DORCHESTER TOWN COUNCIL

INFORMATION TECHNOLOGY SECURITY POLICY

The Council relies heavily on the use of computers and computer systems. It is therefore important that these facilities are used in a secure, efficient and legitimate manner. This means that all computer users, including permanent and temporary employees, Council Members and people or organisations acting on behalf of the Council, must observe three key components of computer security:

- Confidentiality
- Integrity
- Availability

Confidentiality means that sensitive information must be protected from unauthorised disclosure.

Integrity means that the accuracy and completeness of information and computer software must be safeguarded.

Availability means that information and vital services are available to users when required.

To help maintain an acceptable level of Information Technology Security the Council –

- retains the services of an experienced external consultant to act as systems administrator;

- requires staff members and other users to sign up to the attached acceptable use policy on internet and e-mail;

- protects its computer systems against viruses and unauthorised hackers via a suitably equipped server through which all external electronic contents are made;

- only installs software legitimately procured on the Council's systems and ensures that it is used in accordance with the user licences;

- where possible restricts access to computer programs and files to those whose duties require access to the applications concerned;

- ensures that its data is regularly backed up in accordance with best practice both on- and off-site and stores the local back-up tapes in a fire-resistant environment;

- is developing a Business Continuity Plan to ensure the continuity of the Council's activities in the event of a disaster (e.g. catastrophic hardware failure, fire, flood etc) as part of its ongoing attention to risk management.

This policy requires that employees comply with the following points –

- confidential and personal information must be kept secure, (whether held electronically or in manual records);

- passwords should only be issued to users who need to use them;

- no software other than that legally procured by or on behalf of the Council should be loaded or used on Council equipment;

- no-one should take computer equipment away from their usual place of work without formal authorisation;

- back-up copies should be made of all important files and the copies should be stored in a safe place in accordance with recommended management practices;

- copying of software is not permitted;

- access to computer facilities with criminal intent is not permitted;

- damage to or unauthorised modification of data is not permitted and may be a criminal offence under the Computer Misuse Act 1990;

- unauthorised disclosure of personal information contrary to the provisions of the Data Protection Act, is not permitted.

Secure Access

To ensure security of access to the IT systems –

- passwords should be used where possible;

- users whose computers are logged into password-protected applications should lock their machines or exit from the applications if leaving their workstation for any period of time;

- access by third parties should be properly authorised and supervised.

Password Guidance

- Whenever possible use passwords to protect systems and only issue the password to people who need to know. Passwords should be kept secure, they should not be written down and staff should ensure that nobody is watching when they are being typed in. Passwords should never be included in an automated login process.

- Passwords should be changed on a regular basis by all users and always on the computer previously used by a member of staff who has left the Council's service.

- Passwords should preferably be over six characters long and contain some upper and lowercase letters and numbers if possible.