SEVENOAKS TOWN COUNCIL

IT SECURITY POLICY

Why is a Security Policy Required?

1 Information systems are important Council assets. However, information security threats are becoming more widespread. Some of these, such as virus infections, could cause major damage to the systems we use and the cost in time and money to repair the damage could be significant.

2 The Council must also act legally with regard to the use of software. Unauthorised, illegally copied or other unofficial software must not be used. To do so makes us liable for prosecution.

3 We have duties and responsibilities under the Data Protection Act and other legislation which defines some activities as criminal offences.

General Security

4 You must ensure that portable computers and any other easily-stolen equipment is securely locked away when not in use.

5 You must only remove from STC premises, computer equipment for which you have appropriate authority.

6 You must change your personal password(s) on a regular basis.

7 If you leave your terminal or PC unattended for up to 10 minute, a password-protected time-out or screen saver must be operating.

8 Do not use unauthorised software on any Council machine.

9 Do not bring disks from home to use on Council machines.

10 The Council disks must not be removed from the office or used on non-Council machines.

Internet

11 Internet connection is for business use only. The only exception is for personal use during normal working hours in the Officer's own time.

12 Visiting and Downloading of indecent pictures, racist or sexist material from the Internet will be considered an act of gross misconduct.

Downloading from the Internet

13 The downloading of files, shareware or freeware to the organisation's processors is authorised for business use only and is considered a high risk activity. Any applicable licence conditions must be complied with. The downloading of games, screensavers and other "fun" software is not considered to be legitimate business activity. These are more likely to contain viruses and programming errors which can severely compromise the organisation's systems.

Email

14 External and internal email is to be used for business use only. The only exception is for personal use during normal working hours in the Officer's own time.

15 Please conserve space on the server with regular housekeeping of your messages – both received and sent. Remember to delete files from your "Inbox" and "Sent Items" when you no longer need them. Your Inbox should be used as a temporary location only – either copy the file to a more suitable location or print a hard copy for retention.

Email Content

16 Messages sent on the email systems are to be written in accordance with the standards of any other form of written communication and the content and language used in the message must be consistent with best practice. STC will not tolerate the use of email or related services to communicate material which disparages others on grounds of race, gender, nationality, culture, religion, sexual orientation, age, disability or any other personal characteristics. This includes communications, jokes, pictures or stories which are harassing, demeaning or offensive to any individual or group.

Confidentiality

17 Email is not a secure system of communication. Sensitive or confidential information should not be sent externally by email.

Email Attachments

18 Email attachments should not be opened unless the recipient knows who they are from and is expecting to receive them.

19 File attachments sent internally or externally are to be zipped using Winzip if over 500k.

20 File attachments on emails received must be detached and saved in an appropriate folder before opening.

21 Files may then be opened/printed from the network directly allowing Council virus checking software to confirm safety of file before use.

Ordering Goods and Services

22 Any goods and services may only be ordered or purchased via the internet under written authority from the Town Clerk and only from a secure site.

Copies of this memorandum will be placed in the individual staff records. Any proven breach of the provisions of paragraphs 4, 5, 12, 16 will be regarded as an act of gross misconduct leading to dismissal.

I confirm that I have read and understood the Council's IT Security Policy.

Signed ..... Date .....