# FINANCE AND GOVERNANCE COMMITTEE Fin REP 08.19

## Minutes of the Meeting of the Finance and Governance Committee held on 15th October 2019 at 2.30pm at the Committee Room at the Town Hall

Present; Cllrs Betts, Bradbury, Flunder Jordan and Ladd. Also present the Town Clerk.

**Agenda**

1. *Apologies for absence* – there were no apologies for absence.

2. *Declarations of Interest* –
   a. Cllr Ladd declared a personal interest in the matter relating to a request from the Xmas Lights group
   b. There were no Declarations of prejudicial interest
   c. There were no requests for dispensation

3. *Matters from the public* – there were no members of the public present.

4. *Minutes of the last meeting* - the minutes of the September meeting were approved and signed and had been noted at the previous Town Council meeting.

5. *Management accounts 2019/20.*
   Management accounts for the 6 months to September 2019 were presented by the RFO and discussed on a line by line basis with analysis against budget code for each individual account code. The actual spend for each account code was considered against agreed budget.
   There were no matters of concern to highlight noted by the Finance cttee within the 6-month accounts relating to expenditure.
   With regards to income due, the cttee noted the decision of Town Council with regards to rents due and outstanding, and those rent reviews awaiting completion.
   The month end management accounts and bank reconciliations for September 2019 were reviewed and approved by the Chair of the cttee and signed off as required.

6. *Insurance*
   Town Clerk updated members about the insurance claim for the CCTV monitoring information. Cost for suitable replacement £2180. **Insurance claim being progressed, and it is recommended that should the claim not be fully met, the sum of £2180 be spent to replace the necessary parts or any shortfall arising from the amount received from the claim itself to ensure full replacement.**

7. *Governance matters* –

   **Information Protection Policy / Information Security Incident Policy – See attached. It is recommended that these policies be readopted. No amendments required.**

**Laptops Policy – see attached. It is recommended that the laptops policy be amended to enable use in Town Council meetings. This will support the Climate Emergency initiative by enabling Councillors to opt in to receiving all council and cttee papers by e mail if they so desire.**

8 *Budget meetings for 2020/2021 budget*

Dates to work towards;
Precept to be submitted – January 2020
Council Briefings – Dec 2019 and Jan 2020
Finance and Gov cttee to start considering budget – 11th Nov 2019
RFO – to start budget – Nov 2019

Mention was made that as part of the budget discussions for 2020/21 the Town Council should consider the non -receipt of rent from ESC for the camping field, and that discussions with ESC should be expedited in this respect.

9. *Donations*

*Cllr Ladd left the meeting*

*To receive requests from;*

Xmas Lights cttee – are requesting contribution of £1000 towards the PA system and First Aid provision for the event. **Discussed by the cttee and it is recommended that the sum of £1500 be allocated from the donations budget to cover these bills.**

Community Emergency Group – the community emergency group are seeking an allocation of £500 from both Reydon PC and Southwold PC to enable them to replace the items in the emergency boxes and resupply full boxes to those who need them. It is intended that the Town Council undertakes the purchasing of the items required. **It is recommended that £500 be allocated to a community emergency budget.**
The Group would also like to have £25 per year allocated in case of need for replenishment of items in the boxes. This to be duly considered at the annual town council budget meetings.

Southwold and Reydon Society – request £100 donation for the repurchasing of dog bags. £100 also being requested from Reydon PC. It has been established that the bags are bio- degradable and **it is recommended that the Town Council allocates £100 from its donations budget for this purpose.**

*Cllr Ladd returned to the meeting*

The Town Mayor advised the cttee of the dog bag dispenser that Suffolk Secrets have placed outside their premises by the Market Place – Town Clerk was asked to ascertain costs of these dispensers.

10. *Strategy Priorities and Tactics* – The Finance and Governance cttee considered that their role within the priorities / tactics document. The cttee considered that they should act as the facilitator to oversee and provide the governance for the tactics of each priority, and to also act as the conduit to consider the financial implications within the town council budget.

*11. Date of next meeting* – Tuesday 19th November 2019 at 10.00am.

***Exclusion of Public and Press:*** *This cttee will consider information about individuals disclosure of which would breach the obligations of a council under Data Protection Act 1998, information that is commercially sensitive including tenders/ quotes, communications from professional advisers solicitor/ surveyors, architects which is protected by legal professional privilege, legal documents such as leases which are subject to contract. All such information is subject to confidentiality. Pursuant to section 1 (2) of the Public Bodied (Admission to Meetings) Act 1960 it is resolved, due to the confidential nature of the business to be transacted, the public and press leave the meeting during consideration of the following;*

*12.To receive update on legal matters including; outstanding rents, disputes etc.*
The cttee were brought up to date on outstanding debtors and the action being taken on each. The cttee were brought up to date with a potential dispute with an energy supplier on one of the councils' properties for which legal advice is presently being sought. The Chair to work with the Town Clerk to resolve the matter as soon as possible.

*There being no further business the meeting closed at 4pm*

*Chair*.....

*Dated*.....

The CCTV monitoring information. Cost for suitable replacement £2180. **Insurance claim being progressed, and it is recommended that should the claim not be fully met, the sum of £2180 be spent to replace the necessary parts or any shortfall arising from the amount received from the claim itself to ensure full replacement.**

**Information Protection Policy / Information Security Incident Policy – See attached. It is recommended that these policies be readopted. No amendments required.**

**Laptops Policy – see attached. It is recommended that the laptops policy be amended to enable use in Town Council meetings. This will support the Climate Emergency initiative by enabling Councillors to opt in to receiving all council and cttee papers by e mail if they so desire.**

Xmas Lights cttee – are requesting contribution of £1000 towards the PA system and First Aid provision for the event. **Discussed by the cttee and it is recommended that the sum of £1500 be allocated from the donations budget to cover these bills.**

Community Emergency Group – the community emergency group are seeking an allocation of £500 from both Reydon PC and Southwold PC to enable them to replace the items in the emergency boxes and resupply full boxes to those who need them. It is intended that the Town Council undertakes the purchasing of the items required. **It is recommended that £500 be allocated to a community emergency budget.**

Southwold and Reydon Society – request £100 donation for the repurchasing of dog bags. £100 also being requested from Reydon PC. It has been established that the bags are bio- degradable and **it is recommended that the Town Council allocates £100 from its donations budget for this purpose.**

## Southwold Town Council

## Laptops/Tablets Policy

- Tablets and laptops be allowed for use in Town Council/Committee/Working Group meetings to access council business related papers only.
- ~~Laptops are not permissible for use at Town Council meetings, but would be permissible at Working Group and Committee meetings.~~
- Mobile phones to be turned off or on silent at all meetings. If there is any reason why a member of the Council would require their mobile phone on during a meeting then this would be at the discretion of the Chairman of the Council.
- ~~The working group recommends that this policy be applicable to any person attending council meetings including; councillors, members of the public, WDC, Suffolk County Council, other organisations, members of the public, and guests at meetings.~~

Originally drawn up 26.2.13

Reviewed and Updated 31.3.15

Reviewed and confirmed 29.11.16
Reviewed and confirmed 23.05.17

Amended 29.10.19

# Southwold Town Council

# Information Protection Policy

**Adopted: April 2018**

**Review: October 2019**

**Contents**

## Document Control

| | |
|---|---|
| **Organisation** | |
| **Title** | |
| **Creator** | |
| **Source** | |
| **Approvals** | |
| **Distribution** | |
| **Filename** | |
| **Owner** | |
| **Subject** | |
| **Protective Marking** | |
| **Review date** | |

## Document Amendment History

| Revision No. | Originator of change | Date of change | Change Description |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

25

## 1 Purpose

1.1 Information is a major asset that Southwold Town Council has a duty and responsibility to protect.

1.2 The purpose and objective of this Information Protection Policy is to specify the means of information handling and transfer within the Council.

## 2 Scope

2.1 The Information Protection Policy applies to all Councillors, Committees, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Southwold Town Council purposes.

2.2 Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video
- speech

## 3 Information Storage

3.1 All electronic information will be stored on centralised facilities to allow regular backups to take place.

3.2 Information will not be held that breaches the Data Protection Act (1998) or formal notification and guidance issued by Southwold Town Council. All personal identifiable information will be used in accordance with the Caldicott Principles.

3.3 Records management and retention policy will be followed.

3.4 Staff should not be allowed to access information until line managers are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

3.5 Databases holding personal information will have a defined security and system management policy for the records and documentation.

3.6 This documentation will include a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection Notification.

3.7 Files which are listed by Southwold Town Council as a potential security risk should not be stored on the network, except for in designated application storage areas. To facilitate this Southwold Town Council will implement an electronic File security solution.

4

**Disclosure of Information - Computer and Paper Based**

4.1 The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is be reported to the Data Control Officer (Clerk) who will take appropriate action.

4.2 Do not remove printed information from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances

4.3 Protectively marked, personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

4.4 Disposal methods for waste computer printed output and other media must be in accordance with Southwold Town Councils disposal policy.

4.5 Distribution of information should be via the most secure method available.

**5 Disclosure of Information – Telephone, Fax and E-mail**

5.1 Where this involves the exchange of sensitive information then the following procedures will be applied.

**6 Telephone calls:**

6.1 Verify the identification of members before disclosing information. If in doubt, return their call using a known telephone number.

6.2 For external callers, verify their identity and their need to know the requested information. Telephone them back before releasing information and ask the caller to provide evidence of their identity (this could be passport, driving license, household bill).

6.3 Ensure that you are authorised to disclose the information requested.

6.4 Ensure that the person is entitled to be given this information.

6.5 Ensure that the information you give is accurate and factual.

**7 Fax transmissions:**

7.1 Fax should not be used to transmit personal or sensitive information.

## 8 Disclosure of information by email:

8.1 Personal or sensitive information is at risk if sent outside of the Council's network.

8.2 If an e-mail is sent to an address that is not a Council domain address the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted.

8.3 Email should not be used for sending personal or sensitive information unless technical measures are in place to keep the message secure.

8.5 The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.

8.6 No identifiable personal information should be included when sending on emails.

8.7 The recipient of Southwold Town Council emails are prohibited from being forwarded, copied or blind copied to any third party within or outside of the Council.

8.8 Any Councillor email contact with a member of the public shall be directed to the Councils Office for the attention of Southwold Town Council.

## 9 Sharing of Personal Information

9.1 Information relating to individuals shall not be shared with other authorities without the agreement of the Data Control Officer.

9.2 Staff should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

# Southwold Town Council

# Information Security Incident Policy

April 2018

Reviewed October 2019

## Contents



30

## Document Control

| | |
|---|---|
| **Organisation** | |
| **Title** | |
| **Creator** | |
| **Source** | |
| **Approvals** | |
| **Distribution** | |
| **Filename** | |
| **Owner** | |
| **Subject** | |
| **Protective Marking** | |
| **Review date** | |

## Document Amendment History

| Revision No. | Originator of change | Date of change | Change Description |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 1 Purpose

1.1 This document defines an Information Security Incident and the procedure to report an incident

## 2 Scope

2.1 This document applies to all Councillors, Committees, Departments Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Southwold Town Council purposes.

## 3 Definition

3.1 An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it, or data is at risk from corruption.

## 4 An Information Security Incident includes:

- The loss or theft of data or information
- The transfer of data or information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent
- Unwanted disruption or denial of service to a system
- The unauthorised use of a system for the processing or storage of data by any person.

## 5 When to report

5.1 All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported as soon as they happen.

## 6 Action on becoming aware of the incident

6.1 Follow the information security procedure, according to the type of incident.

## 7 How to report

7.1 The Responsible Financial Officer must be contacted by email or telephone. They will log the incident and forward it on to the relevant departments.

7.2 The Responsible Financial Officer will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident
- The type of data or information involved

32

- Whether the loss of the data puts any person or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of data or equipment affected
- Type and circumstances of the incident.

7.3 Your line manager must also be informed to enable them to investigate and confirm that the details represent a valid security incident as defined above. The outcomes of these actions are to be reported to the Responsible Financial Officer for inclusion in the incident details for the Responsible Financial Officer's investigation.

## 8 What to Report

8.1 All Information Security Incidents must be reported.

## 9 Examples of Information Security / Misuse Incident Protocols

9.1 Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

### 9.2 Malicious Incident

- Computer infected by a Virus or other malware, (for example spyware or adware)
- An unauthorised person changing data
- Receiving and forwarding chain letters – Including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Social engineering - Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).
- Unauthorised disclosure of information electronically, in paper form or verbally.
- Falsification of records, Inappropriate destruction of records
- Denial of Service, for example
- Damage or interruption to Southwold Town Council equipment or services caused deliberately e.g. computer vandalism
- Connecting non-council equipment to the council network
- Unauthorised Information access or use
- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Printing or copying confidential information and not storing it correctly or confidentially.

### 9.3 Access Violation

- Disclosure of logins to unauthorised people
- Disclosure of passwords to unauthorised people e.g. writing down your password and leaving it on display
- Accessing systems using someone else's authorisation e.g. someone else's user id and password
- Inappropriately sharing security devices such as access tokens

33

- Other compromise of user identity e.g. access to network or specific system by unauthorised person
- Allowing Unauthorised Physical access to secure premises e.g. server room, scanning facility, dept area.

### 9.4 Environmental

- Loss of integrity of the data within systems and transferred between systems
- Damage caused by natural disasters e.g. fire, burst pipes, lighting etc
- Deterioration of paper records
- Deterioration of backup tapes
- Introduction of unauthorised or untested software
- Information leakage due to software errors.

### 9.5 Inappropriate use

- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Personal use of services and equipment in work time
- Using unlicensed Software
- Misuse of facilities, e.g. phoning premium line numbers.

### 9.6 Theft / loss Incident

- Theft / loss of data – written or electronically held
- Theft / loss of any Southwold Town Council equipment including computers, monitors, mobile phones, Blackberries, Memory sticks, CDs.

### 9.7 Accidental Incident

- Sending an email containing sensitive information to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature, e.g. containing pornographic, obscene, racist, sexist, grossly offensive or violent material
- Receiving unsolicited mail which requires you to enter personal data.

### 9.8 Miskeying

- Receiving unauthorised information
- Sending information to wrong recipient.

## 10 Escalation

10.1 Serious incidents will be escalated via the national WARP scheme if determined to be of national value.

**Authorisation**

This policy has been authorised by:

Signature ..... Date .....

Name: Position:

35

# CAMPING FIELD FERRY ROAD – UPDATE 23/10/19

This matter is not about any part of Southwold Harbour Lands.

On 24 June last, Cllrs Windell and Bradbury held a meeting with ESC Officers Andy Jarvis and Kerry Blair at Riverside, Lowestoft, in relation to STC's concerns that money was due, by way of annual rent, for the field which had been populated (at Will), increasingly, over many years.

A further meeting was promised to consider potential proposals from ESC for a joint venture for the current field as well as expanding further into ***Havenbeach Marsh.*** This further meeting has not taken place – Kerry Blair, has advised that this will happen once a Business Case for the Static Caravan Site, (expected mid-November), has been completed.

Based on July to August occupancy, when the Camping Field is full (and there are, already advance bookings for this entire period in 2020) on 104 pitches a minimum income of:

**104 (no. pitches) x £25 over sixty-two days = £161,200**

STC receives no income from ESC's **Tenancy at Will**, of the Camping Field and Members are reminded that as far back as 2003, the District Auditor was recommending a rental of £23k per annum be paid.