WARWICK DISTRICT COUNCIL

TO: PERFORMANCE REVIEW SUB-COMMITTEE - 19th JANUARY 2000

SUBJECT: INFORMATION SECURITY POLICY, CODE OF PRACTICE AND GUIDELINES

FROM: IT STEERING GROUP

1. PURPOSE OF REPORT

1.1. To seek Members' approval for implementing a new Information Security Policy, Code of Practice and related good practice guidelines to replace the existing Computer Security Policy and Guidelines.

2. BACKGROUND

2.1. The existing Computer Security Policy and Guidelines dates from 1995 with only a few minor amendments since. Various developments have rendered this document obsolete, including:-

(a) new legislation - in particular the Data Protection Act 1998;

(b) proliferation of desktop facilities and local area networking;

(c) new technologies and expansion of availability (including mobile computing, remote dial-up, e-mail, Intranet/Internet and Members' facilities);

(d) minimum expected standards under the British Standard on Information Security Management (BS7799).

2.2. It is not intended at present to seek any formal accreditation under BS7799. The new draft Policy is designed to observe the basic principles of the Standard relevant to all organisations irrespective of size. These are enshrined in 10 minimum controls which, briefly stated, are:-

1. Policy document
2. Clearly defined allocation of responsibilities
3. Education and training programme
4. Clear procedures for reporting and acting on security incidents
5. Effective anti-virus measures
6. Business continuity planning process
7. Control of proprietary software copying
8. Safeguarding of organisational records
9. Compliance with legal and regulatory issues
10. Compliance with security policy

3. NEED FOR SECURITY POLICY

3.1. In maintaining an effective defence against IT fraud, abuse and other hazards, awareness among staff and Members is a vital factor. For this reason, the Council must set a clear policy on the standards to which all staff and Members are required to conform when accessing systems or otherwise using Council IT facilities.

4. DATA PROTECTION POLICY

4.1. The proposed Information Security Policy and related documentation will **not** replace the Data Protection Policy now in force. Some overlap between the two is inevitable and a degree of duplication will be noticeable, although this is seen as helping to reinforce security awareness.

5. INFORMATION SECURITY CODE OF PRACTICE (Appendix I)

5.1. In recognition that the Information Security and Data Protection Policies will operate side by side, it is proposed that an 'umbrella' Information Security Code of Practice be implemented

together with the Policy. The Code of Practice has a further purpose of ensuring that the Council can demonstrate that the Information Security Policy and the consequences of failure to comply with it have been fully communicated to staff and Members. Failure in this could jeopardise disciplinary action or prosecution where any actual breach becomes known or suspected.

5.2. It is therefore proposed that all staff and Members be issued with a copy of the Code of Practice, each being required to sign an acknowledgement of having received and read it.

6. INFORMATION SECURITY POLICY (Appendix II)

6.1. A limited distribution of the Policy in paper form is proposed which will include Members, Heads of Business Units, divisional managers and section heads, while at the same time publishing the Policy on the Intranet.

7. INFORMATION SECURITY GUIDELINES

7.1. As part of implementing the Information Security Policy, the Head of IT will from time to time publish guidelines on good security practice for all staff and Members. Guidelines listed at the end of the draft Policy have already been prepared and will, subject to approval of the Policy, be published on the Intranet.

7.2. In addition, it is proposed that the guideline entitled **Summary User Checklist (Appendix III)** be issued with the Code of Practice in an illustrated leaflet form.

8. CONSULTATIONS

8.1. Representatives of UNISON and MPO have been consulted on the draft Policy and Code of Practice. No objection to implementation has been raised nor any amendment requested. Some overlap with the draft Whistleblowing Policy was noted but with no conflict arising.

9. KEY ISSUES STRATEGIES

9.1. The Council's ability to demonstrate effective information security management is seen as a prerequisite to maintaining the confidence of the community and partnership bodies on which achievement of the Key Issues Strategies clearly depends.

10. RECOMMENDATIONS

10.1 Members are asked to support:-

(a) implementation of the Information Security Policy and Code of Practice.

(b) proposals for publication and distribution of the Policy, Code of Practice and Summary User Checklist.

Background Papers: IT Steering Group 29/10/99 - Report and Minutes (Item 3)
BS7799 - Code of Practice for Information Security Management
Computer Security Policy and Guidelines
Model e-mail, internet, etc. policies (various sources)

Areas in the District affected: All

Author and Contact: Ian Wilson, Senior Internal Auditor
Telephone: (01926) 884746; E-mail: iwilson@warwickdc.gov.uk

WARWICK DISTRICT COUNCIL

INFORMATION SECURITY CODE OF PRACTICE FOR EMPLOYEES AND MEMBERS

1. Introduction

1.1. With ever greater reliance on information technology in the day to day work of employees and

Members in conducting Council business, the dangers posed by misuse of the technology place a duty on the Council to manage its information in a secure manner. The Council has implemented a system for information security which draws on British Standard BS7799 (Code of Practice for Information Security Management) and is intended to conform to the minimum key controls detailed in Part 1 of the Standard.

1.2. This Code of Practice is intended to advise staff and Members of Warwick District Council of the standards of security to which they **must** conform at all times when accessing any of the Council's information systems and/or when using any of the Council's information technology facilities. These standards are prescribed to ensure that such activities of employees and Members:-

(a) remain within the law;
(b) do not threaten the integrity of the Council's systems nor the information they process;
(c) do not compromise the bona fide interests of the Council;
(d) do not lead to conflict among staff and/or Members.

1.3. Breach of any part of this Code will be deemed misconduct and may result in one or more of the following actions:-

(a) withdrawal of the relevant facility;
(b) disciplinary action and possible dismissal;
(c) criminal prosecution and/or civil action.

2. Relevant Policies

2.1. All employees and Members must comply with the **Information Security Policy**, a copy of which is available from your relevant manager, IT Liaison Officer or from the Information Security page on the Council Intranet. The Information Security Policy supersedes the previous Computer Security Policy.

2.2. All employees and Members must comply with the **Data Protection Policy.**

3. Information Security Guidelines

3.1. The attention of employees and Members is drawn to the Information Security Guidelines which are published in association with the Information Security Policy and advise on good practice in managing and operating information systems and technology in a secure manner. These Guidelines are indexed at the end of the Information Security Policy and are available from the Council Intranet Information Security page.

3.2. Employees and Members may be held personally accountable for any complaint, claim, or legal action against the Council where it can be shown to have been a direct consequence of failing to observe good practice as set down in the Information Security Guidelines.

4. Access to Systems

4.1. No employee or Member may access any computer system operated by the Council unless authorised to do so by the relevant System Owner. Such authorisation will normally be in the form of a user ID created for the individual employee/Member or for a generic group of users, protected in both cases by a password. Group IDs should normally be restricted to users who are not permitted to amend data within the systems.

4.2. Unless notified to the contrary by the System Owner, any user ID will be deemed personal for the sole use of the individual employee/Member.

4.3. Employees and Members must not divulge passwords for personal user IDs to any other persons except where specifically required by the IT Unit for diagnostic purposes (in which case the password must be changed immediately on completion of the diagnostic procedure).

4.4. Employees and Members are responsible for ensuring that they do not provide unauthorised persons with the means to access any Council systems.

4.5. Except for IT personnel (in circumstances where diagnostic routines require such disclosure), no employee or Member must request any other employee or Member to disclose their personal user passwords.

4.6. Where group IDs are used, permission must be obtained from the System Owner before disclosing passwords to any persons.

4.7. The attention of employees and Members is drawn to Information Security Guideline 23 which deals with good practice on using passwords.

5. E-Mail

5.1. The Council reserves the right to monitor e-mail messages and file attachments sent from internal Council addresses to external 'mail boxes' (and vice versa) as necessary to safeguard the interests of the Council, its employees and Members.

5.2. The regulations for use and disclosure of passwords in Paragraphs 4.2. to 4.6. above apply equally to Council e-mail facilities and must be observed by all employees and Members.

5.3. Employees and Members must not in any way allow their personal Council workplace e-mail addresses to be accessible to any other persons to send e-mails. Similarly, users of 'group' e-mail addresses must not allow access by any unauthorised persons.

5.4. Employees and Members must not send e-mails other than in their own name or in the name of 'group' mailboxes that they are authorised to use.

5.5. The attention of employees and Members is drawn to Information Security Guideline 18 which deals with good practice on using e-mail and faxes.

6. Internet

6.1. The Council reserves the right to monitor Internet sites accessed from any Council facility and material obtained.

6.2. Employees and Members must not connect any Council computing facilities to the Internet except as directed by the Head of IT and, in the case of employees, authorised by the Head of Business Unit.

6.3. Internet access IDs are <u>always</u> personal and employees and Members must under **<u>no</u>** circumstances divulge their passwords to any other persons.

6.4. No employee or Member must request any other employee or Member to disclose their

Internet password.

6.5. Employees and Members must not in any way allow their Internet ID to be used by any other persons. All logs of Internet activity carry the address of the logged on user in each case and that user will be held personally responsible where such activity breaches any part of this Code.

6.6. Employees and Members must not attempt to access sites that are pornographic or 'adult' in nature. The Council reserves the right to withdraw the facility immediately from any employee or Member suspected of such activity.

6.7. Employees must not use the Internet during working hours other than for legitimate Council business.

6.8. Use by employees of the Internet from Council facilities for private purposes is permissible **during free time** at the discretion of the individual Heads of Business Unit.

6.9. The Council accepts no responsibility for any loss suffered by any person resulting from entering into transactions on the Internet irrespective of whether Council facilities are used for the purpose. This includes placement of debit/credit card orders.

6.10. The attention of employees and Members is drawn to Information Security Guideline 16 which deals with good practice on using the Internet and Intranet.

7. Personal Computers

7.1. No software of any kind must be introduced to Council PCs, laptops or file servers except with the approval of the Head of IT. This prohibition also includes downloading off the Internet.

7.2. No copies must be taken of software installed on Council PCs, laptops or file servers except as directed by the IT Unit for back-up purposes only.

7.3. Permission must be sought from employees' line managers before taking any Council portable computer equipment away from the normal work place.

7.4. Council portable computer equipment taken home is for the sole use of the employee/Member in each case and access must under **no** circumstances be given to any other persons in the household.

7.5. No diskettes, CD-ROMs, etc from external sources must be introduced to any Council PC, laptop or file server without first being referred for scanning by an approved virus scanning station (IT Liaison Officers within the Business Units have such facilities).
Note: ***This applies equally to diskettes containing files that have been created or edited on the employee's/Member's home PC irrespective of whether or not they relate to Council business.***

7.6. All employees and Members processing information for Council purposes must ensure that PCs, laptops and networks holding that information, whether Council-owned or otherwise, are appropriately secured to prevent unauthorised access.

7.7. The attention of employees and Members is drawn to Information Security Guideline 17 which deals with good practice on using PCs, laptops, etc.

APPENDIX I

Information Security Policy

WARWICK DISTRICT COUNCIL

1. INTRODUCTION

1.1. This Policy is intended to outline the required framework for the maintenance of secure information systems within Warwick District Council, hereafter referred as the Council.

1.2. This Policy is in accord with corporate policies on information security and the British standard BS7799 - Code of Practice for Information Security Management. This Policy has been endorsed by the Council.

2. PURPOSE OF INFORMATION SYSTEMS SECURITY

2.1. The purpose of security in any information system, computer installation or network is to preserve an **appropriate** level of:-

Confidentiality access is confined to those with specified need and authority to view and/or change the information;

Integrity the system, installation, network is operating according to specification and in the way the user expects it to operate;

Availability the system or service is available, and the output delivered to the user who needs it, when it is required.

2.2. The level of security required in a particular system will depend upon the risks associated with the system.

3. NEED FOR SECURITY AND A SECURITY POLICY

3.1. Data stored in the information systems of the Council represent an extremely valuable asset, essential to the effective and continuing operation of the Council. The increasing day to day reliance of the Council on information technology makes it imperative that **all** information systems are developed, operated, used and maintained in a safe and secure way.

3.2. The increasing use of laptop computers and the need to transmit information across networks both within the Council and to/from external organisations renders the data more vulnerable to accidental or deliberate modification or disclosure. Some of the information systems contain highly critical data which if not handled securely could present a serious problem to the Council, its employees, Members and customers.

3.3. The purpose of this Security Policy is to establish an organisational structure and framework of controls from which detailed security procedures can be implemented. To this end, the document contains a number of Policy Statements which are supplemented by a series of security guidelines. The guidelines are for reference by Heads of Business Unit, Information Security Co-ordinators, IT Liaison Officers, line managers etc. in ensuring that their systems are protected in the most appropriate and effective way.

4. SCOPE

4.1. The term **Information**, shall be considered to include the use of media such as papers,

printed output and information collected for input, fax output, databases, tapes, discs, CD's as well as conversations and any other methods used to convey knowledge and ideas relating to the Council. All information systems are subject to this Policy - be they financial or non-financial, be they central mainframe systems, departmental server based applications or simple systems running on a PC. The Policy applies to information which is processed on computers owned by the Council and also information that is retrieved, accessed, transmitted to/from other organisations using modems, network gateways and fax machines. It also applies to information processed in respect of Council affairs by Members and employees on **any** equipment irrespective of the ownership and location of that equipment.

This Policy applies to all full time and part time employees and Members of the Council, and to all contracted third parties in respect of information relating to the Council whether this is on Council premises, at their offices or from home.

5. POLICY STATEMENTS

5.1 Responsibility for Information Security

SECURITY IS THE RESPONSIBILITY OF EVERYONE

5.1.1. Whilst information security policies, guidelines and measures have to be devised, implemented and managed by specific functions and individuals, **everyone** within the Council has a responsibility to ensure that they take basic steps to safeguard the security of the information that they are using and seeing. To facilitate this, this Policy and associated guidelines have been summarised into one checklist designed to give day to day reminders to users. **Line Managers** must ensure that all staff under their control receive and adhere to this checklist.

5.1.2. The IT Steering Group has nominated an **Information Security Officer** who is responsible for:-

(a) co-ordinating the operational implementation and monitoring of this Policy and associated guidelines;

(b) arranging for the review and monitoring of security incidents and investigation of major breaches of security;

(c) arranging for the Policy and guidelines to be updated as new technology and systems change the risk scenario.

(d) co-ordinating awareness initiatives across the Council to maximise impact and effectiveness.

5.1.3. The **Heads of Business Unit** will overview the implementation of, and adherence to, this Policy within their respective Business Units. Each Head of Business Unit will nominate an officer of appropriate seniority as **Information Security Co-ordinator** who will be responsible for:

(a) implementing and monitoring compliance with the Policy and associated Code of Practice and guidelines in conjunction with line managers;

(b) promoting and advising on information security matters.

5.1.4. **Line managers** have day to day responsibility for ensuring that their staff understand and comply with this Policy and associated Code of Practice and guidelines.

5.1.5. The **IT Business Unit** has specific responsibilities for managing the security of the IT service that it provides, but is not responsible for the security of the information that they process. That is the responsibility of each **System Owner,** whose role is to establish and manage the security of the information in their application(see 5.6 for details).

5.1.6. The Council's **Internal Audit** service is responsible for:-

(a) testing compliance with Council policies, guidelines and procedures;

(b) working with the IT Business Unit to assess, control and manage the risks of the Council's IT infrastructure;

(c) ensuring, in consultation with the Heads of Business Unit, that there is appropriate audit coverage for existing systems and that the risks in the implementation of new applications are duly assessed and appropriate measures taken.

5.2 Compliance and reporting of suspected incidents

5.2.1. Failure to comply with this Policy could result in disciplinary action taken by the offender's line manager. In some cases, the breach of security could also result in criminal proceedings.

5.2.2. All employees have a duty to report suspected security incidents and any other security concerns to their line managers or Information Security Co-ordinators, who in turn should notify the IT Help Desk who will then log the incident and inform the Information Security Officer. If there are reasons for not wishing to bring such incidents or concerns to management within their own Business Units, employees should contact Internal Audit who will deal with the matters reported in the strictest confidence.

5.3 Confidentiality of Information

All employees and contracted third parties working for the Council must observe the utmost care and attention in dealing with personal information - in no circumstances must **any** information about the Council or its customers be divulged to anyone outside the organisation, without proper authority from line management who must ensure that such disclosure would not contravene the Data Protection Act 1998.

5.4 System Ownership

For each information system, there shall be a named senior member of staff designated as System Owner - typically the manager or section head responsible for the principal service(s) for which the system operates. The System Owner is responsible for:-

- determining who can access the system and the scope of operation available to

each permitted user as appropriate to the particular classification of the information - see 5.6;

- ensuring that a risk assessment is carried out on a new or replacement system, prior to going live;

- ensuring that the system is maintained in an effective and controlled manner;

- ensuring that all changes to the software are performed to an agreed **change control mechanism;**

- ensuring that staff immediately report any violations or misuse of the system to their line manager;

- dealing with requests under the Data Protection Acts in a timely manner.

5.5 Legal Requirements

The Council and all its staff shall observe all external laws and regulations, which are relevant to Information Systems. These include:-

5.5.1. Data Protection Act 1998.

The Council shall comply with the requirements of the Data Protection Act 1998, and any replacement law and /or guidance from the Data Protection Commissioner. To do so, the Data Protection Officer, appointed by the senior management of the Council, will co-ordinate the registration/notification of personal data for all Business Units within the Council ensuring that the registration/notification details are up to date and reflect the way that the data is being used. It is also vital that the data held is properly recorded in such a way as to assist requests for information from members of the public. Each Business Unit will nominate a Data Protection Co-ordinator.

5.5.2. Copyright, Designs and Patents Act 1988.

The Council through the IT Business Unit will ensure that the software which is being used on its premises and by its employees is subject to an authorised and appropriate licence agreement. Any illegal copying of software or other infringement of the licence agreement will be dealt with in an appropriate way by senior management.

5.5.3. **Computer Misuse Act 1990.**

If it is suspected that any unauthorised access is made to a computer system, constituting infringement of the Computer Misuse Act, then the relevant Head of Business Unit shall report the incident to the IT Security Officer who shall advise on immediate action and arrange any subsequent investigations as appropriate. All staff should be made aware that under no circumstances must any computer misuse be reported to anybody outside the Council. Such matters are highly confidential. Disclosure could be embarrassing and possibly damaging to public confidence in the Council.

5.5.4. **Health & Safety at Work Act 1974**

The Council shall ensure, through the appointed Health & Safety Adviser that all IT equipment is located and used in such a way as to not impede the health and safety of the users or others. Each work station is to be installed in compliance with the Health and Safety (Display Screen Equipment) Regulations 1992.

5.6 Classification of Information

The information used and recorded by each system must be reviewed by the relevant System Owner and placed in one or more of the following classifications.

Class A - Commercially sensitive

Example:	Financial/performance data relating to contracts with customers, clients, suppliers, etc.
To be avoided:	Holding/processing on unprotected PCs, unprotected networks, Web Pages, Internal and External Electronic Mail, access by suppliers, access by persons other than designated staff

Class B - Personal data relating to customers, clients, suppliers

Example:	Details of Council Tax payers, Benefit claimants, service customers, creditors, etc
To be avoided:	Holding/processing on unprotected PCs, unprotected networks, Web Pages, External Electronic Mail, access by persons other than designated staff

Class C - Personal data relating to staff

Example:	Personnel/payroll data
To be avoided:	Access by other than designated staff.

5.7 Contingency Planning

It is the responsibility of each System Owner to ensure the availability of their system. A

formal decision shall be made for each system to decide on the need and format of a contingency plan in the event of various system breakdown scenarios. These scenarios might typically include failure for 2 hours, 1 day, 1 week, 1 month. Each system contingency shall form part of an overall Business Recovery Plan determined by Senior Management and co-ordinated by the Council Executive.

5.8 Implementation of new systems

All system implementations must be part of the overall IT Strategy for the Council. Security issues must be adequately considered. All major system implementations must be officially authorised by the IT Steering Group. Where end-user report generating applications which do not alter the data are being developed and used, this must be done in an appropriately secure way by the individual user, who in this context, will be regarded as the System Owner. Such operation must be authorised by the relevant line manager.

5.9 Software Packages

New applications which are purchased from a software house, must form part of the overall IT strategy for the Council and be authorised by the IT Steering Group. Packages must be evaluated on the basis of security as well as functionality and total costs. The IT Unit must always be consulted on proposed purchases.

5.10 Wide Area Network Security

It is the responsibility of the IT Business Unit to maintain the security of all Wide Area Network connections used to/from any computer/network within the Council. It is vital that the network connections do not compromise the security of the information being transmitted and the security of that information must be maintained in line with the requirements of the relevant System Owner.

5.11 Local Area Network Security

It is the responsibility of the IT Business Unit, in consultation with the relevant line managers/system owners, to maintain the security of all Local Area Networks used within the Council. It is vital that the network connections do not compromise the security of the information being transmitted and the security of that information must be maintained in line with the requirements of the relevant line manager, system owner.

5.12 Electronic Links to other parts of the organisation and to/from third parties

The IT Business Unit is responsible for ensuring the protection of all information being sent /received to/from other parts of the Council or to/from external organisations via Internet or direct modem access. In doing so it shall make no assumptions as to the quality of security used by any third party. A Connection Agreement must be completed between the relevant site/centre and the connecting organisation - this must be authorised by the Head of IT before the connection is utilised.

5.13 Use of Internet/Intranet

5.13.1 The Council's Intranet is maintained as a means of publishing information for the benefit of employees, Members and the public at large. Information of classification A or B must **never** be published on the Intranet. Additionally, no personal information must be published on the Intranet without the express consent of all persons concerned.

5.13.2. Access to the Internet is provided through the Council's central gateway and its associated security "Firewall". Access other than through the gateway will only be authorised where justified by special circumstances and in such a case must be authorised by both the prospective user's Head of Business Unit and the Head of IT. In such a case, a dedicated stand-alone PC with no network connections will normally be used.

5.13.3. Regardless of the method of access, information of classification A or B should never be sent or loaded onto the Internet. Any web site **must** only be set-up and managed by the IT Business Unit. Downloading of software from the Internet is strictly forbidden except as expressly authorised by the Head of IT.

5.14 Controlling Personal Computers, laptop computers, electronic organisers

Each Personal Computer (PC), laptop computer, electronic organiser shall have a designated Owner responsible for the overall security of that piece of hardware and associated peripherals. Each user has responsibility for the workstation they use and the

data held on it. These responsibilities cover:-

- Physical Security (securing where and when the machines are used);
- Logical Security (securing against viruses, unauthorised use of software);
- Confidentiality (of data within the system and resultant printouts).

It is the responsibility of Line Mangers to ensure that all PC users are trained and aware of recognised good practice and that all the hardware and software has been procured through, or in consultation with, the IT Business Unit.

5.15 Electronic Mail

Line Managers are responsible for ensuring that their staff take appropriate precautions whilst reading and sending electronic mail. Specifically information of classification A **should not** be sent via e-mail, either within the context of a free format message or as a file attachment.

5.16 Central Computer Suite

It is the responsibility of the IT Business Unit to ensure that adequate policies and procedures are in place and followed to cover the security of the central computer suite, specifically the hardware, software, information and staff involved at the centre.

5.17 Millennium compatibility

The Year 2000 Steering Group is responsible for ensuring that the issue of millennium compliance is being properly addressed within the Council. All contracts for new applications, computers and any equipment with microprocessors must contain appropriate provisions to ensure Year 2000 compliance. The Heads of Business Unit are responsible for ensuring that existing specialist computer systems not supported by the IT Unit are checked for compliance or replaced/upgraded as required.

5.18 Awareness

Line managers and Heads of Business Unit are responsible for ensuring that all staff and contracted third parties working for them are aware of and adhere to this Policy and its

associated guidelines.

5.19 Implementation

5.19.1 Implementation measures will include:-

(a) suitable training in which all employees and Members with access to Council IS/IT facilities will be required to participate;

(b) production and, where appropriate, publication of associated documentation.

5.19.2 This documentation will take the following form:-

(a) **Information Security Code of Practice**
This Code is intended to set out specific standards of acceptable practice in using Council IS/IT. The Code will be binding on **all** employees and Members as a condition of being given access to any Council information systems and breach of any part may lead to withdrawal of facilities or even disciplinary action.

(b) **Technical Policies**
Produced by the Head of IT, these are specific standards that IT Unit staff are required to comply with in setting security configurations on all Council IS/IT facilities.

(c) **Information Security Guidelines**
Produced by the Head of IT in conjunction with Internal Audit, these are informatory and advisory guides on legal matters and good practice to be read in conjunction with this Policy.

(d) **Specific Policies, Guidelines, Codes of Practice, etc.**
These are documents produced independently of this Policy which deal with specific information security related issues in greater depth.

5.19.3. A reference page will be maintained on the Intranet listing all the above documentation currently in force. With the exception of (b) above, the documentation itself will, together with this Policy, be also published on the Intranet and made accessible via the reference page.

6 INDEX TO INFORMATION SECURITY GUIDELINES AND CHECKLISTS

At the time of publication, the following linked guidelines and checklists have been produced in order to give more detail on specific security issues. The functions who would normally be responsible for ensuring adherence to them are indicated, together with a cross reference to the above Policy statement

Guideline:	Policy statement:		Function Responsible for implementation:
	5.1	Summary User Checklist	SO, LM
1	5.5.1.	Legal - Data Protection Act	LM, SO, DPC
2	5.5.2.	Legal - Copyright, Designs & Patents Act	LM, HOB,
3	5.5.3.	Legal - Computer Misuse Act	LM, SO
4	5.5.4.	Legal - Health & Safety at Work Act	LM, HOB
5	5.17	Millennium compatibility	SG
6	5.4	System ownership	SO
7	5.6	Classification of Information	SO
8	5.7	Contingency planning	SO, IT
9	5.8	Implementation of new systems	SO
10	5.8	Controls in applications	SO, IA
11	5.8	Control of UNIX based departmental systems	IT, ITSG
12	5.9	Software Package procurement	SO, IT
13	5.10	Control of LAN's	IT
14	5.11	Control of WAN's	IT
15	5.12	Control of dial-up links	SO, IT
16	5.13	Controlled use of Internet/Intranet	LM, ITLO
17	5.14	Controlling Personal Computers	LM, ITLO
18	5.15	Use of E-mail and Faxes	LM, ITLO
19	4	Working off Council Premises	LM
20	5.16	Computer Centres	IT
21	Various	Risk Assessment	SO, IT, IA
22	Various	Evaluation and use of security products	IT
23	Various	Use of Passwords	SO, LM

Key to functions identified:

SG - Year 2000 Steering Group
LM - Line Manager
HOB - Head of Business Unit
SO - System Owner
SA - Systems Administrator
IT - IT Business Unit

ITLO - IT Liaison Officers
IA - Internal Audit
DPC - Data Protection Co-ordinators
ITSG - IT Steering Group

Summary User Checklist

NEED FOR SECURITY

To protect information systems from the threat of:

theft - PC's, laptops and fax machines are particularly vulnerable.

human error - the phrase "Garbage In Garbage Out" illustrates the need for accuracy over input to ensure that the council maintains quality information.

equipment failure - computers, printers, fax machines can and do go wrong, for a multitude of reasons.

software failure - "bugs" in old (and new) systems can be a time consuming problem.

unauthorised access - to the equipment and to the information stored on the equipment, possibly even by someone "hacking" via an external network.

viruses - can spread from a single PC to a complete network quickly and with devastating effects.

disaster - takes many forms - the system being down for just an hour, or a month

SUMMARY OF POLICY

The Council has developed detailed policies on Information System Security. The broad objectives of the policies are to:

- instil in each member of staff a proper awareness and concern for information security and adequate appreciation of their responsibility for information security;
- provide a framework and management support for the establishment of standards, procedures and computer facilities to effect a high level of information security;
- specify broad organisational responsibilities
- specify the security organisation.

YOUR role in Information Systems Security

Fundamentals:

OWNERSHIP - each computer system, be it a stand-alone PC or a departmental system must have a designated SYSTEM OWNER - responsible for the security of information within that system.

RESPONSIBILITY - EVERYONE WITHIN THE COUNCIL is responsible for the PC, terminal, fax machine that they use and more importantly the information which they use on a day to day basis.

CLASSIFICATION - the amount and sophistication of security on a particular system should be relative to the sensitivity and criticality of the information being processed. To this end the Council has four levels of classification:

A - Commercially sensitive
B - Personal data relating to customers
C - Personal data relating to staff
D - Unclassified.

System Owners must ensure that the appropriate classification and hence security is applied to THEIR systems.

WHAT EVERYONE SHOULD DO:

DO ensure passwords are kept private and changed at appropriate intervals.

DO ensure regular backups are taken to cover at least the last month and do check how to recover from a backup tape *- just in case the worst happens!*

DO lock away discs, tapes, printouts when you are not using them.

DO be careful about what you send via e-mail, and who you send and copy it to.

DO lock your PC to the desk if it is in public view or in a vulnerable position (perhaps even move it to a safer spot - if that is practical).

DO ensure that any incoming diskettes, CD-ROMs, etc are checked for viruses by your IT Liaison Officer before loading them to any Council PC.

DO refer to the IT Help Desk before you buy any software - they may have a site licence for it already

DO check the results from your system occasionally - computers can produce inaccurate information no matter how impressively it is presented!

DO check before you send a fax containing sensitive information

DO dispose of waste computer output with regard to confidentiality, sensitivity and personal data content
- user shredders where appropriate;
- avail your self of arrangements for disposing of bulky confidential waste.

DO secure work-related files held on computers at home to prevent access by any other persons in your household.

DO RING FOR HELP if you have a problem

WHAT YOU SHOULD NEVER DO:

DO NOT use an obvious password, or share it with a friend or colleague unless you have the permission of the 'system owner'.

DO NOT leave your workstation or PC signed on to privileged facilities (e.g. Internet, e-mail, business application systems) when it is not being used.

DO NOT install software on any Council PC unless authorised by the Head of IT.

DO NOT attempt to download software from the Internet - talk to IT about how you can "surf" the net, without putting the Council at risk.

DO NOT make copies of software other than for backup, and then only as directed by IT.

DO NOT take machines home without first obtaining permission from your Line Manager - ensure that any discs exchanged between home and work are checked for viruses before being used.

DO NOT use non-standard unsupported software:-
- from Universities
- from bulletin boards and especially from the INTERNET
- from the front cover of magazines
- from your friend next door.

It may be free, but the virus it may contain can costs thousands of pounds to trace and remove!

DO NOT leave portable computers where a thief might be tempted - like the back of your car.

DO NOT allow anyone in your household to operate any Council-owned portable computer equipment taken home from the workplace.

DO NOT P A N I C - if you think you have a problem, ring the IT Help Desk NOW!