B

CABINET – 2 JUNE 2004 **PORTFOLIO FINANCE & SUPPORT**

EXECUTIVE SUMMARY – ICT Security Policy for Employees

Summary of Purpose and Recommendations:

Cabinet to approve revised ICT Security Policy for Employees.

Cost to Council: £TBA **Within existing budget?** TBA

Contribution to Corporate Plan (Minor/Moderate/Major/Neutral):

	+	⚖	-
★	Moderate		
👥		Neutral	
💱	Minor		
♥		Neutral	
🍃		Neutral	

	+	⚖	-
Priorities			
Clean Streets and Public Space		Neutral	
Crime and Disorder	Moderate		
Housing		Neutral	
Managing our Finances	Moderate		

Comments on Impacts on Corporate Objectives and Priorities:

The revised Security Policy accords with BS7799 national security standards and in that respect meets the standards expected of an organisation of excellence.

The policy seeks to minimise computer fraud and ensure that the Councils ICT infrastructure and financial and management systems remain secure.

★ Organisation of excellence

👥 Working with public and partners

💱 Economic well being

♥ Social well being

🍃 Environmental well being

CABINET – 2 JUNE 2004

INFORMATION & COMMUNICATIONS TECHNOLOGY SECURITY POLICY FOR EMPLOYEES (REVISION MAY 2004)

1. INTRODUCTION

1.1 A special Central Services Committee approved the Council's Information & Communications Technology (ICT) Security Policy on the 1st August 2000. This policy was modelled on BS7799 national security standard templates.

1.2 An independent consultant review of this policy was commissioned in November 2002. The consultant's draft report was received in February 2003 wherein it recommended that improvements be made to the style and format of the existing policy on the basis that it was "…confusing in structure", notwithstanding that it followed BS7799 standard templates.

1.3 Results of a number of investigations concerning internal ICT Security breaches confirmed this fact given that many employees found the existing policy complex, repetitive and difficult to interpret

1.4 A revised ICT Security Policy, as shown at *Appendix 1,* has been developed
# to rectify these apparent weaknesses. Members are asked to approve this revised policy.

2. BACKGROUND

2.1 The aforementioned report from the consultants, LDA plc of Newbury, confirmed that the Council's existing ICT Security policy was good but as stated, had a confusing structure. LDA recommended that the Council consider utilising the Office of the e-Envoy's BS7799 compliant template.

2.2 Further internal review of existing policy and the recommended e_Envoy model identified the need to develop a more focussed and user friendly policy in-house.

2.3 To this end the Council's ICT Security Policy has been revised to meet good practice but more particularly to meet specific internal needs.

3. POLICY ISSUES

3.1 LDA plc further confirmed that not only did the policy conform to good practice it also provided good guidance on legislative matters such as Data Protection and Computer Misuse but did not address e-Government objectives and the development of a fully transactional web-site. The revised policy concerns ICT security matters relevant to employees only and whilst it maintains good guidance on legislative and other matters it has been determined that is not the vehicle to regulate e-Government initiatives. These external security matters e.g. receiving payments via the Internet, are being addressed as part of this Council's e-Governance strategy and will be subject to separate policy statements as appropriate.

3.2 The existing ICT Security Policy defines protocols and procedures for both Employees and Members. Following a review of Members ICT conducted by Councillors Di Brooks and Maureen Robinson in March 2003 significant operational changes were made to the Members ICT infrastructure. Due to these changes a separate security policy was drafted in August 2003, specifically for Members. This policy will be subject to further review in the context of the changes made to employee policy and will be submitted to Cabinet in due course.

3.3 Notwithstanding the soundness of existing policy, this Council is not immune from internal computer abuse. The conclusion drawn from a number of investigations is that some employees, although trained, do not fully comprehend the requirements of existing policy. This revised policy, together with further targeted training and other planned initiatives should clarify the position with regard to misuse of the Council's systems.

4. CORPORATE MANAGEMENT TEAM (CMT)

4.1 CMT recognised the need to safeguard the Council's assets, maintain the integrity of information and ensure compliance with legislation and in that respect supports the revised ICT Security Policy.

4.2 CMT did however identify the need to enable employees to utilise ICT without compromising the Council's security protocols. To this end CMT proposed that officers research the possibility of upgrading the present "Internet Café" arrangements to provide a stand-alone facility (i.e. with an alternative Internet Service Provider outside of the Council's current Wide Area Network) to facilitate some relaxation of the present private use rules.

4.3 This arrangement would provide scope for employees (in their own time) to make personal payment transactions on line, manage their personal e-mail accounts, print off data of personal interest to them, book holidays and play interactive games subject to availability of resources. The overarching requirement not to browse sites that may offend others would be retained.

5. FINANCIAL IMPLICATIONS

5.1 There may be some costs associated with the development and upgrade of the present Internet Café arrangements (refer to 4.2 above). If such costs, once identified, cannot be contained within existing budgets a separate bid for funding will be made.

5.2 There is also a renewed requirement to further train all employees with Internet and/or external e-mail privileges. The costs associated with this training can be contained within existing budgets.

6. ENVIRONMENTAL AND CRIME AND DISORDER IMPLICATIONS

6.1 There are no environmental or crime and disorder implications.

7. EMPLOYEE SIDE COMMENTS

7.1 The Security Policy has been a concern to Employee Side when in the last year the number of employees that were investigated was significantly higher than previously. This could be down to many more employees having Internet access from home on their personal PC's where controls, if any, are likely to be more relaxed.

7.2 This problem is not localised, other Council's do let employees have more access for not only work but personal use re: job vacancies, train times, union web-sites, banking etc.

7.3 Whilst appreciating that there has to be some guidelines on what can and cannot be done on the Internet, Employee Side have expressed that to most employees the Security Policy was lengthy and confusing and therefore unclear in some respects. The policy content has not changed from the previous one but would be less confusing for the average user.

7.4 The intention of the revised policy has been to make it more understandable by employees, giving clear guidelines in non-technical terms. Other means still under investigation are short guidelines (maybe one page) and pop up warnings when accessing the Internet.

7.5 Training on-line did raise an issue. Understanding of the security protocols and standards of ICT use has dropped below average. Further investigation into training methods is ongoing by the Employer.

7.6 The Council must consider the addictive nature of the Internet and may have to publicise this side of access; therefore guidelines and booklets are needed to advertise this.

7.7 Only additions to the Policy are to refer to Telephone access and therefore this needs to be replicated on the Members Security Policy when submitted to Cabinet in the very near future.

7.8 Employee Side approves the Security Policy as it stands and supports the CMT initiative to provide enhanced Internet Café facilities for employees. Employee Side would also support a review on the implementation of the new policy within a year.

8. PORTFOLIO HOLDER COMMENTS

8.1 The Portfolio Holder supports the recommendation contained in this report.

9. RECOMMENDATIONS

9.1 ***It is recommended that*** Cabinet approve the revised ICT Security Policy for Employees as appended to this report.

For Further Information Contact:

Steve Cranston – Audit Manager
Tel: 02380 285786
Email: steve.cranston@nfdc.gov.uk

Janet Clarke – ICT Security Officer
Tel: 02380 285677
Email: janet.clarke@nfdc.gov.uk

Background Papers:

ICT Security Policy
(Available on the Intranet)
Draft ICT Security Policy for
Members – August 2003
(Copy available from the
ICT Security Officer)
LDA Review of Security Policy –
February 2003. (Copy available from the
ICT Security Officer)

Cabinet 2nd June 2004 – **Appendix 1**

New Forest
DISTRICT COUNCIL

INFORMATION & COMMUNICATIONS TECHNOLOGY

SECURITY POLICY
FOR EMPLOYEES

REVISION 1.1 – MAY 2004

ICT - SECURITY POLICY (EMPLOYEES)

Revision 1.1 – May 2004

Page No ***TABLE OF CONTENTS***

Section One *POLICY SUMMARY*

1.0 *Policy Statement*

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

- Information will be protected against unauthorised access and the confidentiality of information will be assured.
- The integrity of information will be maintained.
- That all legislative and regulatory requirements will be met.
- Appropriate use of the Internet will be maintained.
- Use of internal & external e-mail will meet required standards.
- The use of e-mail, Internet and Voice will be monitored in accordance with the ICT Security Policy and Standards.
- All breaches of the ICT Security Policy shall be reported.
- Breaches of policy will be investigated and any action taken against individual employees will be in accordance with the Police & Criminal Evidence Act 1984 and/or the Council's disciplinary procedure.
- An ICT Disaster Recovery Plan will be maintained and tested.

2.0 *Policy Overview*

2.1 Information & Communications Technology (ICT) systems 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.

2.2 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.

2.3 Adherence to this policy is a condition for using Council equipment and networks. Computer use may be monitored and any breach of this policy (actual or suspected) will be reported to and investigated by the Audit Manager. The Audit Manager in consultation with management may invoke formal disciplinary action against employees, and in cases of breach of Statute, the Police and other agencies may be consulted with a view to instigating legal action.

2.4 *Section 2* defines the applicability of this policy. It also considers personal use of the Council's ICT resources, training, and changes in technology and health and safety matters.

2.5 *Section 3* details the ICT Security Standards which form the basis of the Council's ICT Security Policy and conform to BS7799 national security standards.

2.6 *Section 4* defines the roles and responsibilities of officers and managers in the management of this Policy.

2.7 Cabinet approved this policy in May 2004.

3.0 Policy Summary – Do's and Don'ts

Employees are required to read this ICT Security Policy in full and in respect of Internet and external e-mail use will be required to certify that they have done so. However, some basic "do's and don'ts" are shown as an aide-memoire to users:

3.1 **DO:**

- Keep passwords and confidential data secure.
- Restrict access to authorised users only.
- Seek permission to use PCs, Internet or e-mail for personal use.
- Undertake personal use in your own time and not that of the Council.
- Use proprietary software in accordance with the licence of issue.
- Have all disks and CDs virus checked before use.
- Password protect (wherever possible) any Council documents or information e-mailed or transferred by other media to your home computer. Avoid transferring confidential, sensitive or personal information.
- Inform ICT of any starters, leavers and changes in authorised users.
- Have regard for relevant legislation.
- Report breaches of the ICT Security Policy to the ICT Security Officer.
- Seek advice if in doubt.

3.2 **DO NOT*:***

- Use Council equipment for personal gain.
- Store personal information on the Council's equipment.
- Send contentious or libellous electronic communication.
- Send offensive material, including jokes, on the Internal and External e-mail system.
- Access Internet sites in breach of legislation or that may cause offence to others.
- Use the Council's Internet domain to play games, gamble, make payment for personal goods or services or register with other ISP or e-mail providers.
- Import or download executable programs without the express permission of ICT.
- Download wallpapers or screensavers from the Internet
- Put the Council's reputation at risk.

4.0 Policy Advice & Guidance

4.1 Should you require any help or guidance with any matter concerning ICT Security, please phone Janet Clarke, ICT Security Officer on (023) 8028 5677 or e-mail janet.clarke@nfdc.gov.uk

Section Two *GENERAL GUIDANCE:*

This section defines who is covered by this policy and considers matters of personal use, training, health & safety and changes in technology.

1.0 Applicability Of This Policy

1.1 This policy applies to:

- All Council employees, using Council equipment from whatever location, including home.
- Other persons working for the Council, agency personnel or contractors whilst engaged on Council business or using Council equipment and/or networks.
- Any other use by Council employees, which identifies the user as a Council employee or which could bring the Council into disrepute.

1.2 This policy applies, in full, to business, formal homeworking and personal use of the Council's ICT resources.

2.0 Personal Use

2.1 The Council will permit the personal use of its computer equipment, Internet, e-mail and voice (telephones) facilities under the following additional conditions:

2.2 Personal Use of Computer Equipment

2.2.1 Using the Council's computer equipment for personal use is only permitted with the express permission of your Manager and must be undertaken in your own time. This includes the creation of CV's, letters and spreadsheets and the playing of pre installed Microsoft games.

2.2.2 To ensure that electronic storage space is not compromised, resulting in denial of service, personal material (e.g. personal letters, CV's and photo's etc.) must not be stored on the Council's Information Systems Network or on the local drives of the Council's computers. This applies equally to the storage of personal e-mails.

2.2.3 In respect of wallpapers and screen savers preference is given to the use of pre-installed Microsoft products in the personalisation of desktops. Use of photographic images for example of friends and family will be permitted provided that they are not offensive to others, are not otherwise stored on the Council's equipment and are subject to virus checking procedures as specified in Section 3 (paragraph 2.2.3) of this policy. PC wallpapers and screen savers must not be downloaded from the Internet.

2.2.4 The Council's equipment must not be used for personal gain. This can apply to both fraudulent and non-fraudulent activity. Running a business would fall into this category, as would the use of the Council's name and/or logo with a view to obtaining goods or services.

2.3 *Personal Use of the Internet*

2.3.1 Employees that have an Internet Connection may use it for occasional personal purposes at the discretion of their Director or Head of Service, provided:

- It is done in the User's own time and does not interfere with Council work.
- It is not related to a personal business interest.
- It is not tantamount to misuse of the Councils Internet system as defined in Section 3 paragraph 4.3 of this policy.

2.3.2 Managers are responsible for supervising 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 be subject to disciplinary action.

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

2.3.4 Employees are encouraged to use the computer facilities in the communal recreation areas for personal research in their own time.

2.4 *Personal Use of E-mail*

2.4.1 Personal use of e-mail should be kept to a minimum and employees should ask themselves how they would feel if the content of an e-mail were read by anyone other than the intended recipient. Where the subject is of a confidential nature another means of delivery should be considered i.e. internal or external post.

2.4.2 The creation of and response to personal e-mails should be done in the Users own time and should not affect the business of the Council.

2.4.3 All domain name registrations are verified by Ukerna naming committee, .gov.uk domains relate to council/local authority/government @NFDC.gov.uk has been assigned to the Council because we are a government body not a private business. It must not be used to conduct personal business interests or to transmit offensive text or images (including jokes however inoffensive they appear). Failure to adhere to this requirement may seriously damage the Council's reputation.

2.4.4 Users should have regard to what is deemed misuse at Section 3 (4.3) of this policy.

2.5 *Personal Use of Telephones*

2.5.1 The Council is part of the Hampshire Public Services Network (HPSN) for its telecommunications connections. This enables the authority to communicate via the telephone between sites and with other HPSN users incurring no additional costs. Where an HPSN ONNET telephone number is available it must be used and employees are encouraged to investigate the existence of these numbers when contacting other public authorities in the Hampshire area.

2.5.2 Personal calls made on Council telephones both static and mobile are restricted to those that are deemed necessary e.g. to make arrangements for lateness home. Again the reasonableness test applies and any personal calls made should be kept short and concise. Family and friends should be made aware that although the receiving of personal phone calls is allowed they should be kept to a minimum.

2.5.3 The use of personal mobile phones, whether receiving calls or text messages, can be disruptive to others in the office and should be switched off during work hours unless agreed otherwise with your Line Manager. Where it is necessary to leave a contact number during working hours i.e. for children at school, your extension number should be given.

3.0 Employees Joining and Leaving the Council

3.1 Managers (or the officer responsible) must ensure that the user has read the Security Policy and is aware of their Role and Responsibilities before requesting access to Information Systems.

3.2 There is a standard form that the manager responsible must complete for new employees and leavers (or temporary employees needing access to our information systems). These forms must be completed and returned to ICT at least one week before the start or termination date.

4.0 Training

4.1 All users will be trained to use e-mail, the Internet and the Intranet correctly and will be made aware of the security issues. Managers will be responsible for ensuring that employees are trained on computer systems applicable to their service.

4.2 New Employees will be made aware of ICT Security Policies as part of their induction package.

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

5.0 Changes in Technology

5.1 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.

5.2 Where developing technology necessitates changes in security measures the ICT Security Officer will review these measures.

5.3 The ICT Security Officer will issue instructions for any changes in security arrangements to all users using a variety of relevant communication channels.

6.0 Health & Safety

6.1 Employees are required to comply with the Council's Health & Safety Policy as it relates to the use and maintenance of electronic equipment.

6.2 Information on this and related matters such as Visual Display Unit (VDU) Assessments may be obtained from the Corporate Health & Safety Risk Manager.

Section Three ICT SECURITY STANDARDS:

These standards set the framework for the ICT Security Policy. Whilst these are New Forest District Council's own standards they are compliant with BS7799 national security standards.

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

1.1 Passwords

1.1.1 Access to the Council's Information Systems is controlled by the use of User ID's and secure passwords.

1.1.2 Passwords are a means of preventing access to systems or parts of systems by unauthorised users. They also identify users on system audit trails. The password should be made up from characters and numerals as a combination. It should not have repeated characters and should not be a name or any string that can be identified with the user easily i.e. surname, other family names, car registration, telephone numbers, etc.

1.1.3 All ICT users will be set up with an individual User ID and password. To ensure the integrity of data and the verification of electronic authorisation this is not to be divulged to anyone under any circumstances. It is advisable not to keep a manual record of individual password/s but if this cannot be avoided then such records must be kept secure at all times.

1.1.4 Group working will be permitted utilising shared drives and systems areas. However, access to such group work areas will only be granted by way of individual (personal) User ID and password to provide an adequate audit trail of activity on an individual user basis.

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

1.1.6 Should a user forget their ID or password or believe that another user knows their ID **and** password they should contact the ICT Help Desk immediately.

1.2 Other Access Controls

1.2.1 If access to a users data is required while the user is not present, an access request form must be completed by the line manager, if the line manager is not available access can be requested via the ICT Security Officer.

1.2.2 Computers should not be left unattended when signed on. If users need to leave their computer or laptop for any length of time they should ensure that current data is "saved" and access is prohibited, by logging out of all major applications and using a screen saver with a password or using the "lock workstation" option that NT offers.

1.2.3 If users need help with setting any of the above up they can call the ICT Helpdesk on extension 5797

1.3 Landesk

1.3.1 You should be aware that ICT Services have a network management tool that is capable of accessing your machine remotely. This will enable them to respond to help desk calls that have been logged and update any generic software i.e. virus checking agents and the synchronisation of clocks. Generally this maintenance will only be undertaken while you are present and with your knowledge although mass upgrades are likely to be completed out of hours.

1.4 Laptops

1.4.1 Users must not leave laptop/notebook computers unattended. When travelling with laptop/notebook computers or when they are not in use, users must ensure that they are put out of sight. The use of a plain carrying case, rather than one that is branded with the computer supplier's name, is recommended.

1.4.2 Any sensitive or confidential information that users have had to save on the local drive of the laptop/notebook must be password protected.

1.5 Homeworking

1.5.1 The Council maintains a formal "Homeworking" policy. Installation, maintenance and support of computer equipment and matters of health and safety are subject to that policy. Refer to Personnel Services for advice.

1.5.2 Employees should not generally transfer Council information, systems or data to their personal home computer. However, where agreed with their manager employees may transfer by e-mail or other media such information provided that it is not confidential, sensitive or contains personal data. Wherever practicable any information so transferred should be password protected. Floppy disks, CDs or other remote media used to transmit data to and from home must be subject to virus checks as specified in paragraph 2.2.3 below.

2.0 THE INTEGRITY OF INFORMATION WILL BE MAINTAINED

2.1 Data Security & Back Up:

2.1.1 Users must save all work on the appropriate network server. A storage area, usually a grouped area by department or section, will be established for this purpose.

2.1.2 System procedures must be established to backup data whenever it changes, either immediately or daily, and a complete backup of system's data files taken on an appropriate periodic basis. It is not normally necessary to backup software as the original disks will be available from ICT Services when necessary.

2.1.3 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 the server then other backup procedures should be put in place e.g. save a copy to A:\ (floppy disk).

2.1.4 In the event of server hardware failure or loss of connection to the server, computers should continue to operate. Users can work as normal on some applications but they will have to save work/data to C:\ (hard drive) until the server is fully functional then move the work/data to the relevant area on the server.

2.1.5 Work/data should not be saved to the C:\, unless no alternative is available. It should be noted that any work saved to the C:\ could be lost through it not being backed up or theft of the hard drive. Sensitive or confidential personal information should not be saved to the C:\ under any circumstance.

2.1.6 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) in accordance with the Councils Retention Policy.

2.2 Virus Checking:

2.2.1 A computer virus is a computer program. Unlike most other programs, viruses are specifically designed to spread themselves from one computer to others and, in some cases cause damage and annoyance.

2.2.2 Viruses normally enter organisations because an infected diskette, CD or program is brought into the organisation. It is also possible for an infected program file to be downloaded from the Internet.

2.2.3 ICT Services will ensure that computers are virus free when they are installed. To keep the computers free from viruses:

- ICT Services will keep all virus signatures up-to-date.
- Users must without exception submit all disks and CD's to ICT Services for virus checking before using them.
- Any downloads from the internet must be virus checked.

Please contact ICT Helpdesk for advice on the above.

3.0 REGULATORY AND LEGISLATIVE REQUIREMENTS WILL BE MET

All ICT users are subject to the following legislation. Other relevant Acts include the Obscene Publications Act 1959, Protection of Children Act 1978, Telecommunications Act 1984, Malicious Communications Act 1988, Human Rights Act 1998, Race Relations Act 1998 and Electronic Communications Act 2000. This list is not exhaustive.

3.1 Computer Misuse Act 1990

3.1.1 It is an offence for anyone to access or modify computer held data or software without authority, or to attempt to do so. These offences can carry a penalty on conviction of an unlimited fine or imprisonment for up to five years.

3.1.2 Using any of the Council's Systems or Internet access to attempt to access any Council or third party IT facility without authority is an offence under the Computer Misuse Act.

3.1.3 More information on this act can be found on the intranet or by contacting the ICT Security Officer on extension 5677.

3.2 Copyright Design and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992)

3.2.1 Essentially copyright is a right given to authors or creators of works such as books, films or computer programs to control the copying or other exploitation of their work. It is an offence to copy/install or authorise someone else to copy/install any of the above without the correct license or consent of the author. This offence can carry a penalty on conviction of a maximum imprisonment of two years.

3.2.2 Loading of unlicensed software is forbidden and may result in disciplinary action. In order to ensure compliance with the law and maintain security, the loading of software is restricted to ICT Services and other authorised persons.

3.2.3 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.

3.2.4 For further information contact the ICT Security Officer on extension 5677

3.3 Data Protection Act 1998

3.3.1 The Data Protection Act 1998 sets out rules for the processing of personal information and applies to some paper records as well as those held on computer. The Act regulates the collection, processing and disclosure of information relating to individuals and ensures that the information is safeguarded against accidental destruction or misuse.

3.3.2 The Act also provides individuals with a right to access information held about themselves. In order to comply with the Act the Council and its employees must adhere to the eight data protection principles. More information including the Council's Data Protection Policy and the eight principles can be found on the Intranet.

3.3.3 User 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 personal responsibilities, including criminal liability, that this brings. This will include not giving sensitive or confidential data to unauthorised colleagues or members of the public. If in doubt contact the Data Protection Officer on extension 5785.

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

3.3.5 Before committing personal data to newsgroups or web-sites you must ensure the Data Protection Principles are adhered too.

3.4 Freedom of Information Act 2000

3.4.1 The Freedom of Information Act 2000 establishes a right for any person making a request to a public authority to be informed in writing whether or not the authority holds the information sought and, if so, to have access to that information subject to some limited exemptions. The Act makes it an offence for any person, including employees, to alter, deface, block, erase, destroy or conceal records held by a public authority with the intention or preventing disclosure to an applicant who has requested the information.

3.4.2 All information is covered under the Act, this includes manual and electronic records and extends to e-mails and post it notes. Users should be aware of this right of access when compiling notes and records, which should be done in a professional and factual manner.

3.4.3 In compliance with the Act the retention and destruction of records should be done so in accordance with the Council's Records Management Policy and associated retention schedules.

3.5 Libel & Defamation

3.5.1 Libel law extends to electronic communication. Action may be taken against both the Council and the originator in respect of any libellous communication.

4.0 USING THE INTERNET

4.1 Internet Connections

4.1.1 All connections to the Internet will be arranged through ICT Services.

4.1.2 Connection to the Internet will be channelled via management software. This software will provide an account of all incoming and outgoing network connections***.***

4.1.3 All Internet access will be through a firewall to the Council's Internet Service Provider who protects the Council's network from viruses and unauthorised entry via the Internet.

4.2 Access

4.2.1 Internet capability will be installed on each networked computer within the Council. Directors and Heads of Service (Authorised Requesters) will be responsible for authorising the connection. Authorisation cannot be delegated to any officer below the rank of Heads of Service. Access will not be provided without this authorisation.

4.2.2 Access to certain sites will be blocked via the network management software, if they are deemed to be unsuitable for Council usage.

4.2.3 Employees may 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.

4.2.4 Users are not permitted to use their browsers for connecting to Internet e-mail sites and must only use the e-mail system provided by the Council.

4.3 Misuse

4.3.1 It is incumbent on employees not to misuse the Council's Internet facilities. Misuse of the Council's Internet facilities will include:

- Creation, use, transmission or encouragement of material, which is illegal, obscene or libellous, is offensive or annoying, defamatory or infringes another person's copyright.
- Transmission of unsolicited advertising or commercial material
- Obtaining unauthorised access to the Council's or another organisation's ICT facilities.
- Violating other people's privacy.
- Using chat lines or similar services.
- Online banking facilities other than the business of the Council.
- Any online sale or purchase of goods and services for personal purposes.
- Payment of personal bills.
- Playing games and gambling.
- Illegal activities including breaching the Data Protection, Computer Misuse and Design Copyright and Patents Acts.
- Wasting network and other resources.
- Disrupting the work of others in any way by introducing viruses or by corrupting data.
- Expressing personal views, which could be misinterpreted as those of the Council.
- Committing the Council to purchasing or acquiring goods or services without proper authorisation or following appropriate Financial Regulations, Standing Orders and without regard to the Council's Procurement Strategy.
- Importation or downloading of executable program files without the express permission of ICT Services.
- Downloading copyrighted or confidential information.
- Failing to adhere to this policy.

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

4.3.3 A good test is whether, with hindsight, you could justify your actions to your manager or a member of the public (Code of Conduct).

4.4 Offensive And Illegal Material

4.4.1 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 or nudity.

4.4.2 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.

4.4.3 Users should be aware of the risk of inadvertently accessing inappropriate sites. Any employee accidentally accessing offensive material should inform their manager and the ICT Security Officer immediately. Accidental access will not result in disciplinary action, but failure to report it may do so.

4.4.4 People who receive offensive or sexually explicit mail should inform their manager and the ICT Security Officer immediately. Such material may not be identifiable until an e-mail is opened and in these circumstances employees will not be held responsible provided they promptly report it.

4.5 Publication and Quality of Information on the Internet and Intranet

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

4.5.2 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 CMT and follow standards set by ICT Services.

4.5.3 Any publication of unsuitable material on either the Council's web site or Intranet will be regarded as misconduct. Advice on suitability should be sought from the Internet Development Team.

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

4.5.5 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.

4.5.6 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.

5.0 USING E-MAIL

5.1 Security & Content of E-Mail

5.1.1 E-mail either internal or external 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.

5.1.2 E-mail must not be used for sending offensive, threatening, defamatory or illegal material. The transmission of jokes on both the Council's internal and external e-mail systems is prohibited.

5.1.3 Users should be particularly careful about what they commit to e-mail. It can be used as evidence in internal disciplinary and grievance hearing as well as more formal external settings. 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. Users should also reflect on the areas of misuse noted at Section 3 (4.3).

5.1.4 The use of e-mail offers the opportunity to send personal information electronically. However due to its nature, employees deciding to transmit personal data via e-mail should take regard of the appropriateness of this transmission to ensure that Data Protection Principles are adhered to. Employees may like to consider alternative methods of delivery i.e. internal or external mail. If there is any doubt as to the appropriateness of the content of an e-mail advice should be sought from the Council's Data Protection Officer.

5.1.5 Information retained or stored electronically may be required to be produced under the Data Protection and/or Freedom of Information Acts

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

5.1.7 E-mail must not be used for personal business or gain

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

5.1.9 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.

5.1.10 Circulating general e-mail messages to all users is a useful way of conveying information. 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. The Intranet should be used to display certain information instead of sending an e-mail to all.

5.1.11 Employees 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 the ICT Security Officer.

5.1.12 Junk mail (spam) is a hazard of Internet life. Employees registering their e-mail address on the Internet should be aware that "spammers" get their mailing lists this way. Please take care where you register your Council e-mail address.

5.1.13 The Council has facilities to block individual junk e-mail addresses. Refer repetitive junk mail received to the ICT Security Officer for action.

5.1.14 Restrict the size of e-mail attachments wherever possible. The Council's filter systems will generally prohibit attachments over 2mb. Use "zip" files where necessary.

5.1.15 The use of "away from the office" messaging should not include personal details such as home address and telephone numbers and should not state specific dates of holiday absences. Messages should be kept to a minimum and as bland as possible e.g. *"I am unable to deal with your enquiry at the moment but if you require an immediate response please contact…".*

6.0 *THE USE OF THE INTERNET, ELECTRONIC MAIL AND VOICE WILL BE MONITORED IN ACCORDANCE WITH THE ICT SECURITY POLICY*

6.1 Internet and e-mail usage will be closely monitored by the ICT Security Officer to ensure compliance with this policy thus safeguarding the Council's networks and providing protection for the organisation and its employees. All users should not expect Internet or e-mail related activities to be considered private.

6.2 Browser connections to the Internet will be challenged by management software. This software provides a detailed account of all incoming and outgoing network connections by individual users.

6.3 From this automated monitoring system the ICT Security Officer 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.

6.4 Analysis of usage is limited to users with the highest number of recorded browsing hours, where a breach/misuse has been reported or at the request of Management. Where this analysis confirms actual or potential misuse it will be reported to the Audit Manager for investigation. This could result in disciplinary action, which may lead to dismissal. Where necessary the ICT Security Officer will advise Managers on the suitability of material, investigate and seek the opinion of the Police.

6.5 The Council also has an e-mail management system, which enables us to report on the traffic outbound and inbound to our mail servers. These reports detail: [Sent to/ Received from/Subject /Attachment type/Date and Time]

6.6 This traffic is monitored and may provide information, which indicates actual or potential misuse. Depending on the type and severity of the misuse, the ICT Security Officer will refer the reports to the Audit Manager for an impact assessment on the necessity to examine the content of the e-mails. Again misuse could result in disciplinary action, which may lead to dismissal. Where necessary the ICT Security Officer will advise managers on the suitability of material, investigate and seek the opinion of the Police.

6.7 Recipients of external e-mail are informed via the disclaimer that their e-mail may be subject to monitoring.

6.8 The HPSN voice system enables phone usage to be monitored and is able to report on duration and destination of calls made, these reports are restricted to itemised call records and do not monitor call content. A separate system operates in some areas of the Council i.e. Revenues that enables monitoring to a greater extent. This includes the ability to record and listen to calls made and received to ensure good customer service and to identify training needs

7.0 *REPORTING OFFENCES (WHISTLEBLOWING)*

7.1 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.

7.2 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.

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

8.0 ***ALL BREACHES OF THE SECURITY POLICY WILL BE INVESTIGATED***

8.1 All investigations will be undertaken at the direction of the Audit Manager and will be conducted in line with the severity of the breach.

8.2 For criminal offences investigations will be conducted in accordance with the Police and Criminal Evidence Act.

8.3 All other investigations will be conducted in accordance with the Council's Disciplinary Rules.

9.0 ***AN ICT DISASTER RECOVERY PLAN WILL BE MAINTAINED AND TESTED***

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

9.2 Contracts with suppliers of ICT software and/or hardware should include maintenance response times and provision for use of substitute hardware, possibly at a different location. Departments should consider standby arrangements when work is being scheduled to take place outside normal hours.

Section Four ROLES AND RESPONSIBILITES

1.0 **The main contacts relating to the management of this policy are**:

- Assistant Director (Financial Services) – Overall responsibility for ICT Security, Data Protection and Freedom of Information
- Assistant Director (ICT) – Head of ICT
- Audit Manager – Audit & Investigations
- ICT Security Officer - ICT Security Policy & Monitoring
- Senior Auditor and Data Protection Officer – Data Protection & Freedom of Information
- Head of Legal & Democratic Services – Legal advice
- Corporate Health & Safety Risk Manager – Health & Safety

2.0 **The roles and responsibilities of employees and managers are**:

Responsible Officer	***Responsibilities***
CMT	To endorse and fully support the application of the policy across the authority.
Assistant Director (ICT)	To manage the Council's ICT environment. To ensure that ICT maintains a Disaster Recovery Plan. To ensure ICT employees only install software for which a valid licence is held.
Head of Legal & Democratic Services	To advise on associated legislation as required.
Audit Manager	To monitor employees' use of systems and take disciplinary action when required. To ensure that all suspected breaches are investigated
ICT Security Officer	To implement the access standards across ICT infrastructure and liaise with all systems administrators ensuring that all user details are maintained and up-to-date. To check system logs of users access to systems and all monitoring reports for breaches in Policy. To provide information to the Audit Manager on any attempted or actual security breaches. To check regular data and system back ups of corporate systems are carried out and completed and ensure that the data is recoverable. Co-ordinate the ICT Disaster Recovery Plan in relation to technology based services across the Council's sites and verify its adequacy.
Senior Auditor and Data Protection Officer	To ensure that employees understand the implications of maintaining the integrity of data and to ensure that all information systems holding data are (where applicable) properly registered with the Information Commissioner.

Responsible Officer	***Responsibilities***
Project & Business Analyst (ICT)	In respect of Voice (Telephony) to provide User logs as necessary.
Managers	To ensure that employees are aware of the policy and standards and relevant legislation at induction and have the relevant training. To inform the ICT Helpdesk promptly about employees leaving, or access being terminated. To ensure that software is only installed by ICT employees. To ensure that employees comply with the Policy and Standards and Legislation. To monitor use and refer cases to the Audit Manager. Create relevant business continuity plans prioritised across the business unit.
Employees	To comply with the Policy, Standards and Legislation. To ensure that any software to be installed is registered with ICT Helpdesk for installation by ICT employees. To be aware of the Business Unit plan and their role in its implementation should this be required.