Agenda No. 18

Appointment of a Data Protection Officer

Reviewing Microshade quote and the Senior Policy and Data Compliance Officer workload I recommend that Microshade be appointed to act as the Council's DPO on a 12-month contract providing the following data audit services and that this be reviewed at the end of the 12-month period:

1. Provide a data audit as described in section 1.1 of the quote - £695.00 (basic training session provided FOC)

2. Provide DPO services as described in 1.2 of the quote - £500.00

Due to the initial amount of work involved to bring the Council up to the required standards I recommended appointing Microshade because the Council still remains at a 'working towards' stage.

Appointing Microshade will ensure that the Council will be able to meet all the criteria set out by the new GDPR legislation.

Other Town and Parish Councils consider the appointment of a DPO value for money in the initial stage of the new GDPR legislation.

The owner of Microshade is a Town Clerk with a wealth of Public Sector experience.

Office Manager

Saltash Town Council

Agenda No. 19a

STC Policy/Procedure
DRAFT

Saltash Town Council

Policy/Procedure:	**Information Security Policy**
Date of Adoption:	

This is a Policy or Procedure document of Saltash Town Council to be followed by both Councillors and employees.

Current Status			
Version	1 DRAFT	**Approved by**	
Date		**Date of approval**	
Responsible Officer		**Minute reference**	
Responsible Committee		**Review date**	

Version History			
Date	**Version**	**Author/Editor**	**Comments**

Review Record				
Date	**Type of Review**	**Date of completion**	**Summary of actions**	**Completed by**

STC Policy/Procedure
DRAFT

Contents

Saltash Town Council

Information Security Policy

Introduction

This policy document encompasses all aspects of security surrounding confidential information held on council information and telecommunication systems, including the handling of sensitive customer information. Employees should also refer to the Management of Transferable Data Policy and the Information and Data Protection Policy.

All employees must read this document in its entirety and sign the attached form.

The document will be reviewed and updated on an annual basis or when relevant to include newly developed security standards.

Information Security Policy

The Council handles sensitive customer information daily. Sensitive Information must have adequate safeguards in place to protect the customer data, customer privacy, and to ensure compliance with various regulations.

The Council commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end the Town Council is committed to maintaining a secure environment in which to process customer information.

Employees handling sensitive customer data should ensure that they:

- Handle council and customer information in a manner that fits with their sensitivity and classification;
- Limit personal use of the Council information and telecommunication systems and ensure it doesn't interfere with their job performance;
- The Council reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Council resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive data and lock computer screens when unattended;

- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – the Senior Policy and Data Compliance Monitoring Officer.

All employees have a responsibility for ensuring the Council's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

1. Network Security

A high-level network diagram of the network is maintained and reviewed on a yearly basis. The network diagram provides a high-level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS (point of sale) devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.

In addition, ASV should be performed and completed by a PCI SSC Approved Scanning Vendor, where applicable. Evidence of these scans should be maintained for a period of 18 months.

2. Acceptable Use Policy

The Council's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Council's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Council from illegal or damaging actions, either knowingly or unknowingly by individuals. The Council will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix C.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data [which includes card holder data].
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops, workstations, tablets and mobile phones should be secured with a password-protected screensaver with the automatic activation feature.
- All POS (point of sale) and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- The List of Devices in Appendix C will be regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.

- Users should be able to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour should be reported accordingly.
- Information contained on portable devices and computers is especially vulnerable, special care should be exercised.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Suspicious emails not picked up by the installed antivirus software should not be opened but referred to the IT consultant.

3. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the Council if disclosed or modified. *(Confidential data includes cardholder data.)*

Internal use data might include information that the data owner feels should be protected to prevent unauthorised disclosure.

Public data is information that may be freely disseminated.

4. Protect stored data

All sensitive data stored and handled by Council employees must be securely protected against unauthorised use at all times.

Customer payment details

- Any sensitive card data that is no longer required for business reasons must be discarded in a secure and irrefutable manner.
- If there is no specific need to see the full Permanent Account Number (PAN), it must be masked when displayed.
- Unprotected Permanent Account Numbers should never be sent via end user messaging technologies.

It is strictly prohibited to store:

1. **The contents of the payment card magnetic strip (track data) on any media whatsoever.**
2. **The CVV /CVC (the 3 or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
3. **The PIN or the encrypted PIN Block under any circumstance.**

5. Access to the Sensitive Customer Data (including Cardholder Data)

All Access to sensitive customer data should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix C.
- The Council will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- The Council will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider.
- The Council will have a process in place to monitor the PCI DSS compliance status of the Service provider.

6. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by an employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on Council sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces are periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices

- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and must be approved by management.
- Strict control is maintained over the storage and accessibility of media.
- All computers all that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

7. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

8. Disposal of Stored Data

- All data must be securely disposed of when no longer required by the Council, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- The Council will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The Council will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using

military grade secure deletion processes or the physical destruction of the media;
  - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

9. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Council.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

10. Credit Card (PCI) Security Incident Response Plan

The Council PCI Security Incident Response Team (PCI Response Team) is comprised of the Information Security Officer and Merchant Services. The Council PCI security incident response plan is as follows:

1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
2. That member of the team receiving the report will advise the PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The PCI Response Team will determine if policies and processes need

to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

The Council PCI Security Incident Response Team (or equivalent in your organisation):

Town Clerk
Office Manager
Senior Policy and Data Compliance Monitoring Officer
Finance Officer
Collections & Merchant Services
Risk Manager

Information Security PCI Incident Response Procedures:

- A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform the Council PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

Incident Response Notification

Escalation Members:

Escalation – First Level:
Information Security
Officer Controller
Executive Project Director for Credit Collections and Merchant
Services Legal Counsel
Risk Manager
Director of the Council Communications

Escalation – Second Level:
Chairman of the Council
Executive Cabinet
Internal Audit
Auxiliary members as needed

External Contacts (as needed)
Merchant
Provider Card
Brands

Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable) Communication Carriers (local and long distance) Business Partners
Insurance Carrier
External Response Team as applicable (CERT Coordination Centre_1, etc) Law Enforcement Agencies as applicable inn local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyse the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See Appendix Bfor these requirements.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The Senior Policy and Data Compliance Monitoring Officer and/or the Finance Officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the Senior Policy and Data Compliance Monitoring Officer will alert management and begin informing all relevant parties that may be affected by the compromise.

11. Transfer of Sensitive Information Policy

- All third-party companies providing critical services to the Council must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with the Council's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must

  1. Adhere to the PCI DSS security requirements.
  2. Acknowledge their responsibility for securing the Card Holder data.

3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

12. User Access Management

- Access to Company is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

  Name of person making request;
  Job title of the newcomers and workgroup;
  Start date;
  Services required (default services are: MS Outlook, MS Office and Internet access).

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all the Council systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves the Council employment, all their system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

13. Access Control Policy

- Access Control systems are in place to protect the interests of all users of the Council computer systems by providing a safe, secure and readily accessible environment in which to work.

- The Council will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. The IT Consultant shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the Council CISO.
- Access to the Council IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any the Council IT resources and services will be provided without prior authentication and authorization of a user's the Council Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by the Council policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by their Line Manager and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights,

firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.

- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with the IT Consultant to review users' access rights. The review shall be logged, and Line Manager shall sign off the review to give authority for users' continued access rights.

Appendix A: Agreement to Comply Form – Agreement to Comply with Information Security Policies

_____
Employee Name (printed)

_____
Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the Council by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Council, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Council security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____
Employee Signature

_____
Date

Appendix B: Credit/Debit Card Security Incident Reporting

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret" *.

a. Executive Summary
   i. Include overview of the incident
   ii. Include RISK Level (High, Medium, Low)
   iii. Determine if compromise has been contained
b. Background
c. Initial Analysis
d. Investigative Procedures
   i. Include forensic tools used during investigation
e. Findings
   i. Number of accounts at risk, identify those stores and compromised
   ii. Type of account information at risk
   iii. Identify ALL systems analysed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)
   iv. Identify ALL compromised systems. Include the following:
      - DNS names
      - IP addresses
      - OS version
      - Function of System(s)
   v. Timeframe of compromise

vi. Any data exported by intruder
vii. Establish how and source of compromise
viii. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
ix. If applicable, review VisaNet endpoint security and determine risk

f. Compromised Entity Action
g. Recommendations
h. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

a. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
b. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
c. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
d. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as detailed forensics evaluation).
e. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
f. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
g. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Employees of The Council will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within The Council and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

a. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
b. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
c. Prepare a list of all known compromised account numbers
d. Obtain additional specific requirements from Discover Card

American Express Steps

a. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
b. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
c. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

Appendix C: List of Devices

Asset/Device Name	Description	Owner/Approved User	Location

Appendix D – list of abbreviations

CDE Cardholder Data Environment

POS Point of Sale

ASV Approved Scanning Vendor

PCI Payment Card Industry

SSC Security Standards Council

PAN Permanent Account Number

DSS Digital Security Standard

AES Advanced Encryption Standard

PGP Pretty Good Privacy Encryption Program

IPSEC Internet Protocol Security

CISO Chief Information Security Officer

Agenda No. 19b

Saltash Town Council

Policy/Procedure:	**Grants Policy DRAFT**
Date of Adoption:	

This is a Policy or Procedure document of Saltash Town Council to be followed by both Councillors and employees.

Current Status			
Version	2 DRAFT	**Approved by**	
Date		**Date of approval**	
Responsible Officer		**Minute reference**	
Responsible Committee		**Review date**	

Version History			
Date	**Version**	**Author/Editor**	**Comments**

Review Record				
Date	**Type of Review**	**Date of completion**	**Summary of actions**	**Completed by**

Contents

1. Policy/Procedure Background

This document sets out a clear and structured procedure for grant applications being submitted to Saltash Town Council.

This procedure is prepared in accordance with the Town Council's new policy on grants.

Saltash Town Council is committed to support a range of causes each year within a limited budget. It is therefore imperative that the Town Council has in place an established method of scrutinising grant applications to ensure it uses its budget to the best possible effect.

Applications will be considered providing sufficient funds remain in the budget.

2. Policy Statement

A grant or subsidy is any payment made by Saltash Town Council to be used by an organisation specific purpose in the furtherance of the well-being of the community, either generally, or for a specific purpose and which is not directly controlled or administered by Saltash Town Council. The purpose of any grant or subsidy given by Saltash Town Council is to support initiatives in the local community and to help create opportunities for the residents of Saltash that are not, as a matter of course, funded by Saltash Town Council or Cornwall Council.

3. Application principles

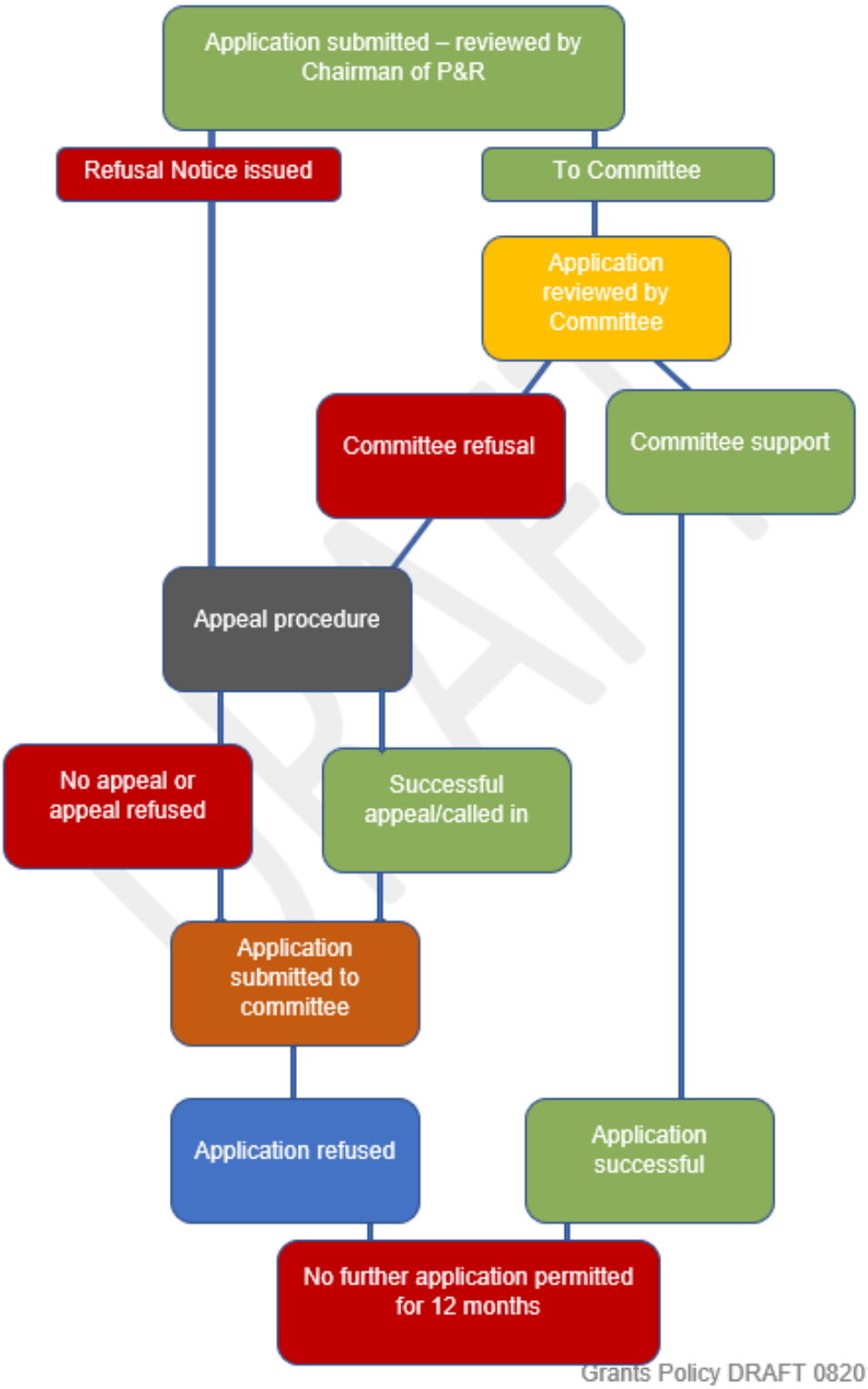
1. Applications must be fully completed and assessed against a set of criteria laid down by members of Saltash Town Council.

2. If an application is refused by the Committee, then an appeal procedure can be implemented under certain circumstances and within a set deadline.

3. If an application is:
   a. not called in by a relevant number of Town Councillors
   b. is refused on appeal
   c. is not appealed within the deadline set or
   d. has been turned down by members at a previous Committee meeting

   then a new request/re-application or a request of a similar nature will automatically be turned down for a period of not less than 12 months' time from the date the previous application was turned down without the ability to appeal.

4. Application process



Application Submitted

Applications should be made using the Grant application form (Appendix 1). Applicants should ensure that all relevant documents are included or there may be a delay to the application being considered. It is the responsibility of the applicant to ensure that the application is submitted 20 working days before the meeting of the Policy and Resources Committee. Successful applicants will be expected to clearly acknowledge the support of the Town Council on publicity material and sufficient time to undertake this should be factored in when submitting the application.

Application reviewed by Chairman of Policy and Resources Committee[1]

The application will be reviewed by the Chairman of Policy and Resources Committee against the eligibility criteria (listed in this document) and will either notify the applicant of refusal with details of the appeal procedure or submit it to the next available meeting of the Policy and Resources Committee.

Chairman of Policy and Resources Committee Refusal

When an application is refused by the Chairman of Policy and Resources Committee the applicant will be notified immediately and given 30 days to appeal. Members of the Policy and Resources Committee will also be notified who may choose to call in the application themselves.

Appeal procedure

Following notification of refusal, applicants have 30 days to appeal in writing. Within this period a member of the Policy and Resources Committee may request that the application is called in.

No appeal or appeal refused

Appeals will be considered by the Chairman of the Policy and Resources Committee. Where no appeal is received this will be noted on the application form.

Successful appeal or call in

Where an appeal is successful or a member of the committee has called the application in, it will be submitted to the next available meeting of the Policy and Resources Committee.

Restrictions on re-applications

Applications that have been refused by the Chairman of the Policy and Resources Committee, the Policy and Resources Committee or that have not been appealed after 30 days will be closed. Applicants may not apply for a grant for the same or similar scheme until 12 months from the date of closure.

[1] If Chairman unavailable Vice Chairman will undertake all roles outlined in this document

Chairman of the Policy and Resources Committee Support

Where the Committee Chairman considers the application is valid and meets required criteria the application will be placed on the agenda for the next Policy and Resources meeting.

Application submitted to committee

The Policy and Resources Committee will consider applications at the next available meeting. The applicants may be invited to attend the meeting to answer questions and will be given at least five working days' notice. If an applicant is unable to attend the Committee Chairman may defer the application to a future meeting.

Application successful

Successful applicants will be advised in writing and given two months to apply for funding to be released. Any conditions placed on the funding will have to be met before funds are released. If the applicant wishes to extend this period the request should be put in writing which will pass this to the Committee Chairman for a decision.

Application refused

If an application has been heard by the Policy and Resources Committee and been refused, the applicant cannot reapply or submit a further grant request for the same or a similar project for a period of 12 months. Any application received will be automatically rejected without appeal or the option for a member to call in the application.

5. Types of grant and funding limits

Saltash Town Council has two separate funds available to the local community. To enable as many organisations as possible to benefit from the grants, there will only be one grant per organisation permitted in any 12-month period.

The Community Chest supports small scale community projects intended to improve the town environment to strengthen the community fabric or the common economy of the town.

The Festivals Fund supports larger events that are free, 6 to 7-hour long events likely to attract several thousand people.

Both funds have a cap on the amount which can be awarded:

The Community Chest grant will not exceed £1000.

The Festivals Fund grant will not exceed £1000 per day up to a maximum of three days per event.

6. Normal Eligibility Criteria

This section outlines the normal criteria organisations have to fulfil for grants.

a. Mandatory requirements

All of the following requirements must be met by applicants. Where they are not met a clear reason should be given in writing with the application.

i. Copies of the most recent bank statements must be provided
ii. Public Liability Insurance Certificates are required for any events or projects
iii. If staff will be involved Employee Liability Insurance Certificates are required
iv. Buildings Insurance will be required if an application relates to funding towards this purpose
v. Full contact details for the applicant as well as any registered address for the organisation should be supplied
vi. A copy of the constitution for the organisation should be included
vii. Applicants may be required to attend a meeting to answer questions on the application or make a presentation
viii. Match funding is extremely important and the applicant needs to demonstrate that this is in the process of being sought or is already in place.
ix. All successful applications will be required to provide receipts and supporting documents after the event and return to the Town Council any unused grant awarded.

b. Key Priority Areas

Grants may be given for projects that fit into one or more of the following areas:

i. The promotion of tourism and leisure for both residents and visitors to the area with a community focus
ii. Supporting local safety campaigns
iii. Enhance existing events
iv. Promote pride in the community
v. Highlight important local issues/history/culture to local residents and students
vi. Promote a sports -related initiative or event
vii. Increases visitors to Saltash and improves the local economy
viii. Promotes environmental issues which improve the local area

7. Applications that will not be eligible

The Town Council will not consider applications for or from the following except in exceptional circumstances:

a. Statutory services
b. Expeditions or trips
c. Replacement for statutory funding
d. Bursaries or scholarships
e. Projects outside of Saltash
f. Individuals
g. Hospitality
h. National Charities
i. Salaries or routine administration costs

j. "Upward funders"-local groups who send fundraising to central headquarters for redistribution
k. Private organisations operating as a business to generate a profit or surplus
l. Cost of routine maintenance and repair of equipment
m. Projects with party political links
n. Organisations intending to support or oppose any particular political party or to discriminate on any grounds
o. Projects which discriminate on any grounds
p. Projects which do not benefit the Saltash community at large
q. "Branches" that could be funded by the main organisation
r. Buildings that are uninsured
s. A project that competes or conflicts with any service, project or event being supported, organised or funded by the Town Council
t. Applications from organisations with substantial and allocated resources will not be considered a priority for funding and will usually be unsuccessful
u. Applications will not normally be considered from national organisations or local groups with access to funds from national "umbrella" or "parent" organisations, unless funds are not available from their national bodies, or the funds available are inadequate for a specified project.

8. Guidelines for Grant Applications and Further Information

a. In most cases, if a grant has been successful in the past, then there will be a limit to the number of times the same or similar grant can be requested again.
b. If an organisation (or a subgroup of the same organisation) is successful in obtaining a grant in one financial year, it is unlikely it will receive another grant for a period of not less than 23 months.
c. It is a condition of any grant application that the group or project must bring direct benefit to the residents of Saltash. All applications must clearly demonstrate how this will be achieved.
d. Application forms are available from the Guildhall or from the Town Council website. Application forms must be submitted along with the latest set of the group's accounts. It is important that all questions on the application form are fully answered and that any appropriate additional information, which supports an application, is provided at the time of submission.
e. Applications cannot be made retrospectively.
f. The scheme provides start-up awards for new as well as grants for existing organisations. Applications will be considered for day-to-day running expenses and individual projects.
g. Saltash Town Council will only grant aid to churches for parish clocks and possibly for environmental purposes. Church Halls can also be grant aided if they are used by the community.

h. Schools will only be grant aided for environmental purposes or if, in the opinion of Saltash Town Council, their application is for the benefit of the wider community. The project must also be in addition to statutory services.
i. Applications from education, health or social service establishments will be considered where the organisation can demonstrate that it is working in partnership with other groups and where there are benefits to the wider community within the parish. The project must also be in addition to statutory services.
j. Grant applications will be considered against the following criteria:
    i. meeting the priorities are set out above
    ii. meeting an identified need
    iii. viability of the project
    iv. the majority of those benefiting our residents of the town
k. Saltash Town Council reserves the right to reclaim the grant in the event of it not being used for the purpose specified on the application form.
l. Grants will not be awarded retrospectively.
m. A grant must only be used for the purpose for which it was awarded. Written approval must be obtained from the Town Council in advance for a change in use of grant money.
n. Any underspent portion of the grant must be returned to Saltash Town Council within 12 months of the award.
o. Where equipment has been purchased using grant funding and is going to be disposed of the Town Council should be given the opportunity to have the items returned to them so that they meet may be offered to other eligible organisations.
p. Administration of and accounting for the grant is the responsibility of the recipient.
q. The Town Council reserves the right to request any further information that it deems necessary to assist the decision-making process. Account will be taken of the amount and frequency of previous awards and of the extent to which funding has been sought or secured from other sources or own fundraising activities.
r. In the case of grant awarded for projects for which additional grant funding is to be sought to enable the project proceed, the funds approved will only be available to the organisation when all other funding is in place/secured subject to a time limit of 12 months from date of approval. After this 12 month period the applicant should submit in writing a full update, reasons for the delay and a request to extend the period of the grant. Requests will be considered by the Policy and Resources Committee following review by the Chairman.
s. Organisation seeking funds for buildings must demonstrate a reasonable security of tenure in the relevant property.
t. The size of any grant awarded is at the discretion of the Policy and Resources Committee.

u. All awards are made subject to any additional conditions and requirements as deemed appropriate by the Policy and Resources Committee.
v. The Town Council reserves the right to refuse any application considered inappropriate or not meeting the objectives of the Council.

9. Banking Arrangements

Organisations should have a bank account in the name of the organisation with at least two authorised representatives required to sign a cheque.

10. Chairman Refusal

This section provides details of possible reasons for the Chairman of the Policy and Resources Committee refusing an application. It is not an exhaustive list and attempts to provide clarity over some of the topics which are considered:

a. Application does not meet the eligibility criteria
b. Application is not complete
c. Further information requested on an application has not been received in good time and no-communication has been achieved with the applicant
d. Standard mandatory requirements are not in place/being met
e. Does not fit in with the Key Priorities of the Town Council
f. Similar applications have been rejected
g. Following an established precedent
h. Such an application would set an unfair or unsustainable precedent for future applications of a similar nature
i. The project is considered too high risk for public funds to be contributed to it
j. The business case is considered flawed or unsustainable (if appropriate)
k. The Town Council does not hold any more funding for grants and there are no suitable reserves that could be utilised
l. Any other relevant reason(s) which are considered important enough to warrant refusal to safeguard the Town Council and the local public funds.

11. Automatic Refusal

An application will automatically be refused with no appeal rights if it is an application for the same or is similar to a previously refused application and has been submitted within the 12 months following the refusal (same applicant/organisation/family).

12. Appeals Procedure

a. The Appeals Procedure is only available to applicants at the initial stages of the process whereby an officer has issued an "Officer Refusal Notice". The applicant has 30 days from the date of the "Officer Refusal Notice" to apply for an appeal to the decision, irrespective of when the applicant receives the Notice (which may be via email or in the post).
b. To appeal, the applicant needs to do any of the following:

i. answer and justify any observations made to the satisfaction of the officer
ii. provide information which is required by the officer
iii. put forward a strong case for an officer to re-view the decision taken
iv. give further clarification on how the application meets the normal qualifying criteria

c. An officer will take any appeal requests deemed valid to the committee Chairman/Vice Chairman to obtain approval to progress the application to committee or to refuse the appeal.
d. Applicants, who are appealing under 11b, must make sure they correctly justify why their project does meet the normal criteria and does not conflict with any of the Town Council's strategies.

Appendix 1: Grant Application Form (attached)

Appendix 2: Definition of a Voluntary Community Organisation

Appendix 3: Application scoring matrix

Appendix 2

Definition of Voluntary / Community Organisation

For the purposes of Saltash Town Council's Community Grants Scheme, a voluntary or community organisation is:

1. **Formal**. It has a formally-constituted character (excludes informal groups, households, families and friends) and may be a company limited by guarantee, a housing association, an unincorporated association, a friendly society, etc.
2. **Private**. It is not a part of government, established by statute or royal charter, or under a substantial degree of executive control by government (excludes universities and non-department public bodies); it may include consortia composed of local authorities and others (e.g. local regeneration and development bodies), if the consortium is formally constituted and, at the very least, given a name
3. **Self-governing**. It has its own decision-making system and usually a formal constitution with procedures for accountability to independent trustees or its own members or constituents (e.g., excludes any so-called "self-help groups" which are in fact directly run by clinicians)
4. **Non-profit-making and distributing**. It does not distribute any surpluses to owners or members but spends them on serving its basic purpose (excludes commercial concerns but includes organisations which charge users or the public for services, undertake contracts for statutory bodies or operate commercial subsidiaries which trade and transfer profits to parent organisations)
5. **Non-political**. It is not engaged in supporting candidates for political office (excludes political parties but includes campaigning and pressure groups, even though they are not eligible for charitable status e.g. Greenpeace, Child Poverty Action Group)
6. **Voluntary**. It has an element of involvement of volunteers (some voluntary and community organisations appear to be entirely reliant on paid staff; however, their trustees or committee members are, in fact, their only volunteers).

While this definition applies to formal organisations (those with constitutions or rules and which probably are registered with the Charity Commission, local authority or intermediary bodies, etc.), less-formal groups based in neighbourhoods or local communities are not necessarily excluded.

Appendix 3

Application scoring matrix

Key Priority Areas

Grants may be given for projects that fit into one or more of the following areas:

1	The promotion of tourism and leisure for both residents and visitors to the area with a community focus	
2	Supporting local safety campaigns	
3	Enhance existing events	
4	Promote pride in the community	
5	Highlight important local issues/history/culture to local residents and students	
6	Promote a sports -related initiative or event	
7	Increases visitors to Saltash and improves the local economy	
8	Promotes environmental issues which improve the local area	
	Total	

Scoring:

0 **Does not meet criteria**

1 **Partially meets criteria**

2 **Meets criteria**

Applications must score a minimum of ---------- to be eligible to receive grant funding

Agenda No. 19b

APPLICATIONS TO COMMUNITY CHEST -

The application form says bids will be assessed on:

- **Strength of the project** – how much it contributes to the general good of Saltash. (Applications that support Saltash Gateway's Community Development Plan, or STC priority areas such as: improving Fore St; improving community safety; improving play provision will be preferred). ***4 pts max***
- **Sustainability** of the project – what long term benefits it offers ***2 pts max***
- **Track record** (as indicated by e.g. membership, most recent accounts, annual reports, previous projects, support from other people/organisations, evidence of partnership projects) ***1 pt max***
- **Cost-effectiveness** (shown by e.g. alternative approaches, competitive quotes etc) **(Value for money)** ***1 pt max***
- What **contribution** the applicant/others are making to the project ***1 pt max***
- What **benefits it offers Saltash Town Council** (in terms of publicity for the scheme, or support for events or projects involving the Town Council). Applicants will be expected to show on their application how they will publicise Saltash Community Chest (in order to encourage others to apply). ***1 pt max***

Applicant	Project	Amount Applied	Received

Agenda No. 19b

Saltash Town Council

Grant Application Form

DATE APPLICATION SUBMITTED:

Contact Name:		
Position:		
Organisation:		
Contact Address:		
Telephone Number:		
E-mail:		
Status of Organisation:		
Charity/Company number (if applicable)	Charity No: Company No:	
Are there any Members of Saltash Town Council on your Committee? (if so, please list them)		
What geographical area does your organisation cover?		
How long has your organisation been in existence?	Less than one year	
	Between one and five years	
	More than five years	

Please note that you may be required to attend a meeting of the Policy and Resources Committee to answer questions on your application.

1. Organisation Background

	Date Applied	Project	Amount Applied for	Successful Y/N
Have you applied for or a grant from Saltash Town Council within the last 5 Years? (Please list – continue on a separate sheet if necessary)				
Please list the aims and objectives of your organisation				
What are the main activities of your organisation?				

	Yes / No or N/A
Is this a retrospective grant application?	
Are you part of a religious group?	
If application is for a Church – is it for anything other than a parish clock, Community Hall (used by all within the community) or environmental purposes?	
If application is for a School – Is it for anything other than environmental purposes or a project that does not benefit the wider community and is not in addition to statutory services?	
If application is from an Education, health or social service establishment – do you work in partnership with other groups?	
If application is from an Education, health or social service establishment – is project in addition to statutory services?	

2. Your project

Project	**Start Date**	/ /
	Finish Date	/ /
	Total Cost	£
	Grant Applied For	£

Project title:	
Description of project (please continue on a separate sheet if necessary):	
Where will the project/activity take place?	

Who will benefit from the project ? (What groups will benefit and approximately how many people will benefit in total)	
What evidence do you have that this project is required? (This might be survey work or statistical evidence)	
What support have you received for this project? (Please tell us about any expressions of support you have received from outside your organisation)	
How will the project be managed and how will you measure its success?	
Please give the timescale and key milestones for your project, including a start date and finish date.	

What arrangements do you have in place to ensure safeguarding of children and /or young people and/or vulnerable people (applicable only if your project involves working with this client group)	

3. **How you will pay for your project.**

What will the money be spent on? (Provide a full breakdown of project cost(s) identifying what cost(s) this grant would be spent on)	

Please list any applications you have made for funding from other organisations in the table below:

Organisation	Contribution Sought (£)	Applied (please tick as appropriate)	Granted (please tick as appropriate)

Please confirm if the bank account you project is using is in the projects name/organisation name with 2 authorised representatives required to sign each cheque?	

4. **Further information enclosed Checklist.**

	Enclosed (please tick)
A copy of your organisation's most recent bank statements (mandatory)	
Copies of all relevant Employer's, Building & Public Liability Insurance Certificates & Title Deeds if appropriate (mandatory)	
A letter head showing the organisation's address and contact details	
A copy of your constitution and articles of association (or similar documents if the above do not exist, showing the organisation's status)	
A copy of your organisation's latest set of accounting statements (if any exist)	
Copies of any letters of support for your project	
Other (please list)	

If any of the above documents have not been enclosed, please give reasons why in the box below:

5. Declaration by the applicant

I/we declare that, to the best of my/our belief, the information given on this application form and in any enclosed supporting document is correct.

I/we declare that, I/we have read the Town Council's Grant Policy and believe to the best of our knowledge, that we meet the criteria set out by the Policy.

I/we accept the following:

(i) that any false information we provide, even if provided in good faith, may lead to the withdrawal of the grant offered,

(ii) that any grant offered will be used only for the purposes set out in this application and

(iii) that we will provide reports on progress at the request of the Town Council

(iv) that should any grant offered, not be used in accordance with the terms and conditions set by the Town Council, we undertake on behalf of the organisation to repay the outstanding amount to the Town Council on demand.

Please be aware that the decision as to whether you have been successful in your application will be communicated to you shortly after the relevant Council meeting.

Signed:			
Print Name(s):			
Position(s):			
Date:			

Applicants should refer to the Privacy Notice on the Town Council Website www.saltash.gov.uk for details on how we use your data.

COMPLETED FORMS SHOULD BE RETURNED TO:
The Town Clerk, Saltash Town Council,
The Guildhall, 12 Lower Fore Street, Saltash PL12 6JX
Email: enquiries@saltash.gov.uk

OFFICE USE ONLY:	
Date received	
Received by:	
Application Reference:	
Date to P&R Chairman	
Approved to go to Committee	
Committee Date	
Decision/Minute number	
Amount awarded	
Application refused by P&R Chairman or refused by Committee	
Appeal notice issued	
Appeal received	
Approved for Committee	
Decision/Minute number	

Agenda No. 19c

Saltash Town Council

Policy/Procedure:	**Annual Governance Statement**
Date of Adoption:	**September /October 2018**

This is a Policy or Procedure document of Saltash Town Council to be followed by both Councillors and employees.

Current Status			
Version	2018/19	**Approved by**	
Date		**Date of approval**	
Responsible Officer		**Minute reference**	
Responsible Committee	FTC/P&R	**Review date**	September Annually - FTC

Version History			
Date	**Version**	**Author/Editor**	**Comments**

Review Record				
Date	**Type of Review**	**Date of completion**	**Summary of actions**	**Completed by**

Saltash Town Council

Annual Governance Statement 2018/19

Scope of Responsibility

Saltash Town Council is responsible for ensuring that its business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for.

The Council also has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised having regard to a combination of economy, efficiency and effectiveness.

Purpose of the Governance Framework

The governance framework in force during the year comprises the systems and processes, cultures and values by which the council is directed and controlled. It enables the council to:

- define the roles of Members and Officers so that each has clearly defined functions and roles
- uphold high standards of conduct for Members, Officers and Staff.
- provide procedures to ensure effective scrutiny
- provide a medium for communication with the public
- meet all legal requirements including those as an employer
- provide a System of Internal Control.

Purpose of the System of Internal Control

The system of internal financial control can provide reasonable and not absolute assurance that assets are safeguarded, sales and purchases are properly recorded, that all transactions are authorised and correctly recorded and that any material errors or irregularities are either prevented or would be detected within a timely period.

The system of financial control is based on a framework of regular management information, financial regulations, administrative procedures (including segregation of duties), management, supervision and a policy of delegation and accountability. The system is reviewed regularly.

The Governance Framework

Review, development and maintenance of the internal control system are undertaken by staff and members within the Council and by the external auditors in the annual audit letter and other reports. In particular, the system includes:

- comprehensive budgeting and costing systems
- circulation of regular financial reports which indicate actual expenditure

against budget forecasts
- clearly defined capital and revenue

The Town Council has adopted a policy of submitting to the Policy and Resources committee and Full Council a detailed report of the work of the internal auditor during the year.

Anti-Fraud & Corruption Strategy

An Anti-Fraud and Corruption Strategy has been approved by Council, including in it the relevant provisions of the Public Interest Disclosure Act 1998.

Member and Employee Protocol

This defines the responsibilities of the parties.

Protocol for Delegation of Financial Responsibility

The Town Council regularly reviews and amends its approved Protocol for Delegation of Financial Responsibility detailing levels of financial responsibility.

Thresholds for Tenders and Quotations

The Town Council has an agreed threshold for Quotations and Tenders within its Financial Standing Orders.

Risk Assessments

An annual internal audit business risk assessment is conducted by
The Chairman of the Policy and Resources Committee.

Processes/ICQs

Written processes for all aspects of the Town Council's finance operations is in place.

Review of Effectiveness

The Town Council has responsibility for conducting, at least annually, a review of the Governance Framework and the system of internal control. This review is carried out by the Chairman of Policy and Resources and the Clerk.

Significant Governance Issues

No significant Governance or internal control issues have been identified.

Appropriate action would be taken to ensure that any such matters were addressed, weaknesses eradicated and any systems revised.

Approval of Statement

This statement was reviewed/amended during the year and approved at a meeting of the Council held on **4th October 2018**.

Signed……

Chairman of the Council

Date……

Agenda No. 20

Tender & Extended Agreement For WPS To Act As Brokers

At the pre-renewal meeting I mentioned that WPS have engaged in a significant re-tender of our Town Council Scheme with a wide insurance market. Effectively from time to time we have had the request from individual Town Councils to review alternative markets, but we felt that to obtain maximum leverage we did do a complete re-tender of our entire Town Council Scheme with the widest possible insurance market.

This exercise was completed earlier this year and with the leverage of in excess of 200 Town Councils we were able to maximise interest from markets based on rating competitiveness, depth of policy coverage, security of insurer and claims and general administration. We presented to over 15 individual insurers including the primary Local Authority markets such as Allianz, Zurich, Axa, Ecclesiastical and Travelers. This was then shortlisted to three insurers namely Aviva, MS Amlin and Royal & Sun Alliance and the decision was made to move our entire scheme facility to Royal & Sun Alliance effective earlier this year.

In essence what this means for Saltash is that on expiry of your Long-Term Agreement with Aviva (next year) we will be recommending transfer on expiring rate to Royal & Sun Alliance with improved levels of coverage/sums insured and further continuity of rating stability. The appointment of Royal & Sun Alliance on expiry next year will also provide continuity for three years and total reassurance to Council that a complete and detailed re-tender of their insurances has been made by WPS based on the leverage of the largest independent scheme of Town Councils in England and Wales.

My recommendation next year of course will be to transfer to Royal & Sun Alliance based on these facts but this year to re-engage with WPS for a further three years to coincide with the Long-Term Agreement with RSA effective from the renewal 10th October 2019.

I hope this is in order and Council will formally agree to our proposal. Incidentally you will be interested to learn that we have had in excess of 30 Town Councils that have so far this year had LTA's expiring with Aviva and each and every one have transferred across to Royal & Sun Alliance.