WHIMPLE PARISH COUNCIL
INTERNAL CONTROL CHECKLIST – QUARTER 3

The Accounts and Audit (England) Regulations 2015 aims to strengthen governance and accountability. This is done through internal control and internal audit. This is documented as:

"A relevant authority must ensure that it has a sound system of internal controls which:
a) Facilitates the effective exercise of its functions and the achievement of its aims and objectives
b) Ensures that the financial and operational management of the authority is effective
c) Includes effective arrangements for the management of risk

A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance procedures…"

Whimple Parish Council has determined that there should be a regular review (at least quarterly) of the internal controls and that this will be carried out by a Councillor that is not an authorised signatory.

This will create a written document which is submitted to the Council for approval and minuted as such.

This is in addition to the internal and external audit requirements.

Control Check	**Frequency of check**	**Documents checked and comments**
1. Proof of payments supported by approved invoices which are authorised and minuted	Quarterly	*Checked all invoices to schedule of payments and minutes of the meetings.*
2. Proof of receipts (including precept) supported by appropriate remittance advice	Quarterly	*Checked evidence of receipts, cross referenced to bank statements*
3. The cashbook is kept up to date and all receipts and payments are included	Quarterly	*Checked invoices and receipts to cashbook*
4. Monthly bank reconciliations have been completed which are supported by the cashbook and bank statements	Quarterly	*Cross referenced cashbook to bank statements and reconciliation*
5. Payments made to the Clerk are accurate and in accordance with the contract of employment and correct salary scale.	Quarterly	*Checked payments paperwork to the contract of employment and NJC salary scales. Confidential item considered at the November 2025 meeting and resolution to increase SCP of Clerk in line with contract and to pay backpay in December 2025. Backpay calculation approved as part of the payment schedule in December 2025.*

Control Check	Frequency of check	Documents checked and comments
6. Any Clerk or Councillor expense claims are completed on the claim form with invoices/receipts attached	Quarterly	*Reviewed Clerk expense claim form approved in October 2025 for 3 Land Registry Searches and stationery.* *Reviewed Cllr Dearden expense claim form approved in November 2025 for the Remembrance Wreath*
7. Check the schedule of transfers to ensure that transfer of money between bank accounts is appropriate and authorised by the Council	Quarterly	*Transfers reviewed for period of October to December 2025.*
8. The budget is being monitored by the Council during the financial year and includes all receipts and payments	Quarterly	*Budget Monitoring Reports come to the council monthly and checked those to the end of October, November and December 2025.*
9. The risk assessment is being reviewed by the Council on a regular basis and any new and emerging risks are identified	Quarterly	*Risk Assessment being considered quarterly – last considered on 20/10/25. No new risks added. Next being considered at the January 2026 meeting.*
10. That any goods/services costing above £5,000 were ordered only following consideration of three quotations	Quarterly	*Checked the quotes in Q3 2025/26 relating to the appointment of an Internal Auditor for 2025/26 (less than £5,000 but cross referenced the quotes to the report and minutes)*
11. Council minutes are signed and retained in a minute book	Quarterly	*Clerk holds a minute book for final signed minutes*
12. Standing Orders are reviewed annually, approved by Council and published on the Council website	Annually (after AGM in May)	*Not applicable in this quarter as checked in Q1*
13. Financial Regulations are reviewed annually, approved by Council and published on the Council website	Annually (after AGM in May)	*Not applicable in this quarter as checked in Q1*
14. Internal Control Statement is reviewed annually, approved by Council and published on the Council website	Annually (after AGM in May	*Not applicable in this quarter as checked in Q1*

Control Check	Frequency of check	Documents checked and comments
15. Risk Management Strategy is reviewed annually, approved by the Council and published on the Council website	Annually (after AGM in May)	*Not applicable in this quarter as checked in Q1*
16. Code of Conduct is reviewed annually, approved by the Council and published on the Council website 17.	Annually (after AGM in May)	*Not applicable in this quarter as checked in Q1*
18. Declaration of Acceptance of Office forms are signed for the role of Councillor, Chair and Vice-Chair	Chair and Vice-Chair Annually (after AGM in May) Councillors when elected or co-opted ss	*Not Checked this quarter as not relevant.*
19. That a VAT return has been completed and submitted to the HMRC to reclaim any VAT incurred by the Council in the previous financial year	Annually (by the end April)	*In Q3 the 2022/2023 VAT Reclaim was completed following the Clerk obtaining all VAT invoices. Checked 126 Reclaim form to invoices and bank statement.*
20. The Asset Register has been reviewed on an annual basis	Annually (by the end April)	*Not applicable in this quarter as being checked in Q4*
21. An annual review has taken place of the Council's insurance arrangements and adequacy of insurance cover	Annually (by the end May)	*Not applicable in this quarter as being completed in Q4*

Date of Review: _____

Reviewed by: _____

Signature: _____

Parish Clerk & RFO signature:

Presented to the Parish Council meeting on: **19 January 2026**

Resolved by the meeting at minute: _____

WHIMPLE PARISH COUNCIL – RISK ASSESSMENT

This risk assessment sits alongside the Risk Management Strategy

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Business Continuity	Risk of Council not being able to continue its business due to an unexpected or tragic circumstance	M	All files and records are kept either electronically or at the Clerks home/in a lockable filing cabinet. The Clerk makes regular back up of files. In the event of the Clerk being indisposed the Chair to contact Devon Association of Local Councils (DALC) or Society of Local Council Clerks (SLCC). Provision of a Council laptop so that records and logins for online banking/HMRC can be accessed.	Existing procedures adequate Review scope for sharing information/passwords Review contingency plans in the event of the Clerk being indisposed. Review if a Council mobile phone is needed (particularly for dual factor authentication).
	The Council is unable to access Council records if the Clerk is indisposed as the information is on their personal laptop	M		
	The Council cannot access online banking or HMRC due to two factor authentication and the Clerks personal phone number being listed	M		
Precept	The precept is not adequate to cover the Council's expenditure	L	The Council reviews the Precept requirement annually in November and presented in the December meeting. Reviews the presented budget update information including actual position and projected position to year end and estimated figures for the next financial year. With this information the Council agrees the precept amount to be requested from EDDC. This figure is submitted by the Clerk in writing by the deadline set by EDDC. The Clerk informs the Council when the monies are received. Checked via the internal control checklist completed by the councillor who is finance, internal control and risk management 'champion' and reported to Council	Existing procedures adequate
	Precept requirements are not submitted to East Devon District Council (EDDC)	L		
	Incorrect amount of Precept paid by EDDC	L		
Reserves	The Council does not have an adequate level of reserves to cover 6 months operating costs	M	The Council needs to have adequate reserves to deal with an emergency. The Council has a Reserves Policy and reviews its reserves annually following the end of the financial year.	Existing procedure adequate
	Lack of reserves to cover any budgetary shortfall	M		

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Financial Records	Inadequate records Financial irregularities	L L	The Council has Financial Regulations that set out requirements and expectations. Financial records are checked via the internal control checklist by the councillor who is finance, internal control and risk management 'champion' and reported to Council The Council has appointed an independent internal auditor to review processes The Parish Clerk is CiLCA qualified	Existing procedures adequate Review Financial Regulations annually Review Internal Control Statement annually Annual Internal Audit completed
Bank and banking	Inadequate checks Bank mistakes Loss Charges	L L L L	The Council has Financial Regulations and Internal Control Statement that set out the requirements and controls for banking, cheques and reconciliation of accounts. Two councillors required to sign off any bank payments. Monthly bank reconciliations identify and errors Banking records are checked via the internal control checklist by the councillor who is finance, internal control and risk management 'champion' and reported to Council The Council reviews its banking arrangements at least annually	Existing procedure adequate Review Financial Regulations annually Review Internal Control Statement annually Reviewing banking arrangements and signatories annually (at AGM) Internal Control checklist completed quarterly Download, save and monitor bank statements monthly
Cash and cheques	Loss through theft and dishonesty	L	The Council has Financial Regulations and Internal Control Statement that set out the requirements and controls for cash and cheques. The Council does not deal with cash and cheques as all payments are made electronically. The Council's insurance policy has a Fidelity Guarantee. Finance reports are standing items on Council agenda including payments and receipts reports and bank reconciliations. Clerk circulates the cash book and bank statement on a monthly basis and it gets signed at meetings	Existing procedure adequate Review the Financial Regulations annually Review Internal Control Statement annually Internal Control checklist completed quarterly Ensure Fidelity Insurance is adequate.

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Purchase of goods or services	Goods or service not supplied but billed Invoice incorrect Bank transfer/cheque payment not correct Unpaid invoices	L L L L	The Council has Financial Regulations that set out the requirements. At each Council meeting, the schedule of payments plus invoices is approved. Payments are processed via onlie banking by the Clerk and signed off by two councillors before being paid. Banking records are checked via the internal control checklist by the councillor who is finance, internal control and risk management 'champion' and reported to Council	Existing procedure adequate Review the Financial Regulations annually Review Internal Control Statement annually Internal Control checklist completed quarterly
Procurement process	The Council doesn't follow procurement legislation or the Financial Regulations when procuring goods or services	M	The Council has Financial Regulations that set out the requirements and procurement limits. Evidence of procurement process and quotes/tenders where appropriate	Existing procedure adequate Review the Financial Regulations annually Review Internal Control Statement annually Internal Control checklist completed quarterly
Salaries and associated costs	Salary paid incorrectly Misappropriation or fraud Wrong deductions of NIC or Tax Unpaid Tax or NIC to HMRC	L L L L	Parish Council authorises appointment of Parish Clerk. Parish Clerk has contract of employment NJC salary scales are followed Payoll administered through the HMRC Payroll software All salary payments and amounts due to the HMRC are approved by the Council and recorded in the meeting minutes Salaries paid by BACs with two councillors approving the payment Payroll records are checked via the internal control checklist by the councillor who is finance, internal control and risk management 'champion' and reported to Council	Existing procedure adequate

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Grant payable (S137)	There is no power to pay the grant Grant paid without evidence as to how it will be used or how it will benefit the local community S137 expenditure is not calculated correctly and Council overspends	L L L	All such expenditure goes through the required Council process of approval, minuted and listed accordingly if a payment is made using the S137 power of expenditure.	Existing procedure adequate Parish Councillors request a copy of S137 rules if required. Clear audit trail of the S137 amount each year
Grants receivable	Council receives a grant and doesn't spend it appropriately or fails to keep an audit trail	L	Parish Council has a grants and donations policy. All applicants must complete the grant funding application, and these are considered by the Council. One off grants (e.g. DCC Locality Budget) would be dealt with within the specifically defined terms and conditions and would be itemised explicitly in the financial information and accounts presented to the Council If grant received is for a specific purpose Council may allocate it as an earmarked reserve	Existing procedure adequate Grants and Donations Policy Grant Application form Budget monitoring reports Financial statements Information re grants recorded in the minutes of Council meetings
Employees	Loss of the Parish Clerk through resignation or being indisposed Parish Clerk is inexperienced and fails to meet the requirements of the role	L L L	In the event of the Clerk being indisposed the Chair to contact DALC or SLCC. The Parish Clerk is CiLCA qualified The Parish Clerk is provided with access to relevant training, reference books and legal advice required to undertake the role	Existing procedure adequate
Councillors	Councillors are unclear about their role and responsibilities Councillors do not follow legislation or powers and duties Councillors are not adequately trained to enable them to conduct their role effectively	L L L	Parish Clerk provides inhouse training for councillors Councillors are provided with access to relevant training, reference books and legal advice required to undertake their role Councillors follow the list of powers and duties set out	Existing procedure adequate

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Councillors interests	Councillors fail to declare pecuniary and/or personal interests Councillors fail to complete the Register of Interest form Councillors have a conflict of interest	M M L	The declaration of interests by councillors at meetings is a standing item on all agendas. Register of Interest forms should ne reviewed regularly by councillors and the Clerk notified of any changes Councillors seek advice from the Clerk or Monitoring Officer if they are unsure	Existing procedure adequate
Election costs	Financial risk to the council of an election	L/M	The risk is higher in an election year. There are no measures which can be adopted to minimise the risk of having an election as this is a legal requirement and democratic process. Council to ensure that it has enough reserves to cover any costs	Existing procedure adequate
Value Added Tax (VAT)	Re-claiming/charging	L	The Council has Financial Regulations that set out requirements regarding VAT The Parish Clerk reclaims VAT for the previous financial year annually in April VAT records and reclaim are checked via the internal control checklist by the councillor who is finance, internal control and risk management 'champion' and reported to Council	Existing procedure adequate Internal Control checklist completed quarterly
Annual Governance and Accountability Return (AGAR)	The Council fails to complete the correct paperwork within the correct timescales for the AGAR The information contained within the AGAR is incorrect or false	L L	The AGAR is completed and approved by the Council, documents subject to internal audit prior to being forwarded to the External Auditor within the required time limit.	Existing procedure adequate
Internal Audit	The acts unlawfully be not having an internal audit carried out by an appropriate and competent person	L	The Council has an internal audit on an annual basis by a person who is an appropriate and competent person The internal audit report is considered at a Council meeting and published on the Council website.	Existing procedure adequate

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Legal powers and duties	The Council acts illegally by undertaking activities that fall outside of its legal powers and duties	L	Any decisions made are considered against the list of legal powers and duties Decisions are resolved at Council meetings and recorded in the minutes. The minutes are published on the Council website	Existing procedure adequate
Agendas, minutes, notices and statutory documents	The Council fails to give the correct statutory notice period for the publication of agendas There is a lack of accuracy and/or legality	L L	Minutes and agendas are produced with the prescribed method by the Clerk and adhere to the legal requirements At least 3 days notice is given when agendas are published (taking into account any bank holidays) Agendas are published on the Council website and Parish noticeboards Draft minutes are published on the website and changed to Final once approved at the next Council meeting Business conducted at Council meetings is managed by the Chair	Existing procedure adequate
Public Liability	Risk to third party, property or individuals	L	Insurance is in place which includes £10m for public liability	Existing procedure adequate
Employer Liability	Non-compliance with employment law and risk to employees	L	Insurance is in place which includes £10m employer liability	Existing procedure adequate
Insurance	The Council doesn't have insurance or it is not adequate for its needs. Insurance provision is not regularly market tested and does not provide value for money	L L	Insurance provision is reviewed at least annually. When the Council is due to renew its insurance it is market tested with quotes from three suppliers where possible.	Existing procedure adequate
Data Protection	The Council does not meet the requirements of the Data Protection Act	L	The Council is registered with the Information Commissioner. The Council has a Data Protection Policy The Council has a Privacy Statement The Clerk is delegated at the Data Protection Officer	Existing procedure adequate

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Freedom of Information	The Council does not meeting the requirements in respect of Freedom of information	L	The Council has a Freedom of Information Policy and Model publication scheme The Clerk completes any FOI requests that come in	Existing procedure adequate
Council records – Paper	Loss of records through inappropriate destruction, loss, theft or damage (e.g. from fire or flooding) Council records are held longer than they need to be and not in accordance with the Data Protection Act	L/M	Papers records are stored at the home of the Parish Clerk and in a lockable filing cabinet at the Parish Hall. Paper records are backed up by scanning and saving them Older records including minutes books are stored in the South West Heritage Centre archives Where appropriate, paperwork with personal information is securely destroyed when appropriate Document retention guidelines are followed.	Existing procedure adequate
Council records - electronic	Loss of records through inappropriate destruction, loss, theft or damage (e.g. from fire or flooding)	L/M	Electronic records are stored on the computer at the Clerk's home. Backups of the files are taken at regular intervals and stored on a portable hard drive. Where appropriate, electronic files with personal information is securely destroyed when appropriate Document retention guidelines are followed.	Existing procedure adequate
Assets	Assets are lost or damaged There is not an accurate record of the assets held by the Parish Council	M	The Council has an asset register which is reviewed annually An annual review of assets is undertaken for insurance purposes	Existing procedure adequate
Asset Maintenance	Assets are not maintained appropriately. Assets become a hazard to members of the public	L L	All assets owned by the Council are regularly reviewed and maintained. All repairs and relevant expenditure for those repairs are authorised in accordance with the procedures of the Council.	Existing procedure adequate

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Grounds Maintenance contract	The grounds maintenance contract is not procured correctly. The contractor does not deliver the contract to the standard expected by the Council The contractor does not have appropriate public liability insurance	L L L	The Grounds Maintenance contract was market tested and quotes considered by the Council There is a contract in place between the Council and contractor Regular reviews of the contractors work will take place The contractor has provided their public liability insurance certificate	Existing procedure adequate
Allotments	Revenue/loss through poor management/ badly maintained sites	M	Regular inspections Timely maintenance interventions	
	Lack of security	M	Regular inspections Feedback from allotment tenants	
	Damage/nuisance to adjacent residents	M	Regular inspections Rules shared with tenants	Allotment Policy
	Accidents/ Personal injury	M	Risk assessment is reviewed at least annually and public liability insurance	
	Vandalism	M	Regular inspections Feedback from allotment tenants and members of the public Clear reporting channel	
	The cost of renting the Grove Road Allotments exceeds a reasonable amount to recharge to allotment holders	H	Discussions with Savills (representing Exeter Diocese) Consideration of purchasing the land Consideration of giving the management of the allotments back to Exeter Diocese	
Open Spaces	Damage/Vandalism	M	Regular inspections and reports to the Council Clear reporting channel	

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
	Trees	M	Regular inspections at intervals Commissioning recommended works in a timely manner	
	Condition of land	M	Maintenance programme Grounds maintenance programme	
Play Area	Damage/ Vandalism/ rubbish	H	Regular visual checks Weekly inspections identifying defects and remedial action required Regular reports to the Council identifying any issues Annual independent inspections to RoSPA standard	
	Trees	M	Regular inspections at intervals Commissioning recommended works in a timely manner	
	Personal Injury	H	Regular visual checks and weekly inspections Annual independent inspections to RoSPA standard Removal or cordoning off any pieces of equipment requiring repair Adequate insurance coverage	
Parish Car Park	Facilities not maintained	M	Use of contractor for keeping the car park in a good state of order	
	Damage/ Vandalism/ rubbish	M	Regular inspections and reports to the Council Clear reporting channel	
	Personal Injury	M	Clear lined spaced for vehicles Signage installed highlighting dangers Adequate insurance cover	
Local Government Reorganisation (LGR)	The asset or service may be lost if the Parish Council decides not to take it on and the Unitary / County / District may stop providing it.	H	Keep up to date with what is happening with regards to Local Government Reorganisation. Engage in discussions with the Unitary / County / District councils to ascertain if it	

Topic	Risk	H/M/L	Management or risk (mitigating factors)	Review/Assess/Revise
Asset transfer from Unitary / County / District Councils to the Parish Council	Unlikely to receive appropriate funding from Unitary / County / District to run additional services so the precept would likely increase	H	would be beneficial to local people for the Parish Council to take on additional services. Engage with local people to get their views (especially if the service is likely to be lost if not taken on by the Parish Council or if the Precept will likely increase) Consider allocating funding to a specific Ear Marked Reserve for LGR when setting the 2026/27 and 2027/28 budgets	
Neighbourhood Plan	Neighbourhood Plan is not completed promptly, doesn't meet regulations and guidance and isn't robust in planning terms	M	Work with the Neighbourhood Planning Officer / Team at EDDC to ensure that the Whimple Neighbourhood Plan meets regulations and guidance and is robust in planning terms	
Use of personal device for Council business	Inadequate or lack of appropriate security measures used to control access to the device meaning personal data may be accessible to third parties Device is used in an insecure manner, e.g. could be impacted by malware Device is lost or stolen meaning that third parties can access council information and personal data Device sold or given away and still able to access council information and data Clerk ceases to be employed by the Parish Council or councillor ceases to be on the council. Information and personal data may remain accessible to unauthorised third parties	M	The Council has an IT Policy and Bring Your Own Device Policy clearly setting out how a personal device(s) must be used for council business. Wherever possible information and data (including personal data) is securely stored on a cloud based system (i.e. not held on the personal device) subject to a robust Data Sharing Agreement or appropriate Data Protection measures being in place. Ensure that the Council's data is regularly backed up on a cloud based system and an external hard drive. Ensure that there is an exit checklist for the Clerk and councillors.	

ASSET REGISTER 13/01/2026

Description	Date acquired	Purchase Price		Insurance valuation	
Office Equipment					
3-Drawer filing cabinet	22/07/1985	£49.74		£0.00	
4-Drawer filing cabinet	21/07/1988	£65.00		£0.00	
Computer	30.12.2019	£874.92	Remove from insurance schedule	£0.00	Note 1
Computer Rucksack	13/01/2020	£66.61	Remove from insurance schedule	£0.00	
Projector	27/05/2016	£329.99	Review insurance schedule as totalling to £502.37	£120.00	Note 2
Presenter	27/05/2016	£24.99		£0.00	
Computer back up external hard drive	09/10/2024	£33.24		£0.00	
		£1,444.49		**£120.00**	
General Parish Assets					
Almet park seat	25/11/1974	£41.48	No idea what this is - deleting	£0.00	
Lomas Seat	?	£1.00	Adding as on insurance schedule	£2,560.03	
2 x Bus shelters	28/02/1981	£899.20	Located at Hand and Pen	£8,533.47	
Notice case	13/03/1986	£95.45	Located at Hand and Pen	£0.00	Note 3
2 x seats/ benches	29/03/1990	£259.67		£2,560.03	Note 4
Footbridge	11/07/1992	£3,501.50	Stone bridge over river in The Square?	£0.00	Note 5
Car Park	15/01/1996	£8,225.00		£0.00	Note 5
5 x Dog waste bins	01/10/2003	£1,133.74	EDDC invoices lists 6 dog bins and 1 litter bin.	£1,536.01	
Bin (replacement)	07/11/2014	£342.70	Is this the 6th dog bin?		
Dog waste and general bin	17/11/2020	£538.49	Is this a duplicate entry? AR listing 6 dog waste and 2 litter bins. Invoiced for 6 + 1		
Litter bin	02/03/2006	£347.99	EDDC invoices lists 6 dog bins and 1 litter bin.		
Village signs x 3	18/06/2012	£800.00		£1,249.49	
Allotments (Heb Close)	24/06/2016	£1.00	Nominal fee	£0.00	Note 5
Defibrillator	06/02/2017	£1,831.14	Does this need to be added to the Insurance schedule?	£990.00	Note 6
5 x grit bins (incl vat)	21/01/2019	£1,129.02		£0.00	
Noticeboard	04/04/2022	£854.00	Noticeboard in The Square	£1,014.00	Note 7
		£19,959.90		**£18,443.03**	
Town Lane Site Assets					
Children's playground	22/04/1985	£500.00	Deleted as removed from Town Lane site	£0.00	
Fencing children's playground	02/02/1987	£2,500.79	Is this the fencing at Town Lane?	£0.00	Note 8
2 x Picnic tables	10/03/1990	£504.85	Deleted as removed from Town Lane site	£0.00	
Footpath	27/03/1993	£834.88	FP12 through Town Lane playground.	£0.00	Note 5
Taylor Made play equipment	01/03/2002	£2,167.50	Deleted as removed from Town Lane site	£0.00	
Youth shelter	10/03/2007	£2,800.00	Deleted as removed from Town Lane site	£0.00	
		£3,335.67		**£0.00**	
Parish Field Assets					
Whimple Parish Field	30/02/1989	£3,250.00		£0.00	Note 5
Picnic table (wheelchair)	02/06/2009	£614.30		£2,560.03	Note 9
Picnic table	02/06/2009	£429.30			
Adventure trail play equipment	27/05/2009	£16,762.40		£28,607.58	
Cycle track	30/05/2009	£27,754.67	Classed as land as path around Parish Field	£0.00	Note 5
BMX bumps	30/05/2009	£1,840.00		£0.00	Note 5
Sign at entrance	10/06/2009	£200.00		£331.40	
Metal Shed	01/05/2011	£573.25		£1,000.00	Note 10
Benches x 2 (replacement)	07/11/2014	£770.56			Note 4
Pump Track	15/11/2022	£39,654.41		£48,407.34	
		£91,848.89		**£80,906.35**	

Safety Equipment & Clothing (all incl VAT)					
High Visibility Waistcoat x 10	05/12/2018	£35.40	Do we need to remove?	Obsolete as no road wardens	£0.00
High Visibility 2-Tone Site Jacket x10	05/12/2018	£239.40	Do we need to remove?	Obsolete as no road wardens	£0.00
Black Contactor Wellington x10	05/12/2018	£179.40	Do we need to remove?	Obsolete as no road wardens	£0.00
High Visibility Stormbreaker Trouser x10	05/12/2018	£119.40	Do we need to remove?	Obsolete as no road wardens	£0.00
Canadian Rigger Gloves Product x10	05/12/2018	£23.40	Do we need to remove?	Obsolete as no road wardens	£0.00
Red PVC Knit Wrist Glove waterproof for stream cleaning x 10	05/12/2018	£14.40	Do we need to remove?	Obsolete as no road wardens	£0.00
750mm Road Cone x 12	05/12/2018	£71.28			£0.00
Directional Arrow Right	05/12/2018	£17.94			£0.00
Directional Arrow Left	05/12/2018	£17.94			£0.00
Road Narrows Nearside	05/12/2018	£15.54			£0.00
Road Narrows Offside	05/12/2018	£15.54			£0.00
Roadworks Ahead x 2	05/12/2018	£31.08			£0.00
Road Ahead Closed x2	05/12/2018	£69.48			£0.00
Titan Barrier 2m x 2	05/12/2018	£83.88			£0.00
Unipart Dorman UniLamp Flashing x6	05/12/2018	£42.84			£0.00
Lamp Battery 6v x 6	05/12/2018	£14.04	Do we need to remove?	Obsolete as no road wardens	£0.00
Rock Salt Spreader x 2	05/12/2018	£311.88	Do we need to remove?	Obsolete as no road wardens	£0.00
Plastic Snow Pusher Product x 12	05/12/2018	£172.08	Do we need to remove?	Obsolete as no road wardens	£0.00
Plastic snow shovel x 12	05/12/2018	£287.28	Do we need to remove?	Obsolete as no road wardens	£0.00
		£1,762.20			**£0.00**
Grand Totals		**£118,351.15**			**£99,469.38**

Notes:

1. Computer being removed from insurance schedule as the computer is obsolete and clerk uses own laptop
2. Insurance cost of 'new for old' replacement is £120
3. Notice case at Hand and Pen would cost less to replace 'new for old' than paying insurance excess of £100
4. 5 seats/ benches listed on insurance schedule - located in several locations in the village and at the Parish Field. Listed under general assets and Parish Field Assets
5. Land. Insurance have advised that they don't include land in the insurance quotation. Covered under Public Liability Insurance if damage to 3rd party or property
6. Defibrillator added to insurance schedule. 'New for old' price of £990.00
7. Noticeboard in The Square. 'New for old' price taken from website of company that supplied current noticeboard. Two other noticeboards not included as could replace with noticecase that would be cheaper than insurance excess
8. Fencing - checking if this is the Town lane site. Not included in insurance schedule - would presumably be considered as land rather than contents
9. picnic tables. 4 listed on insurance policy and all located in the Parish Field
10. Metal Shed. Added to insurance schedule and Parish Council will be storing items in it. 'New for old' replacement anticipated to be circa £1,000

WHIMPLE PARISH COUNCIL
BRING YOUR OWN DEVICE (BYOD) POLICY

(*Approved 19 January 2026 minute*)

1. Introduction

Whimple Parish Council 'the council' recognises that councillors and employees may use personally owned devices (e.g. computers [desktop and laptop], smartphones, tablets and external hard drives) to conduct Parish Council business.

The purpose of this policy is to ensure so far as possible that personally owned devices used by councillors and the Parish Clerk to conduct Parish Council business are used in a manner which protects Personal Data and ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy has been written to minimise the risks associated with BYOD by outlining the responsibility and acceptable use.

2. Scope

This policy applies to all elected and co-opted councillors, the Parish Clerk, and all employees or volunteers who access or process council data using personal devices.

Breach of this policy may result in disciplinary action (employees) or referral to the Monitoring Officer (councillors).

3. Risks

Under normal circumstances the only device holding personal data is the Parish Clerk's computer: provided that the access and safe usage measures are practiced, then no further action is required.

However, should this computer be unavailable for whatever reason, then the Chairperson or other designated councillor may need to use a personal device to conduct parish business: in which case it must be presumed that personal data may be handled.

Before a personal device is used, the Council must be satisfied that all the following safety measures are in place. Once the official laptop is again available, all council data accumulated on the personal device must be deleted.

The Parish Council has identified a number of risks inherent in using personally owned Devices to conduct Parish Council Business which have been added to the Council's Risk Assessment.

4. Responsibilities

All users of personal devices for council business are responsible for protecting the device. This includes regular updating of software and ensuring it is not used by anyone else to gain access to Council information.

The remaining sections of this Policy set out the guidance that individuals must follow when using a personal device for council business.

- Keep devices updated with the latest security patches and antivirus software,
- Use encrypted connections (e.g. VPN or secure Wi-Fi) when accessing council data,
- Avoid using public Wi-Fi unless protected by a secure connection,
- Ensure that the device is not used by anyone else
- Immediately report any loss, theft, or suspected breach to the Clerk.

5. Access to Devices

- Devices used for Parish Council business must be secured with strong passwords or biometric authentication
- Passwords must comply with the following rules:
    - Passwords must not be written down
    - Passwords must not be disclosed to any other person. If a password is disclosed to any other person, whether deliberately or inadvertently, it must be changed immediately
    - A different password should be used for each and all Devices, email accounts or other hosted systems
    - Passwords should be changed at least every 12 months
    - Passwords should be a complex mix of letters and symbols, at least 8 characters long
- Ensure that the device is not used by anyone else
- You are responsible for paying any network charges that might occur whilst using your device for council business unless otherwise agreed by the Council

6. Security Measures

- Devices must auto-lock after a short period of inactivity.
- Council email accounts must be accessed via secure apps or web portals.
- No council data should be stored permanently on personal devices.
- Remote wipe capabilities should be enabled where possible.

7. Safe usage of Devices

- Keep devices updated with the latest security patches and antivirus software
- Use encrypted connections (e.g. VPN or secure Wi-Fi) when accessing council data
- Avoid using public Wi-Fi unless protected by a secure connection

8. Data Protection Requirements

- Personal data must only be accessed or processed for legitimate council purposes.
- Data must be deleted from personal devices once no longer required or upon leaving the council.
- Sensitive personal data (e.g. health, political views) must be handled with extra care and only stored on secure systems.
- Council data must not be shared with unauthorised individuals or stored in insecure apps or cloud services (unless there is a robust Data Sharing Agreement in place).

9. **Monitoring and Compliance**
   - The council reserves the right to restrict access to council systems from any device that does not meet security standards.
   - Users must cooperate with audits or investigations related to data protection.
   - Breaches of this policy may result in disciplinary action or referral to the Information Commissioner's Office (ICO).

10. **Lost or Stolen Devices**
    In the event that a Device is lost or stolen, or is suspected of having been stolen, the Parish Clerk or Chair and/or Vice Chair (in the event of it being the Parish Clerk's device) must be informed. The Parish Council will work with the owner of the lost or stolen device to identify any personal data at risk and will then take appropriate action, including reporting any breach to the ICO as necessary.

11. **Repair of Devices**
    If a personal device needs to be repaired, the owner will take all reasonable steps to ensure that the repairer cannot access any personal data.

12. **Transfer or Disposal of Devices used for Council Business**
    If the owner wishes to transfer or dispose of a personal device which has been used for Parish Council business all personal data must be deleted from that device using a method which prevents recovery.

13. **Leaving the Council**
    Upon leaving the council, councillors and employees must:
    - Permanently delete all council-related data from personal devices and email accounts,
    - Return any council-issued equipment,
    - Confirm in writing that all data has been removed.

14. **Review and Updates**
    This policy will be reviewed every two years or in response to changes in legislation or council operations.

WHIMPLE PARISH COUNCIL
INFORMATION TECHNOLOGY POLICY
[Based on the NALC Policy Template]

Introduction

Each council will have its own IT setup and, as such, a single 'one-size-fits-all' IT policy is unlikely to be appropriate. Some smaller parish councils may operate with minimal equipment, while others may manage multiple devices connected to a central server. These guidelines are intended to help councils identify key considerations when developing or updating their own IT policy.

Councils that use external IT providers should ensure their policies accurately reflect current practices and contractual arrangements.

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.

Councils will also need to determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

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 only.

1.1.2 Locking computers when leaving desk, 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 Councillors, staff, and other authorised 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 council.

1.1.9 The Clerk must report any faults or necessary repairs to the Chair and/or Vice Chair of the Council along with an estimated cost of any repairs.

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 disenabled 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.

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the Chair and/or Vice Chair of the Council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the cost 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 Council. 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 Clerk.

2.2 Use of own devices

Use of personal devices is permitted and must be used in accordance with the Council's Bring Your Own Device (BYOD) Policy.

2.2.1 The Council recognises that some councillors, staff, and other authorised users may wish to use their own devices (e.g. computers [desktop and laptop] smartphones, tablets) to access the Council's email system, accessing hosted cloud based system and accessing and/or saving documents stored on the council's document management system. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will 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.

2.2.2 However, the same security precautions apply to personal devices as to the council's computer equipment. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.3 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 may result in disciplinary action, including summary dismissal (without notice). This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

2.2.4 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.

2.2.5 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.

2.2.6 The Parish Council has identified a number of risks inherent in using personal devices to conduct council business which have been added to the Council's Risk Assessment.

Health and safety

3.1.1 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.

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

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. Passwords should be a complex mix of letters and symbols, at least 8 characters long.

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 (initially) and then the Parish Clerk.
- 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.

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 with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair of the Council, 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.

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.

Monitoring

5.1.1 The council reserves the right to monitor 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.

5.1.2 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.

5.1.3 The information obtained through monitoring may be shared internally, including with relevant councillors and IT 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.

5.1.4 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.

5.1.5 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.

5.1.6 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.

5.1.7 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.

5.1.8 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.

5.1.9 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 remotely, 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;
- 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 remotely 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.

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 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 are for council use only. Personal use is not permitted.

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 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 Council.

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 and Privacy Statements which are available 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 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 individuals 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.

9.1.3 To protect both the council and its interests, everyone is required to comply with the Council's Social Media Policy which is available on the Council website.

9.1.4 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.

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 may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

Agenda Item: 19

Whimple Parish Council - Forward Plan

Meeting Date	Items for agenda
Monday 16 February 2026 (*agenda published on Tuesday 10 February*)	• Payment Schedule – February 2026 • Transfer Schedule – February 2026 • Bank reconciliations to 31 January 2026 • Budget Monitoring to 31 January 2026 • Planning applications (if appropriate) • Neighbourhood Plan – draft Plan (without the affordable housing allocation)
Monday 16 March 2026 (*agenda published on Tuesday 10 March*)	• Payment Schedule – March 2026 • Transfer Schedule – March 2026 • Bank reconciliations to 28 February 2026 • Budget Monitoring to 28 February 2026 • Planning applications (if appropriate) • Grant Applications • Asset Register
Monday 20 April 2026 (*agenda published on Tuesday 14 April*)	• Payment Schedule – April 2026 • Transfer Schedule – April 2026 • Bank reconciliations to 31 March 2026 • Budget Monitoring to 31 March 2026 • Planning applications (if appropriate) • Internal Control checklist – Quarter 4 • Risk Assessment – Quarter 4