REPORT OF CENTRAL SERVICES COMMITTEE

(Meetings held 1 August and 26 September 2000)

1. ELECTRONIC GOVERNANCE STRATEGY (REPORT A - 1 AUGUST 2000) (MINUTE NO. 19)

The Committee has considered and approved a detailed report on a strategy for Electronic Governance (E-Governance). Members received a presentation on how this strategy and the proposed ICT Strategy (see item 2 below) are interlinked and complemented each other. The E-Governance Strategy provides a strategic framework under which the Council should work in providing services in what is now the Information Age, while the ICT Strategy underpins the E-Governance Strategy. Capital provision of £870,000 has been made for the implementation of the E-Governance Strategy during the period 2000/01 - 2003/04.

The E-Governance Strategy deals principally with the electronic interface between the Council and its customers. The vision is -

"To modernise the Council's service provision by utilising fully information and communication technologies (ICT) to enable joined-up working with partners and internally to provide seamless services to customers when and where they are required to a consistently high standard".

The E-Governance Strategy will become an integral part of the Council's overall business objectives and will be one of the enabling frameworks to assist in the achievement of specific corporate aims and objectives, as well as the continuous improvement of the business as a whole. E-Governance will provide the opportunity to improve services, both corporately and at the service level.

The Strategy has the following objectives -

(a) To create synergy between projects and processes to continuously improve performance;

(b) To speed up processes and the ease with which customers can engage Council services;

(c) To raise the standard of service provision through a process of continuous improvement;

(d) To encourage more people of the New Forest and the wider community, including the business community, to interact more frequently with the Council;

(e) To improve the first line response to customers;

(e) Always to be open for business via the Council's website, to optimise customer choice;

(f) To recognise the importance of diversity in the ways which a customer wishes to contact the Council;

(g) To provide genuine flexibility in the way we work, for example, by homeworking and hot desking for relevant employees;

(h) To provide more information to customers and citizens and other stakeholders.

A list of the major building blocks to enable to the Council to achieve its strategy are set out in Appendix 1.

The E-Governance Strategy also sets out customer and citizen expectations, proposals for consultation and involvement of service providers and customers, anticipated service enhancements and recommendations for evaluating progress on the Strategy. It has been stressed to the Committee that, notwithstanding the drive to improve electronic contact with customers and to maximise the use of electronic service delivery, it is not intended to reduce access by customers to other forms of contact with the Council such as personal visits to an office, or written or telephone communications.

The Committee has asked for members to be provided with full costs and quantified benefits of the implementation of the strategy as these become available. The Committee has also authorised the Assistant Chief Executive, in consultation with the Chairman of the Central Services Committee or the appropriate Portfolio Holder, to reprofile the budget provision within the parameters of the overall total allocated for any one year to achieve project priorities.

An officer team made up of representatives from all Directorates/Departments will be responsible for co-ordinating and delivering the Electronic Governance initiative. A progress report will be made to members in the first quarter of 2001.

2. INFORMATION AND COMMUNICATIONS TECHNOLOGY STRATEGY (REPORT B - 1 AUGUST 2000) (MINUTE NO. 20)

The Council's Information Policy and Information Technology Strategy were adopted in 1994. The Committee has approved an update of these policies to reflect changes in the Council's operations and to exploit the opportunities of technology to improve the provision of services.

The Information and Communications Technology (ICT) Strategy supplements and complements the E-Governance Strategy dealt with in item 1 of this report, to improve customer services, increase organisational effectiveness and efficiency, and to achieve best value through the delivery of high quality, joined-up services. The use of ICT will be a key element in achieving the Council's vision of working together with partners to provide joined-up services to the people of the New Forest and visitors. Provision of £889,000 has been made for the implementation of the ICT work programme in the period 2000/01 - 2003/04 - this amount is in addition to the provision of £870,000 for the E-Governance Strategy. The ICT work programme covers the replacement and renewal of a number of operational systems, and the replacement and upgrade of a number of Personal Computers across all Directorates.

The Information Policy adopted by the Committee is attached at Appendix 2. It will be applied to the implementation of all new information systems, while existing systems will be reviewed to achieve compliance with the policy as appropriate.

With the ever-increasing reliance on ICT to support corporate and departmental objectives, a strategic framework is essential to ensure that -

(a) Investment is properly targeted;
(b) The benefits of ICT investment are identified and achieved;
(c) The roles and responsibilities of the Head of ICT are clearly defined;
(d) The roles and responsibilities of managers with regard to ICT investment are clarified;
(e) The ICT Strategy and Information Policy are regularly reviewed.

The roles of the Head of ICT, Managers in Directorates and Departments and the Finance Directorate with regard to ICT have been clearly defined.

3. INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECURITY (REPORT C - 1 AUGUST 2000 MINUTE NO. 21 and 26 SEPTEMBER 2000 MINUTE NO. 32)

The Council has an ICT Security Policy which the Committee recommends be revised to support the new ICT infrastructure and new methods of working. The recommended new Security Policy, together with supporting documents, are attached to this report as Appendices 3 - 8. The documents include amendments agreed by the Policy & Resources Committee to Appendices 3 and 7, to form part of the Council Constitution.

The recommended policy will apply to all users of information systems, including Councillors and employees accessing information systems from remote locations, for example from home.

RECOMMENDED:

That the ICT Security Policy and Standards, set out in Appendices 3 - 8 to this Report, be adopted.

4. HOMEWORKING - PILOT SCHEME (REPORT D - 1 AUGUST 2000) (MINUTE NO. 22)

The Committee has agreed to a six month trial homeworking scheme, commencing towards the end of this year. Environmental Health, Housing and Environment Services employees have expressed interest in participating in the pilot. A further assessment will be undertaken over the next few months to identify possible opportunities for homeworking within the Finance Directorate and Chief Executive's Department. Until risk assessments are carried out and suitability established, it is not possible to say exactly how many employees will be involved, but it is anticipated that up to 12 officers will take part. The choice of officers to participate in the pilot will be based on the criteria that they already spend a good deal of their working day away from their office bases and may more readily adapt to homeworking.

A draft policy has been developed and will be trialled as an integral part of the pilot study. The policy will be subject to review as a result of the experience of the pilot study.

A great deal of attention is being paid to health and safety issues at each individual employee's workplace at home. To ensure compliance with health and safety regulations, equipment and/or furniture required to enable the employee to work from home will be provided by the Council where necessary. The Employee Side has been and will continue to be fully involved in testing the draft policy against the needs and issues identified through the trial period. It is envisaged that following completion of the pilot scheme the Council and the Employee Side will be able to develop a comprehensive homeworking policy. This will include giving full consideration to homeworkers' colleagues who remain office-based, to ensure that they are not disadvantaged by the scheme and/or its implications on their own working practices.

5. ORGAN DONATIONS (REPORT G - 1 AUGUST 2000) (MINUTE NO. 25)

The Committee has agreed to make use of the electoral registration canvass process this year to deliver organ donor forms to all households in the District. The additional cost to the Council will be a maximum of £1,500. The Policy and Resources Committee has approved this additional expenditure.

Taunton Deane Borough Council undertook a similar exercise last year. If the same rate of return as Taunton Deane is achieved, the initiative in this District should result in approximately 20,000 donors being added to the organ donor register.

(cnreport)

APPENDIX 2

NEW FOREST DISTRICT COUNCIL – INFORMATION POLICY

1) Minimum common data standards will be implemented for all databases to enable the straightforward transfer of information between systems.

2) Detailed information should be held at business unit level and consolidated information at corporate level, with automatic transfer between levels.

3) A single integrated customer/supplier information database should be developed for each business unit bringing together separate stand alone databases to provide co-ordinated operational and management information.

4) Electronic communications methods such as the Internet, Intranets and Electronic Data Interchange (EDI) should be used to enhance reporting arrangements within the Council and with its partners.

5) Improved channels of information will be developed with other agencies such as neighbouring authorities, partners, charities and the voluntary sector.

6) A comprehensive information network (an expanded intranet to include information from partner organisations) combined with an integrated telephone network should be developed for the Council and its partners. The expanded intranet will enable an accurate and a consistent response to public enquiries, via an integrated council-wide telephone system, which enables call transfers and desk-to-desk dialling (possibly between the partners e.g. Hampshire County Council or the Citizen's Advice Bureau). These arrangements will reduce the need for the public to make several calls when tracking down the appropriate service provider. They will also provide the opportunity for partnerships to be realised by providing a single point of contact for the public by using existing facilities.

7) Information will be widely available to all sectors of the community. It will be provided in a clear and unambiguous format and via different channels (e.g. public access kiosks conforming to Disability Discrimination Act guidelines).

8) A common standard for word processing, spreadsheets, graphics and electronic mail should be maintained to facilitate the training and support of employees, the effective interchange of information and economies of scale.

9) Information distribution shall conform to the guidelines of the Data Protection Act and other relevant legislation. Information shall only be used for the purpose for which it was originally intended. Information systems will be recorded on the Data Protection Register.

10) Confidential information will be stored securely and not be made available to inappropriate persons. Information systems will be constructed in such a manner that it is not possible for unauthorised persons to access information contained therein.

11) These themes are intended to be an integral part of service planning and incorporated as key objectives within all ICT development initiatives.

APPENDIX 3

ICT SECURITY POLICY

It is the policy of New Forest District Council to ensure that:

1. Information will be protected against unauthorised access and the confidentiality of information will be assured.

2. The integrity of information will be maintained.

3. Regulatory and legislative requirements will be met.

4. All employee breaches of ICT security (actual or suspected) will be reported to and investigated by the Audit Manager.

5. Any action taken against individual employees will be in accordance with the Council's disciplinary procedure.

6. Member use of the Internet will be fully monitored.

7. E-Mail and files created or received by Members will not be routinely monitored. The appropriate Group Leader will be asked to give consent to monitoring only as part of an investigation relating to conduct or probity.

8. Any breach of the ICT Security Policy (actual or suspected) by Members will be reported to the Chief Executive who will carry out an internal investigation and report to the Council's Monitoring Team for consideration where the breach is in excess of a minor discretion.

9. The use of Electronic Mail will be monitored in accordance with the ICT Security Policy and Standards.

10. The use of the Internet will be monitored in accordance with the ICT Security Policy and Standards.

11. An ICT Disaster Recovery Plan will be maintained and tested.

Each of these elements is explained in detail in the following pages.

APPENDIX 4

ROLES AND RESPONSIBILITIES

1. Information will be protected against unauthorised access and the confidentiality of information will be assured.

Responsible Officer(s)	Responsibilities
OMT	To endorse and fully support the application of the policy across the authority.
Audit Manager	To provide clear standards against which access privileges are gauged.
ICT Security Officer	To implement the access standards across the ICT infrastructure. To liase with all systems administrators ensuring that all user details are maintained up-to-date. To check system audit logs of users access to systems.
Managers	To ensure that employees are aware of the policy and standards at induction time wherever possible. To monitor employees' use of systems. To take disciplinary action when required. To inform the ICT Helpdesk promptly about employees leaving, or access being terminated.
Employees	To comply with the Policy and Standards.

The information security standard relating is set out at Appendix 5.

ROLES AND RESPONSIBILITIES

2. The integrity of information will be maintained

Responsible Officer(s)	**Responsibilities**
OMT	To endorse and fully support the application of the policy across the authority.
Audit Manager	To ensure that employees understand the implications of maintaining the integrity of data.
ICT Security Officer	To maintain system audit logs of all data changes.
	To check that regular data and system back ups of corporate systems are carried out and completed.
	To ensure that data is recoverable from backup.
Managers	To ensure that employees comply with the legislation covering Data Protection and Computer Misuse.
Employees	To comply with the Policy and Standards

The information security standard relating is set out at Appendix 5.

ROLES AND RESPONSIBILITIES

3. Regulatory and Legislative Requirements will be met

Responsible Officer(s)	**Responsibilities**
OMT	To endorse and fully support the application of the policy across the authority.
Audit Manager	To ensure that all information systems holding data are (where applicable) registered with the Data Protection Registrar. To ensure that the Computer Misuse Act (1990) is complied with.
ICT Security Officer	To only install or upgrade data holding systems that comply with Data Protection legislation. To ensure ICT employees only install software for which a valid licence is held.
Managers	To ensure that employees comply with the legislation covering Data Protection and Computer Misuse. To ensure that only ICT employees install software for which a valid licence is held. To ensure that software is only installed by ICT employees.
Employees	To comply with the Policy and Standards. To ensure that any software to be installed is registered with the ICT help desk for installation by ICT employees.

The information security standard relating is set out at Appendix 5.

A synopsis of the Computer Misuse Act is attached Appendix 6.

ROLES AND RESPONSIBILITIES

4. All employee breaches of ICT security (actual or suspected) will be reported to and investigated by the Audit Manager.

Responsible Officer(s)	**Responsibilities**
OMT	To endorse and fully support the application of the policy across the Council.
Audit Manager	To ensure that employees are aware of relevant legislation, Council policies and guidelines.
ICT Security Officer	To provide information to the Audit Manager on any attempted or actual security breaches.
Managers	To ensure that employees comply with Policy and Standards.
	To monitor use and refer cases to Audit Manager.
	Take disciplinary action when required.
Employees	To comply with the Policy and Standards.

ROLES AND RESPONSIBILITIES

5. Any breach of the ICT Security Policy (actual or suspected) by Members will be reported to the Chief Executive who will carry out an internal investigation and report to the Council's Monitoring Team for consideration where the breach is in excess of a minor discretion.

Responsible Officer(s)	**Responsibilities**
OMT	To endorse and fully support the application of the policy across the Council
Audit Manager	To ensure that Members are aware of relevant legislation, Council policies and guidelines.
ICT Security Officer	To provide information to the Chief Executive on any attempted or actual security breaches.
Members	To ensure that Members comply with Policy and Standards.

The information security standard relating is set out at Appendix 5.

ROLES AND RESPONSIBILITIES

6. The use of Electronic Mail will be monitored in accordance with the ICT Security Policy and Standards.

Responsible Officer(s)	**Responsibilities**
OMT	To endorse and fully support the application of the policy across the authority.
Audit Manager	To ensure employees are aware of relevant legislation. To ensure that all suspected breaches are investigated.
Head of ICT	To assess the severity of the breach of policy.
ICT Security Officer	To check all monitoring reports for breaches in policy. To inform the Audit Manager of any suspected breaches of the Electronic Mail policy and to provide any relevant information to the Audit Manager on any suspected breach in security.
Managers	To ensure that employees comply with the Policy and Standards. To ensure that employees have the relevant training. To take disciplinary action when appropriate.
Employees	To comply with the Policy and Standards.

The information security standard relating is set out at Appendix 5.

ROLES AND RESPONSIBILITIES

7. The use of the Internet will be monitored in accordance with the ICT Security Policy and Standards.

Responsible Officer(s)	**Responsibilities**
OMT	To endorse and fully support the application of the policy across the authority.
Audit Manager	To ensure employees are aware of relevant policy and standards. To ensure that all suspected breaches in security are investigated.
Head of ICT	To assess the severity of the breach of policy.
ICT Security Officer	To check all monitoring reports for suspected breaches in policy. To inform the Audit Manager of any breaches of the Internet Electronic Mail policy and to provide information to the Audit Manager on any suspected breaches in security.
Managers	To ensure that employees comply with Policy and Standards. To ensure that employees have the relevant training. To take disciplinary action when appropriate.
Employees	To comply with the Policy and Standards.

The information security standard relating is set out at Appendix 5.

ROLES AND RESPONSIBILITIES

8. An ICT Disaster Recovery Plan Will Be Maintained And Tested.

Responsible Officer(s)	**Responsibilities**
OMT	To endorse and fully support the application of the policy across the authority. To ensure that the Disaster Recovery Plan protects and support operations at New Forest District Council.
Audit Manager	To ensure that ICT maintains a Disaster Recovery Plan. All individual Business Continuity plans to be integrated to form a cohesive overall plan for New Forest District Council.
ICT Security Officer	Co-ordinating the ICT Disaster Recovery Plan in relation to technology based services across all New Forest District Council sites.
Managers	Create relevant business continuity plans prioritised across the business unit.
Employees	Be aware of Business Unit plan and their role in its implementation should this be required.

The information security standard relating is set out at Appendix 5.

APPENDIX 5

ICT SECURITY STANDARDS

Information and Communications Technology Security is the responsibility of all users of ICT.

The following standards should be used as a reference point in the day-to-day use of the Council's ICT systems.

1. INFORMATION WILL BE PROTECTED AGAINST UNAUTHORISED ACCESS AND THE CONFIDENTIALITY OF INFORMATION WILL BE ASSURED.

1.1 Access to Information Systems is controlled by the use of secure passwords. Passwords are a means of preventing access to systems or parts of systems by unauthorised users. The more systems that users have access to the more passwords are normally required.

1.2 Passwords are strings of characters, numerals or combinations that are used to authenticate the user of a system. To be of value passwords need to be greater than 5 characters in total, not repeating characters, or sequential e.g. password1, password2, or abcdefg 123456778, qwertyu. Users should not use a name or any string that can be identified with the user easily, (NOT surname, other family name, car registration, telephone number, etc.)

1.3 Remember the User ID identifies users on system audit trails.

1.4 All ICT users must be set up with an individual login and password where appropriate. The password is not to be divulged to anyone else either internally or external. Users may be requested to provide their password to ICT for maintenance, when the work is complete the user should ask for it to be changed and select a new one.

1.5 When users leave their computer for any length of time they should ensure that access is prohibited, by any of the following:

- Logging out.
- Using a screen saver with a password.
- If you have an NT PC then use the "lock workstation" option.

1.6 If users need help with setting up any of the above then call the ICT Helpdesk.

Employees Joining and Leaving the Council

1.7 ICT have a standard form that the manager responsible must complete for new employees and leavers (or temporary employees needing access to our information systems). Where possible these forms should be completed and returned to ICT at least one week before the start or termination date.

1.8 Before requesting access to information systems, managers (or the officer responsible), must check that the user is aware of the Policy and Standards.

ICT SECURITY STANDARDS

2. THE INTEGRITY OF INFORMATION WILL BE MAINTAINED.

2.1 ICT users must save all work on the appropriate network Server. An area will be set up for their use (in most cases a group area, is set up for each department or section).

2.2 The Servers run an incremental backup on weekdays and a full backup at weekends. An Incremental backup will only backup data that is new or has changed since the full backup at the weekend. A full backup is everything old, new, changed and system.

2.3 Users must ensure that they check that their data is still required on a regular basis. If it is no longer required they should delete or archive it (or arrange to have it done.

2.4 Managers responsible for other persons given access to Council equipment and/or networks whilst engaged on Council business must make sure that when the "employee" leaves (or when access is terminated) that the data held in that users own area is deleted. A call should be placed with the ICT help desk to move the data to a different area if necessary. This will ensure that disk space on the server is not wasted.

2.5 When travelling with laptop/notebook computers, users must ensure that they are put out of sight.

2.6 Users must not leave the laptop/notebook computers unattended.

2.7 The laptop/notebook must be put out of sight when not in use.

2.8 Any sensitive or confidential information must be password protected.

2.9 When users leave the laptop for any length of time they must ensure that the access is prohibited, by any of the following means:

- Logging out.
- Activating an approved screen saver with a password.
- If you have an NT machine use the "lock workstation" option.

Server Hardware Failure/Loss of Connection to the Server

2.10 On older workstations, (e.g. Windows 3.1) a hardware failure or loss of connection to the Server normally means that users could experience a loss of data. Users are advised that users set applications to save frequently.

ICT SECURITY STANDARDS

2.11 NT workstations are more stable but users are advised to set applications to save frequently. These workstations will be able to continue to operate without the server. Users can work as normal but save the work/data to c:\ until the server is fully functional then move the work/data to the relevant area on the server.

2.12 Personal material (e.g. personal letters, CV's etc.) must not be stored on the Councils Information Systems Network.

2.13 Only the work/data on the server will be backed up automatically. Laptop/ notebook users must remember this. If they are not able to gain access to a server then other backup precautions should be put in place i.e. save a copy to A:\ (floppy disk).

2.14 Users must be aware that some of their work will have data in it that will be protected by the Data Protection Act and they should be aware of the responsibilities that this brings.

3. REGULATORY AND LEGISLATIVE REQUIREMENTS WILL BE MET.

3.1 Details of the Data Protection Act and the Computer Misuse Act are set out in full in Appendix D.

3.2 Users must not give sensitive or confidential data to unauthorised colleagues or members of the public: If in doubt contact the Data Protection Officer, Geoff Bettle on (023) 8028 5820.

3.3 Users must not locate visual display units in such a position that screen displays are visible to unauthorised users or members of the public.

4. ALL EMPLOYEE BREACHES OF ICT SECURITY (ACTUAL OR SUSPECTED) WILL BE REPORTED TO AND INVESTIGATED BY THE AUDIT MANAGER.

5. ANY BREACH OF THE ICT SECURITY POLICY (ACTUAL OR SUSPECTED) BY MEMBERS WILL BE REPORTED TO THE CHIEF EXECUTIVE WHO WILL CARRY OUT AN INTERNAL INVESTIGATION AND REPORT TO THE COUNCIL'S MONITORING TEAM FOR CONSIDERATION WHERE THE BREACH IS IN EXCESS OF A MINOR DISCRETION.

5.1 The Public Interest Disclosure Act 1998 has made it possible for an employee who encounters a malpractice, which could threaten the public interest, to raise his concerns without fear of reprisal, instead of turning a blind eye.

5.2 Users are asked to refer to the Fraud, Corruption and Probity leaflet. Copies are available from Administrative Officers, on the Intranet and in the Employee Handbook.

5.3 Any employee who suspects a breach of the Security Policy must inform the ICT Security Officer promptly.

5.4 Once an initial assessment has been made, the ICT Security Officer, together with the Audit Manager will assess the severity of the situation and determine the action to be taken.

6. THE USE OF ELECTRONIC MAIL WILL BE MONITORED IN ACCORDANCE WITH THE ICT SECURITY POLICY AND STANDARDS

6.1 See Appendix E.

7. THE USE OF THE INTERNET WILL BE MONITORED IN ACCORDANCE WITH THE ICT SECURITY POLICY AND STANDARDS.

7.1 See Appendix E

8. AN ICT DISASTER RECOVERY PLAN WILL BE MAINTAINED AND TESTED.

8.1 An ICT Disaster Recovery Plan will be maintained and tested in consultation with business units and departments.

APPENDIX 6

SYNOPSIS OF THE COMPUTER MISUSE ACT

Set out below is a working synopsis of the appropriate section of the Computer Misuse Act:

The Unauthorised Access Offence

1. A person is guilty of an offence if he causes a computer to perform any function with intent to secure access to any program or data held in any computer.

2. A person is guilty of an offence if the access he intends to secure, is unauthorised; and he knows at the time that he attempts such access that that is the case. Therefore, to prove the offence it will be necessary to show:

   a) That the access was deliberate.

   b) That it was unauthorised.

   c) That the person knew it was unauthorised.

3. The intent that a person has to have to commit an offence under this section need not be directed at:

   a) Any particular program or data.

   b) A program or data of any particular kind.

   c) A program or data held in any particular computer.

4. Unauthorised access will cover those seeking access from outside who will, in the most cases, be unable to demonstrate any consent, and authorised users that deliberately exceed their authority.

5. An offender who successfully obtains access and makes the computer display data or listings of a program will plainly be in contravention of the Act. Others who are less successful may also commit the offence. For example, if the offender was trying out guessed passwords, he would be guilty the moment any computer responded with a message stating that the password used was invalid. He would be guilty even before that time, if, as a result of his action, the computer invited him to provide a password, as that invitation would constitute a computer function carried out as a result of the offender's actions.

SYNOPSIS OF THE COMPUTER MISUSE ACT

6. A hacker who, with intent to secure unauthorised access, goes into the telephone network to find out if any computers will respond will be guilty the moment one of them does. It is immaterial whether it was the one which he expected to respond or if he has any idea which computer it is.

7. An authorised user who deliberately exceeds his carefully prescribed authority in order to look at data or software from which he was normally excluded would be as guilty of this offence as a hacker from outside the organisation.

8. However, the offence is deliberately phrased to exclude anybody genuinely blundering into a system or network without authority. The offender must have the intention of accessing and know that he has no authority to do so.

APPENDIX 7

SECURITY POLICY ON THE INTERNET, INTRANET AND ELECTRONIC MAIL

1. INTRODUCTION

1.1 New Forest District Council's use of the Internet, Intranet and Internet Electronic Mail is set to expand rapidly. These technologies will become an important tool for managing and delivering services and speeding up communications.

1.2 This security policy ensures that users receive maximum benefit from the technology, whilst maintaining the security and integrity of the Council Information Systems.

2. POLICY OVERVIEW

2.1 The use of Internet, Intranet and E-mail will increasingly benefit the Council and its employees.

2.2 These facilities must be used responsibly and legally. Users must not misuse them by taking any action which could bring the Council into disrepute, cause offence, interfere with the work of the Council or jeopardise the security of data, networks, equipment or software.

2.3 The facilities should be used primarily for Council business. However, the Council wishes to encourage users to explore the Internet in a constructive manner. Consequently, occasional personal use (e.g. college work) may be permitted with express permission of Senior Managers, provided it does not interfere with the work of the Council, conforms to this policy and is not associated with personal business interests.

2.4 The guiding principle is that, despite its immediacy and ease of distribution, electronic communication and information should be treated no differently from that on paper.

2.5 ICT Services and Internal Audit will carefully and frequently monitor the use made of the Internet by all users (including Members). They may also inspect the contents of e-mail and files for employees and visitors although no Member e-mail or files will be monitored without the prior consent of the appropriate Group Leader. The appropriate Group Leader will only be asked to approve monitoring of Member e mail and files as part of an investigation relating to conduct or probity. All users (including Members) should not expect any Internet related activities to be considered private.

2.6 Adherence to this policy is a condition for using Council equipment and networks.

2.7 Failure to adhere to this policy is a serious disciplinary offence which could lead to dismissal and criminal or civil action if illegal material is involved or if legislation, such as the Data Protection Act, is contravened.

3. APPLICABILITY OF THIS POLICY

3.1 This policy applies to:

a) All Council employees and Members using Council equipment from whatever location, including home.

b) Any other use by Council employees or Members which identifies the user as a Councillor or Council employee or which could bring the Council into disrepute.

c) Other persons working for the Council, whilst engaged on Council business or using Council equipment and/or networks.

4 APPROPRIATE USE AND MISUSE OF THE INTERNET

4.1 Misuse includes using electronic media for:

a) Creation, use, transmission or encouragement of material which is illegal, obscene or libellous, is offensive or annoying, defamatory or infringes another person's copyright.

b) Transmission of unsolicited advertising or commercial material.

c) Obtaining unauthorised access to Council's or another organisation's ICT facilities.

d) Violating other people's privacy.

e) Using chat lines or similar services.

f) Playing games.

g) Illegal activities including breaching the Data Protection Act, Computer Misuse and Design Copyright and Patents Acts.

h) Wasting network and other resources

i) Disrupting the work of others in any way by introducing viruses or by corrupting data.

j) Expressing personal views which could be misinterpreted as those of the Council.

k) Committing the Council to purchasing or acquiring goods or services without proper authorisation or following appropriate financial regulations.

l) Downloading copyrighted or confidential information.

m) Failing to adhere to this policy.

4.2 This is not an exhaustive list but is an indication of the types of conduct that may result in disciplinary action and possibly dismissal.

4.3 A good test is whether, with hindsight, you could justify your actions to your manager or a member of the public (Code of Conduct). Further guidance and clarification is given below.

5 OFFENSIVE AND ILLEGAL MATERIAL

5.1 Offensive material is anything that is pornographic; involves threats or violence; promotes illegal acts, racial or religious hatred or discrimination of any kind. It also covers material, which the person knows, or could have reasonably expected to know would have offended a colleague with particular sensitivities, even if it is not explicitly offensive, e.g. religious views.

5.2 The Internet contains huge volumes of useful information. It also contains some offensive material. Any employee using Council facilities for viewing or downloading such material will face serious disciplinary action. If illegal material is accessed the Council will inform the police and criminal prosecution may follow.

5.3 Newsgroup messages often link to web pages and users should be aware of the risk of inadvertently accessing inappropriate sites. Any employee accidentally accessing offensive material should inform their manager and ICT Services immediately. Accidental access will not result in disciplinary actions, but failure to report it may do so.

5.4 People who receive offensive or sexually explicit mail should inform their manager and Internal Audit immediately. Such material may not be identifiable until an Email is opened and in these circumstances employees will not be held responsible provided they report it immediately to the ICT Services Manager.

6 PRIVATE USE OF FACILITIES

6.1 The Council wishes to encourage the effective use of the Internet and E-mail facilities. Employees and Members may use their Internet connections for occasional private purposes at the discretion of their Director or Head of Service, provided:

a) It does not interfere with Council work.

b) It is not related to a personal business interest.

c) It is not used for commercial purposes including the sale or purchase of goods and services.

d) It does not involve the use of newsgroups, chat lines or similar services.

e) It complies with this policy, including its provision regarding misuse.

6.2 Managers are responsible for monitoring time spent on personal use. Employees spending what their Director or Head of Service considers excessive time on personal use, may have their connection withdrawn and could face disciplinary action.

6.3 Employees wishing to spend significant time outside working hours using the Internet (eg for study purposes) should obtain approval from the Director or Head of Service.

6.4 Employees are encouraged to use the computer facilities in the communal recreation areas for personal research.

7 E-MAIL

7.1 E-mail whether by internal or the Internet should be regarded as public and permanent. It is never completely confidential or secure, and despite its apparent temporary nature, it can be stored, re-sent and distributed to large numbers of people.

7.2 E-mail must not be used for sending offensive, threatening, defamatory or illegal material. Sending an E-mail is the same as sending a letter or publishing a document in law, so defamatory comments could result in legal action. Internal E-mail has been used successfully as evidence in libel cases.

7.3 Users should be particularly careful about what they commit to E-mail. It can be used as evidence in internal disciplinary and grievance hearings as well as more formal or external settings.

7.4 It is unacceptable to use E-mail to criticise or rebuke employees. These matters should always be discussed face-to-face, in a supportive manner.

7.5 E-mail must not be used to harass recipients. Harassment can take the form of argumentative or insulting messages or any other message the sender knows or ought to know would cause distress to the recipient (the reasonable person test).

7.6 Employees or Members posting information to newsgroups which should not include any information that brings the Council into disrepute or expresses a political opinion.

7.7 It is easy to be misunderstood when writing E-mail messages. People often treat E-mail like phone calls but forget that the emotional meaning is often lost in text. Humour can be misinterpreted. E-mail should be unambiguous and authors should carefully consider the context of whether this is the best tool for conveying the message.

7.8 Bulk E-mail addressed to all users is a useful way of conveying a direct message. However, it can alienate and offend users if they are subjected to frequent irrelevant mail. Senders should carefully select the addresses they wish to send their mail to. As it develops the Intranet will be used to display certain information instead of sending to all on E-mail.

7.9 Employees or Members should not re-send E-mail chain letters and should exercise caution with any E-mail that asks the reader to forward it to others. If in doubt seek your manager's advice or contact ICT Services or Internal Audit.

7.10 Junk mail (spam) often referred to us is a hazard of Internet life. Employees and Members signing up to newsgroups should be aware that "spammers" get their mailing lists from newsgroups subscribers.

8 MONITORING USAGE

8.1 The ICT Security Officer will monitor the use of the Internet, contents of mail and file transfers that use the Council's equipment or networks, irrespective of whether the use is for Council or private use.

8.2 Monitoring reports will be made available to Directors, Heads of Service and Managers who are responsible for taking appropriate action where actual or potential misuse has occurred. Where necessary Internal Audit will advise Managers on the suitability of material, investigate sites or seek the opinion of the police.

8.3 The ICT Security officer should consult with the Head of ICT on matters concerning potential misuse and refer to the Audit Manager as appropriate.

8.4 Member use of the Internet will be fully monitored.

8.5 E-mail and files created or received by Members will not be routinely monitored. The appropriate Group Leader will be asked to give consent to monitoring only as part of an investigation relating to conduct or probity.

9. INTERNET CONNECTIONS

9.1 All connections to the Internet will be arranged by ICT Services.

9.2 To safeguard the Council networks, Internet usage will be closely monitored by ICT Services and Internal Audit.

9.3 Connection to the Internet will be channelled via management software. This software will provide an account of all incoming and outgoing network connections. The network administrator will be able to determine Internet usage, including details of which sites have been accessed, services used and time spent at each site by individual users.

9.4 All Internet access will be through a firewall which is a software and hardware product to protect the Council's networks from viruses and unauthorised entry.

10 ACCESS SOFTWARE (BROWSERS)

10.1 Internet capability will be installed on each networked PC within the Council. **Directors and Heads of Service (Authorised Requesters) will be responsible for authorising access. Access will not be provided without this authorisation.**

10.2 Access will be restricted to specified times of the day and specific user groups as determined by Authorised Requesters. Access to certain sites will be blocked via the network management software, if they are deemed to be unsuitable for Council usage.

10.3 Employees may only join newsgroups with the explicit approval of their Authorised Requester and where they relate to areas of the Council or professional interest. Managers should keep records of employees subscribing to such groups.

10.4 Access to chat lines, chat rooms and other similar services will not be permitted.

10.5 Users are not permitted to use their browsers for connecting to internet e-mail sites and to only use the E-Mail systems provided by the council.

11 VIRUS PROTECTION

11.1 Viruses can seriously disrupt operations. Anti-virus software has been installed on the network but due diligence will still need to be exercised.

11.2 Viruses can be transferred by files and E-mail attachments, thus threatening the security of the Council's networks. Consequently files must not be sent via Email unless they have been checked by ICT Services for viruses.

11.3 Files downloaded from the internet must be virus checked.

12 QUALITY OF INFORMATION ON THE INTERNET

12.1 Users should be aware that, as with paper sources, not all information on the Internet is accurate, complete or reliable. Users should evaluate its validity, as they would printed publications, before using it.

13. CONFORMANCE TO LEGISLATION

13.1 All users of the Internet and E-mail are subject to the relevant legislation. This includes the Data Protection, Computer Misuse and Designs, Copyright and Patents Acts.

13.2 The use of personal data in newsgroups or web sites is subject to the Data Protection Act. A synopsis of the relevant section on the Data Protection Act is attached at Appendix F.

13.3 Using the Internet to attempt to access any Council or third party IT facility without authority is an offence under the Computer Misuse Act.

13.4 Using the Internet to download or otherwise copy copyrighted software, information or other material without adhering to its licensing conditions is an offence under the Designs, Copyright and Patents Act.

14 PUBLICATION ON THE INTERNET AND INTRANET

14.1 The Council's web site and internal Intranet site are important parts of communication strategy. Managers should encourage employees to contribute material to both and to seek ways of using them to improve services and consultation.

14.2 The Council's policy is to operate a single public web site. If there are exceptional circumstances which warrant an additional web site, this may be achievable in consultation with ICT Services. Any such site must be approved by OMT and follow standards set by ICT Services.

14.3 Any publication of unsuitable material on either the Council's web site or Intranet will be regarded as misconduct.

14.4 Each item of information provided for publication must include the author's name and date.

14.5 Data Owners should ensure that there are named employees responsible for ensuring that information provided is accurate, up-to-date and conforms to the Council's corporate design standards.

15 PASSWORDS

15.1 All users will be issued a unique password. **Individual passwords must not under any circumstances be made known to other employees except where there is a Secretary/Manager relationship requiring joint use.**

15.2 Users will have a network password plus additional passwords for each system to which they have access.

15.3 System passwords are issued by ICT Services. Should a user forget their password or believe that another user knows their password, they should contact the ICT Help Desk immediately.

15.4 If access to a user's mail data is required while the user is not present to be able to enter their password, that user's departmental manager must authorise the ICT Help Desk to reset the password.

15.5 When passwords are reset by ICT Services, the existing password will be replaced by a temporary password. The user will be prompted by the system to enter a new password. This means that ICT Services employees have no knowledge of user passwords.

15.6 Users will need to change their password regularly when prompted by the system. A new password should be selected. A password which has been used previously or is similar to the previous password will not be accepted (eg if the original password was Roman, it could not be replaced by Roman1).

15.7 When an employee leaves the Council, their departmental manager must inform the ICT Help Desk immediately. The user's E-mail account and any other system access rights will then be frozen.

15.8 It should be noted that if a breach of security occurs because a user has made their password known to another then **both** users will have been deemed to have breached security.

16. TRAINING

16.1 All users will be trained to use E-mail, the Internet and the Intranet correctly and will be made aware of security issues.

16.2 New employees will be made aware of ICT security policies as part of their induction package.

16.3 For more information on training please contact ICT Services, Personnel Services or your Training Co-ordinator.

17. CHANGES IN TECHNOLOGY

17.1 The nature of Information Technology is such that there are continual changes in both hardware and software functionality. Users must however, continue to adhere to security measures as detailed in this policy irrespective of advancements in technology specifications.

17.2 Where developing technology necessitates changes in security measures, these measures will be reviewed by ICT Services and notified to employees.

17.3 ICT Services will issue instructions for any change in security arrangements to all users using a variety of relevant communication channels.

18. CONSULTATIONS

18.1 Police and Social Services will be consulted on reviews of this policy especially with regard to pornography or other offensive materials.

19. GUIDANCE

19.1 Should you require any help or guidance with any matter concerning ICT security, please phone the ICT Help Desk on (023) 8028 5797.

APPENDIX 8

DATA PROTECTION IMPLICATIONS FOR THE USE OF E-MAIL

1.1 The Data Protection Act is complex and sets out the framework within which organisations should operate. The following points are relevant in respect of E-mail.

1.2 The Council is required under the Data Protection Act 1998 to notify the Data Protection Commissioner of all personal data held in electronic (and in some instances) manual form. This notification includes the purpose for which the data is held, a description of the data, where it was obtained from and to whom the data is to be disclosed.

1.3 A criminal offence is committed if an organisation holds and uses unregistered personal data or fails to notify the Commissioner of any changes to existing register entries.

1.4 The use of E-mail offers users the opportunity to send personal data electronically from existing Council systems to individuals outside the organisation. Likewise it also provides the facility to import personal data from sources outside of the organisation.

1.5 In both cases it is important that users consider the appropriateness of any exchange of data. In the case of giving data out, users must ensure that any disclosure is consistent with the registration for that system. When personal data is received from an external source and held for use internally the recipient must check to ensure that an appropriate registration exists to permit the use of the data.

1.6 The seventh principle of the Data Protection Act states that “appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction”. Security of data is clearly therefore essential. Users should be aware that E-mail is neither completely confidential nor totally secure. If users decide to transmit personal data via E-mail regard must be taken as to the appropriateness of the method of transmission.

1.7 The issues identified in respect of external transmission of personal data similarly apply to the transmission of personal data within NFDC as an organisation.

1.8 Sharing of data with other business units for anything other than the purpose for which it was originally supplied is not permitted. The security and confidentiality of E-mail is not guaranteed. Users must carefully consider the appropriateness of E-mail before transmission.

1.9 Users must take care when committing anything to Email to ensure that the Council’s position is safeguarded. If there is any doubt as to the appropriateness of use, officers must consult with the Council’s Data Protection Officer before proceeding.