Oundle Town Council ~ Information Security Policy

PRINCIPLES & PURPOSE

The purpose of the Council's Information Security Policy is to provide a framework on the approach to the risks involved, assessment criteria and the provision of appropriate measures. It will ensure a consistent high standard of security, state the expectations of all staff and provide a sound secure basis upon which information services can be provided.

Our policy is based on the following principles:

Confidentiality Protecting sensitive information from unauthorised access or disclosure;
Integrity: Safeguarding the accuracy and completeness of information and processes;
Availability: Ensuring that information is available to authorised people when needed;
Suitability: All systems are suitable for the required tasks.

The principle of confidentiality will be upheld throughout the Council and be reflected in its protocols and system procedures.

There are a number of legislative items with which the Council must comply; however, the following are significant:

1 Data Protection Act 1998 2 Freedom of Information Act 2000

Our information and IT systems and networks that support it are important business assets. Their confidentiality, integrity and availability are essential in maintaining our respected organisational image, efficiency and legal compliance. Oundle Town Council operates networked IT facilities and has a Service Level Agreement with Pro-Digital Systems Limited for provision and maintenance. Security issues are covered by back ups being taken regularly and stored off site.

The Council will from time to time review its process and procedures and assess the legitimacy of its Information Security Policy in line with developments in UK and European law.

PROTOCOLS

1. System Security Processes and Procedures

The Council will provide and maintain security processes and procedures for all key information systems'. The procedures will uphold the principles of confidentiality, integrity, availability and suitability and be assessed for their impact upon other systems and services.

The security procedures will provide preventative measures to reduce the risks to the system, the information held within the system and the service it supports.

Continuity plans will be developed and maintained for each system to ensure the principles are sustained and enable the continuation of services following failure or damage to systems or facilities.

The Clerk will be responsible for the implementation and promotion of the procedures.

Oundle Town Council ~ Information Security Policy

2 Informing the 'client'

The Council has a duty under the Data Protection Act 1998 to inform clients of the kind of purposes for which information about them is collected and the organisations to which information may need to be passed

In order to ensure a consistent approach on how clients are informed of their rights, correspondence/forms to the client, will include a statement on the use of client information e.g.,

We ask you for information about yourself so that you can receive appropriate services. Your personal information will only be used for legally registered purposes and only available to authorised recipients.'

3 Physical Security

Adequate and practical access controls will be provided in all areas in which personal and business data is stored or used. Unattended rooms should be secured at all times with window blinds and locked doors as a minimum security requirement.

All documents disclosing identifiable information will be transported in sealed containers e.g. envelopes.

Within their level of authority, staff will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as, laptop computers, should not be left unattended or unsecured and paper records should not be left within public view.

The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment e.g. adequate ventilation for computers servers, appropriate fire precautions where paper records are stored, controlled access doors.

The Council will comply with Health and Safety and Fire Safety legislation and policies when implementing security controls.

4. Logical Security

All computerised information and systems must be regularly backed up to a secure environment. Appropriate staff only will be allowed access to appropriate levels of data within the systems.

All computerised information systems will be password controlled. All system passwords will be prompted for change at regular intervals, as suggested within ISO 17799.

All passwords will be treated with the strictest confidence and users will not divulge their password to any unauthorised person.

All sensitive data will be password protected.

Only officially purchased and approved software will be loaded onto Authority computers to lessen the risk of virus infection and loss of the Council's systems. Unofficial and unapproved software will be removed from Council computers.

5 Copyright and licences

Oundle Town Council ~ Information Security Policy

The Clerk is responsible for ensuring all computer software packages and non-electronic media for use within an information environment are used in accordance with the terms and conditions of use as set out in the licence agreement.

6 *E-Mail, Telephone and Fax*

The Council will develop a policy for the use of e-mail, telephone & fax by staff.

7 Disposal and movement of equipment and media

Any media or IT equipment disposed of by the Council will not contain any data or code that could allow an individual to be identified from it.

The disposal of equipment will be made under a controlled and documented environment satisfying the requirements of the Data Protection Act 1998. The disposal of media, such as, diskettes and tapes, must ensure that data cannot be recovered. Disposal of such media through the "everyday" waste collection is not permitted. The Council will implement processes to ensure appropriate disposal of such media.

An inventory of all Council computer equipment will be maintained. Any equipment or media disposed of or relocated (other than portable equipment) must be reported to the Finance and Administration Manager.

8 Personal Computers

Computer users have responsibility for the security of the equipment in his/her care and shall not commit an act to compromise the data or Information Security Policy. Diskettes, CD's and other data storage devices, which have not been checked for viruses, must not be used to load software onto PCs.

Computer users will be made aware of their responsibilities through this policy

9 Internet

The Council believes that the use of the Internet is beneficial to staff and will adopt a reasonable approach to its use. However, it will be a disciplinary offence to use the Internet to download, view or access inappropriate material or web sites (as established through legislation).

The Authority will develop protocols to ensure the security of data and equipment when staff work at home.

10 Staff Responsibilities

The Council will make every reasonable effort to ensure that staff are aware of their responsibilities for the security of information. However, each member of staff is responsible for ensuring that Security Policy is adhered to and report any breaches of security.

11 Incident Reporting

Incidents affecting security must be reported to the Administration and Finance Manager as quickly as possible.