manage risk in accordance with best practice.

2 What is Risk Management?

2.1 *'Risk is the threat that an event or action will adversely affect an organisation's ability to achieve its objectives and to 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.'* Audit Commission, *Worth the Risk: Improving Risk Management in Local Government*, (2001: 5).

2.2 Risk management is an essential feature of good governance. An organisation that manages risk well is more likely to achieve its objectives. It is vital to recognise that risk management is not simply about health and safety but applies to all aspects of the Council's work.

2.3 Risks can be classified into various types but it is important to recognise that for all categories the direct financial losses may have less impact than the indirect costs such as disruption of normal working. The examples below are not exhaustive:

2.3.1 **Strategic Risk** - long-term adverse impacts from poor decision-making or poor implementation. Risks damage to the reputation of the Council, loss of public confidence, in a worse case scenario Government Intervention.

- 2.3.2 Compliance Risk** - failure to comply with legislation, or laid down procedures or the lack of documentation to prove compliance. Risks exposure to prosecution, judicial review, employment tribunals, inability to enforce contracts.
- 2.3.3 Financial Risk** - fraud and corruption, waste, excess demand for services, bad debts. Risk of additional audit investigation, objection to accounts, reduced service delivery, dramatically increased Council tax levels/impact on Council reserves.
- 2.3.4 Operating Risk** - failure to deliver services effectively, malfunctioning equipment, hazards to service users, the general public or staff, damage to property. Risk of insurance claims, higher insurance premiums, lengthy recovery processes.
- 2.3.5 Reputational Risk** – damage to reputation through the actions or inaction of officers and/or members.
- 2.4** Not all of these risks are insurable and for some the premiums may not be cost-effective. Even where insurance is available, money may not be an adequate recompense. The emphasis should always be on eliminating or reducing risk, before costly steps to transfer risk to another party are considered.
- 2.5** Risk is not restricted to potential threats but can be connected with opportunities. Good risk management can facilitate proactive, rather than merely defensive, responses. Measures to manage adverse risks are likely to help with managing positive ones.

3. Why does the Council need a Risk Management Strategy?

- 3.1** Risk management will strengthen the ability of the Council to achieve its objectives and enhance the value of services provided.
- 3.2** The Risk Management Strategy will help to ensure that all Committees across the Council have an understanding of 'risk' and that the Council adopts a uniform approach to identifying and prioritising risks. This should in turn lead to conscious choices as to the most appropriate method of dealing with each risk, be it elimination, reduction, transfer or acceptance.
- 3.3** There is an Audit requirement under the Accounts and Audit Regulations 2015 (SI 2015/234) to establish and maintain a systematic strategy, framework and process for managing risk. Risks and their control will be collated in a Risk Register. A statement about the system of internal control and the management of risk will be included as part of the Annual Statement of Accounts.

4. What is the Council's Philosophy on Risk Management?

4.1 Risk Management Policy Statement

St Austell Town Council recognises that, in addition to its statutory duties, there are cogent moral and economic reasons to take all practicable and reasonable measures to safeguard people and the natural and built environments. Whilst it is acknowledged that risk cannot be totally eliminated it is accepted that much can be done to reduce the extent of injury, damage and financial loss. Therefore, St Austell

Town Council is committed to identifying, reducing or eliminating the risks to both people and the natural and built environments.

The Council will carry insurance in such amounts and in respect of such perils as will provide protection against significant losses, where insurance is required by law or contract and in other circumstances where risks are insurable and premiums cost-effective.

The Council will seek to embed effective risk management into its culture, processes and structure to ensure that opportunities are maximised.

5. What is the Risk Management Process?

5.1 Implementing the Strategy involves identifying, analysing, prioritising, managing and monitoring risks.

5.2 Risk Identification – Identifying and understanding the hazards and risks facing the Council is crucial if informed decisions are to be made about policies or service delivery methods. The risks associated with these decisions can then be effectively managed. All risks identified will be recorded in the Council's Risk Register.

5.3 Risk Analysis – Once risks have been identified they need to be systematically and accurately assessed using proven techniques. Analysis should make full use of any available data on the potential frequency of events and their consequences. If a risk is seen to be unacceptable, then steps need to be taken to control it or respond to it.

5.4 Risk Prioritisation - An assessment should be undertaken of the impact or consequence and likelihood of risks occurring, with impact and likelihood being scored on a scale from 1 to 5 with 1 being low and 5 high.

The scores for impact and likelihood are multiplied together. Risks scoring 12 and above will be subject to detailed consideration and preparation of a contingency/action plan to appropriately control the risk.

5.5 Risk Control – Risk control is the process of taking action to minimise the likelihood of the risk event occurring and/or reducing the severity of the consequences should it occur. Typically, risk control requires the identification and implementation of revised operating procedures, but in exceptional cases more drastic action will be required to reduce the risk to an acceptable level.

Options for control include:

5.5.1 Elimination – the circumstances from which the risk arises are ceased so that the risk no longer exists;

5.5.2 Reduction – loss control measures are implemented to reduce the impact/likelihood of the risk occurring;

5.5.3 Transfer – the financial impact is passed to others e.g. by revising contractual terms;

- 5.5.4 Sharing** the risk with another party;
- 5.5.5 Insuring** against some or all of the risk to mitigate financial impact; or
- 5.5.6 Acceptance** – documenting a conscious decision after assessment of areas where the Council accepts or tolerates risk.
- 5.6 Risk Register** – a register of strategic risks will be collated and an additional system of risk assessments will be maintained for all identified operational risks. Each will be reviewed at least annually.
- 5.7 Risk Monitoring** – The risk management process does not finish with putting any risk control procedures in place. Their effectiveness in controlling risk must be monitored and reviewed. It is also important to assess whether the nature of any risk has changed over time.

The information generated from applying the risk management process will help to ensure that risks can be avoided or minimised in the future. It will also inform judgements on the nature and extent of insurance cover and the balance to be reached between self-insurance and external protection.

6. How will it feed into the Council’s existing policies?

- 6.1** All reports to Council or Committees will consider risk management issues. Initial identification of strategic and operational risks will be by officers who will compile lists of strategic and operational risks. Regular reports on risk management will be presented to the Finance and General Purposes Committee for consideration.
- 6.2 Best Practice** – the current economic climate means that risk management is now more important than ever, it is important for the Council to reassess its objectives and the threats to achieving these objectives. The Council will build risk management procedures into the way that it operates as part of a commitment to quality and continuous service improvement
- 6.4 Localism and Partnership Working** – the Council enters into contracts and partnerships with organisations from the public, private, voluntary and community sectors. Some of these organisations may not have the same sensitivities to the risks that the Council sees as important. Part of the process of setting up future partnerships will be to ensure that all relevant risks are identified and that appropriate control mechanisms are built into the management arrangements for the partnership.

7. Roles and Responsibilities

- 7.1** It is important that risk management becomes embedded into the everyday culture and performance management process of the Council. The roles and responsibilities set out below, are designed to ensure that risk is managed effectively right across the Council and its operations, and responsibility for risk is located in the right place. Those who best know the risks to a particular service or function are those responsible for it. The process must be driven by members but must also involve officers.

7.2 Elected Members – risk management is seen as a key part of the Elected Member’s stewardship role and there is an expectation that Elected Members will lead and monitor the approach adopted.

This will include:

- Approval of the Risk Management Strategy;
- Analysis of key risks in reports on major projects, ensuring that all future projects and services undertaken are adequately risk managed;
- Consideration, and if appropriate, endorsement of the Annual Statement of Internal Control; and
- Assessment of risks whilst setting the budget, including any bids for resources to tackle specific issues.

7.3 Town Clerk and Responsible Finance Officer – will act as the Lead Officer on Risk Management, overseeing the implementation of the detail of the Risk Management Strategy.

The Town Clerk will:

- provide advice as to the legality of policy and service delivery choices;
- provide advice on the implications of potential service actions for the Council’s corporate aims and objectives;
- update Council on the implications of new or revised legislation;
- assess and implement the Council’s insurance requirements;
- assess the financial implications of strategic policy options;
- ensure that the Financial Information System allows effective budgetary control;
- inform investment decisions made by the Council.
- assist in handling any litigation claims;
- provide advice on any human resource issues relating to strategic policy options or the risks associated with operational decisions and assist in handling cases of work-related illness or injury;
- advise on any health and safety implications of the chosen or proposed arrangements for service delivery;
- consider the environmental implications of policy and service delivery choices;
- have due regard to the Equality Act 2010 when dealing with Risk Management issues; and
- report progress to Council via the Finance and General Purposes Committee as detailed in para 8.3 below.

7.4 The Operations Manager will act as the Lead officer for Risk Management and Health and Safety matters associated with the operational services of the Council.

7.5 The Deputy Town Clerk will act as the Lead Officer for Risk Management in connection with employees’ health and wellbeing and human resources issues.

7.6 Employees – will undertake their job within risk management guidelines ensuring that the skills and knowledge passed to them are used effectively. All employees will maintain an awareness of the impact and costs of risks and how to feed data into the formal process. They will work to control risks or threats within their jobs, monitor progress and report on job related risks to the Clerk or their line manager.

- 7.7 Role of Internal Audit** – the Internal Auditor provides an important scrutiny role carrying out audits to provide independent assurance to the Finance and General Purposes Committee and Council that the necessary risk management systems are in place and all significant business risks are being managed effectively.

Internal Audit assists the Council in identifying both its financial and operational risks and seeks to assist the Council in developing and implementing proper arrangements to manage them, including adequate and effective systems of internal control to reduce or eliminate the likelihood of errors or fraud.

The Internal Audit Report, and any recommendations contained within it, will help to shape the Annual Statement of Internal Control.

- 7.8 Training** – Risk Management training will be provided to Elected Members, and key staff. The aim will be to ensure that both Elected Members and staff have the skills necessary to identify, evaluate and control the risks associated with the services they provide.

In addition to the roles and responsibilities set out above, the Council is keen to promote an environment within which individuals/groups are encouraged to report adverse incidents promptly and openly. To assist with this aspect, the Council will develop and maintain an Anti-Fraud and Corruption Policy, a Confidential Reporting ('whistleblowing') Policy, Employee Handbooks and Health and Safety Handbooks.

8 Future Monitoring

- 8.1 Review of Risk Management Strategy** - This Strategy will be reviewed on a regular basis as part of the Council's continuing review of its Policy Documents, Standing Orders and Financial Regulations. Recommendations for change will be reported to the Finance and General Purposes Committee.

- 8.2** Once the initial work to establish Risk Registers has been completed, it is crucial that the information is regularly reviewed and updated. New risks will emerge and need to be controlled. Feedback from Internal and External Audit can identify areas for improvement, as can the sharing of best practice via professional bodies such as the National Association of Local Councils.

- 8.3 Reporting on Progress** – The Town Clerk will present an annual report to the Finance and General Purposes Committee detailing progress on risk management over the year and providing a summary of the Risk Register(s) and control assurance statements.

9. Conclusion

- 9.1** The adoption of a sound risk management approach should achieve many benefits for the Council. It will assist in demonstrating that the Council is committed to continuous service improvement and demonstrating effective corporate governance.

10. Freedom of Information

- 10.1.** In accordance with the Freedom of Information Act 2000, this Document will be posted on the Council's Website and copies of this document and the Risk Register will be available for inspection on deposit in the Council Office.

**ST AUSTELL TOWN COUNCIL
FINANCE AND GENERAL PURPOSES COMMITTEE**

16th FEBRUARY 2026

TREASURY MANAGEMENT

1. PURPOSE OF REPORT

To provide Members with a breakdown of the Council's Treasury Management activity during the 2025/26 financial year and re-confirm the Council's Treasury Management Strategy.

2. LEGAL AND RISK MANAGEMENT ISSUES

Borrowing and investments by Parish and Town Councils are governed by the Local Government Act 2003. Furthermore, the Town Clerk, by virtue of being a Member of the Chartered Institute of Public Finance and Accountancy (CIPFA) is required to comply with guidance issued by that body. CIPFA has issued a Code of Practice and cross sectoral guidance notes relating to Treasury Management. This strategy complies with the legal and professional guidance.

The Town Council is outside of the scope of the Financial Services Compensation Scheme (FSCS). The protection of up to £120,000 for each bank account does not therefore apply to the Council.

The Clerk is authorised to manage investments on behalf of the Council in accordance with the Council's Treasury Management Strategy. This authorises the Clerk to transfer up to £250,000 between bank accounts.

3. RESOURCE ISSUES

None outside of existing budgets. The strategy assumes a low risk approach to investment which means that investment income will be lower than might be achieved through a higher risk strategy. It however does mean that the Council's reserves are safeguarded.

To the end of January, interest received on investments during the 2025/26 financial year stands at £39,178.49.

4. EQUALITY ISSUES

None.

5. ENVIRONMENTAL ISSUES

The Town Council invests with Cornwall Council who are actively working towards net zero carbon status and have ethical investment policies. It also maintains deposit and investment accounts with the Nat West Bank.

6. RECOMMENDATIONS

It is recommended that the report be noted and the Treasury Management Strategy for 2026/27 be approved.

DAVID POOLEY
TOWN CLERK

Summary of Investments

Investments

<u>Date</u>	<u>Investment</u>	<u>Amount</u>
As at 31.1.26	Business Reserve Account (Natwest)	£216,324.50
As at 31.1.26	Treasury Management Account (NatWest)	£203,361.02
As at 31.1.26	Variable Rate Deposit Account Cornwall Council	£978,973.84

Interest Received

<u>Date</u>	<u>Amount</u> <u>£</u>
2024/25	52,082.18
2025/26 to date (excluding accrual)	39,178.49

47



ST AUSTELL TOWN COUNCIL

TREASURY MANAGEMENT STRATEGY

1

Overview

This document gives guidance on borrowing and investments by St Austell Town Council in accordance with 'the Local Government Act 2003'. It highlights that the Council is committed to professional Treasury Management practices to ensure that:

- Capital expenditure plans are affordable.
- All external borrowing and other long-term liabilities are within prudent and sustainable levels, and
- Treasury Management decisions are taken in accordance with good professional practice.

The CIPFA Treasury Management Code of Practice defines Treasury Management as:

'The management of the Council's cashflows, its banking, money market and capital market transactions; the effective control of the risks associated with those activities; and the pursuit of optimum performance consistent with those risks.'

2

INVESTMENT STRATEGY

2.1

Introduction

The Council acknowledges the importance of prudently investing the temporarily surplus funds held on behalf of the community.

This Strategy complies with the requirements set out in the Department for Housing, Communities and Local Government *Guidance on Local Government Investments* and Chartered Institute of Public Finance and Accountancy's *Treasury Management in Public Services: Code of Practice and Cross Sectoral Guidance Notes* and takes account of Section 15(1)(a) of the Local Government Act 2003.

2.2

Investment Objectives

In accordance with Section 15(1) of the 2003 Act, the Council will *have regard to (a) such guidance as the Secretary of State may issue, and (b) to such other guidance as the Secretary of State may by regulations specify.*

The Council's investment priorities are to maintain the security of reserves and liquidity of its investments. As far as possible the Council will seek to invest only in organisations which operate in an ethical and environmentally sympathetic manner.

The Council will aim to achieve the optimum return on its investments commensurate with proper levels of security and liquidity.

All investments will be made in sterling.

The Department for Levelling Up, Housing and Communities maintains that borrowing of monies purely to invest, or to lend and make a return, is unlawful and this Council will not engage in such activity.

Where external investment managers are used, they will be contractually required to comply with the Strategy.

2.3 Specified Investments

Specified Investments are those offering high security and high liquidity, made in sterling and which mature in no more than a year. Such short-term investments made with the UK Government or a local authority or town or parish council will automatically be Specified Investments.

For the prudent management of its treasury balances, maintaining sufficient levels of security and liquidity, St Austell Town Council will use:

- Deposits with banks, building societies, local authorities or other public authorities
- The debt management agency of HM Government
- Cornwall Council variable deposit scheme
- CCLA Public Sector Deposit Fund.

2.4 Non-Specified Investments

These investments have greater potential risk – examples include investment in the money market, stocks and shares.

Given the unpredictability and uncertainties surrounding such investments, St Austell Town Council will not use this type of investment.

2.5 Liquidity of Investments

The Town Clerk, as Responsible Finance Officer, will determine the maximum periods for which funds may prudently be committed so as not to compromise liquidity and may transfer up to £250,000 between bank accounts as appropriate to take advantage of interest bearing deposit accounts while maintaining sufficient liquidity. Larger investments should be in accordance with this strategy and only be undertaken following consultation with the Chair and Vice Chair of the Finance and General Purposes Committee. Such investments will be subject to two signatures as with all payments.

Investments will be regarded as commencing on the date the commitment to invest is entered into, rather than the date on which the funds are paid over to the counterparty.

2.6 Long Term Investments

Long term investments are defined in the Guidance as greater than 36 months.

The Council does not currently hold any long-term investments.

No long-term investments are currently envisaged.

2.7 End of Year Investment Report

Investment forecasts for the coming financial year were accounted for when the budget was prepared. At the end of the financial year, the Town Clerk will report on investment activity to the Finance and General Purposes Committee.

3 EXTERNAL BORROWING STRATEGY

3.1 Introduction

The Council acknowledges the importance of borrowing funds and the financial impact on the Council and the local community. The Council will agree borrowing for specific capital projects (as defined in section 16 of the 2003 Act) and gain approval for borrowing by sending an application to the National Association of Local Councils (NALC). All borrowings must be approved by the full Council.

3.2 Principles

Before a council can borrow a sum of money, it must first receive an approval to borrow (loan sanction) from the Secretary of State by way of the Department for Housing, Communities and Local Government, unless it is for a temporary loan or overdraft from a bank or otherwise of sums which the council may temporarily require to meet revenue expenditure.

The process to be followed and the criteria applied in deciding whether or not approval should be forthcoming, are detailed in the Guide to Parish and Town Council Borrowing in England, jointly published by Department for Housing, Communities and Local Government and NALC.

The Council is only authorised to borrow a maximum of £500,000 in any single financial year for any single purpose.

The Council will ensure the following criteria when considering requesting a borrowing approval:

- The borrowing should be only be used for the purpose of Capital expenditure as defined by Section 16 of the Local Government Act 2003.
- The borrowing amount should not be less than £5 multiplied by the number of local government electors in the area of the Council on the first day of the current financial year (1 April)

- Any unallocated balances including, where appropriate capital receipts beyond those required for the prudent financial management of the council, should be used in the project for which the borrowing is required.
- The Council should have a realistic budget for the servicing and repayment of the debt, taking into account the future effect on the council's precept and cashflow.
- The Council must not mortgage or charge any of its property as security for money borrowed.

3.3 Interest Rates

The Council will look around for the best possible terms when borrowing but will usually use the Public Works Loan Board (PWLB).

The Council feels that the fixed term rates offered by the PWLB are relatively cheap and that PWLB loans are most likely to offer stability for the financial planning of the council.

3.4 Period of Loan

The Council will determine the period of each loan which should not exceed the period for which the expenditure is forecast to provide benefit to the Council i.e. useful life of the asset.

The maximum period will begin on the date on which the money is borrowed, and will be;

- 50 years for acquisition of, or work on or to, land, buildings, roads or structures or
- 10 years in all other cases.

3.5 Current External Borrowing

The Town Council currently has no external borrowing.

3.6 Further Anticipated External Borrowing

The Council has no plans currently to incur capital expenditure which will require a loan sanction or external borrowing.

4 Review and Amendment of Regulations

This Strategy will be reviewed annually. The Annual Strategy for the coming financial year will be prepared by the Town Clerk and presented for approval to the Finance and General Purposes Committee.

The Council reserves the right to make variations to the Strategy at any time, subject to the approval of the full Council. Any variations will be made available to the public.

5 Equality Act 2010

Copies of this document in large print (A3 Format) or larger font size, or recorded onto tape as a 'talking book' can be made available for those with sight impairment on request from the Council Office or by telephoning 01726 829859 or e-mailing david.pooley@staustell-tc.gov.uk

The Council can also arrange to provide versions in other languages.

6 Freedom of Information

In accordance with the Freedom of Information Act 2000, this Document will be posted on the Council's website.

