Chapter 37 A

INFORMATION & COMMUNICATIONS TECHNOLOGY

SECURITY POLICY & GUIDANCE FOR MEMBERS

JUNE 2006

TABLE OF CONTENTS

Section 1

POLICY SUMMARY

1.0 Policy Statement

New Forest District Council will ensure that:

- Information will be protected against unauthorised access and the confidentiality of information will be assured.
- The integrity of information will be maintained.
- All legislative and regulatory requirements will be met.
- Appropriate use of the Internet will be maintained.
- Use of email will meet required standards.
- The use of email and the Internet will be monitored in accordance with this policy.
- All breaches of the ICT Security Policy will be taken seriously and any action taken against individual Members will be in accordance with the Code of Conduct or the Council's guidelines for dealing with breaches of local codes or policies.
- An ICT Disaster Recovery Plan will be maintained and tested.

2.0 Policy Overview

2.1 Information & Communications Technology (ICT) equipment and networks must be used responsibly and legally. Members must not misuse them by taking any action that 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. Members should not interfere with any pre–established operational and/or anti virus settings established by the Council or it's agents without express authority.

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. Failure to adhere to this policy is a serious offence, any breach of this policy (actual or suspected) will be reported to the Chief Executive who with the ICT Security Officer will carry out an internal investigation. Where the breach is in excess of a minor indiscretion it will be reported to the Monitoring Officer in line with the Council's Complaints Procedure. Where illegal material has been accessed, the matter will also be reported to the Police.

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

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

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

2.7 The Council approved this policy in July 2006.

3.0 Policy Summary – Do's and Don'ts

3.1 Members are required to read this ICT Security Policy in full and will be required to certify that they have done so. However, here are some basic "***do's and don'ts***" as an aide-memoir:

3.2 ***DO:***

- Keep passwords and confidential data secure.
- Keep personal use to a minimum. As far as practicable this should be limited to just two hours a week as ratified by Cabinet in April 2003.
- Password protect any confidential or sensitive documents emailed or transferred by other media to or from your computer. Try and avoid transferring confidential, sensitive or personal information unless you are certain that only the intended recipient will see the content. [*Guidance – verify addressee* ***before*** *transmitting and avoid using global addresses such as info@ or admin@ in these circumstances].*
- Remember when sending emails it is easy to be misunderstood. Emotional meaning can often be lost in email messages and humour is easily misinterpreted. Keep your message to the point and do not be ambiguous.
- Be aware that emails can be used as evidence in internal investigations as well as more formal external settings. Defamatory comments may result in legal action.
- Restrict the size of attachments where possible (a 2Mb maximum is recommended). Remember colleagues may be receiving your email over lower speed communication links and messages with high graphical content may fail to download.
- Have regard for relevant legislation. [*Guidance – refer to Section 3 Paragraph7 of this policy].*
- Ask for help if you think you may need to install any additional hardware or software.
- Inform the ICT Security Officer (Janet Clarke) if you accidentally enter an inappropriate web site.
- Seek advice if in doubt through the ICT Helpdesk.

3.3 ***DO NOT*****:**

- Use Council equipment for personal gain or personal business interests.
- Allow others to log in to and use your computer.
- Interfere with pre-set anti virus protection settings.
- Send contentious or libellous electronic communication.
- Send offensive material, including jokes, on the Council's email system.
- Access Internet sites that may cause offence to others or breach this policy.

- Use the Council's Internet domain to play games, gamble or register with other ISP or email providers.

- Import or download executable programs/software without the express permission of ICT. This includes software upgrades.

- Download wallpapers or screensavers from the Internet

- Put the Council's reputation at risk.

3.4 Policy Advice & Guidance

3.4.1 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 *email:* **janet.clarke@nfdc.gov.uk**

3.4.2 All technical problems or issues should be referred via the Council's ICT Help Desk. Telephone 02380 285797or *email:* ***help.desk@nfdc.gov.uk***

Section 2

GENERAL GUIDANCE:

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

1.0 Applicability of this Policy:

1.1 This policy applies to:

- All Council Members, using Council equipment or when connected to the Council's Network from whatever location, including home.
- All Members using their own equipment or equipment not belonging to the Council, when connected to the Internet for browsing and email via the Council's Telecoms and Internet Service Provider or accessing the Council's Network.
- Any other use by Members, which identifies the user as a Councillor.

2.0 Personal Use

2.1 The facilities should be used primarily for Council business. However, the Council wishes to encourage Members to explore the Internet in a constructive manner. Consequently, occasional personal use of two hours a week is permitted provided it conforms to this policy and is not associated with personal business interests.

2.2 In respect of wallpapers and screen savers preference is given to the use of pre-installed Microsoft products. Personalisation of desktops is permitted e.g. with the use of photographic images etc., provided that they are not offensive to others and are subject to virus checking procedures as specified in Section 3 (paragraph 6.0) of this policy. PC wallpapers and screen savers must ***not*** be downloaded from the Internet.

2.3 The Council's equipment must not be used for personal gain. Running a business would fall into this category.

2.4 To ensure that electronic storage space is not compromised, resulting in denial of service, personal material (e.g. personal letters, CV's and digital photographs) must not be stored on the Council's Information Systems Network. However, personal material may be stored on local drives outside of the "My Documents" folder (see also Section 3 paragraph 5.1) but should not be regarded as private and will not be recovered in the event of system failure or reloading of the computer's default setup. This applies equally to the storage of personal emails.

2.5 If a Member wishes additional hardware or software not currently provided by the Council to be installed, a request must be made to ICT who will determine if the requirement will conflict with the computers configuration and advise on the installation. If this results in the Council's computer becoming unreliable the standard configuration will be reloaded.

2.6 All requests for business expenditure are managed through the Democratic Services Unit to maintain proper budgetary control. Therefore the use of personal Credit Cards to purchase goods and services of a business/constituency nature online via the Council's computer is **not** permitted. However the occasional on-line purchase of a personal nature is permitted with the caveat that the Council takes no responsibility for the transaction or the security of personnel details submitted in the transaction or the debt itself.

3.0 Personal Use of Email

3.1 The Ukerna naming committee has assigned the domain names of "@nfdc.gov.uk" & "@newforest.gov.uk" to the Council. These domain names 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.

3.2 Members should have regard to what is deemed misuse at Section 3 (paragraph 10.0) of this policy.

4.0 Training

4.1 All Members will be trained to use email, the Internet and the Intranet correctly and will be made aware of the security issues. Additionally, ICT Services and/or their agents will monitor "user" competency during home visits and offer advice accordingly.

4.2 Members will be required to certify that they have read and understood the ICT Security Policy.

5.0 Health & Safety

5.1 Members must have regard to the corporate policy on health and safety matters relating to display screen equipment, which is shown on the Council's Intranet.

Link to Intranet

5.2 ICT Services and/or their agents will monitor "user" adherence to health and safety matters during home visits and offer advice accordingly.

Section 3

***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.

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

1.0 Passwords

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

1.2 Passwords are a means of preventing access to systems or parts of systems by unauthorised users. They also identify Members 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.

1.3 All Members will be set up with an individual User ID and password. To ensure the integrity of data and the verification of electronic authorisation these are not to be divulged to anyone (including family members) under any circumstance. 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.

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

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

2.0 Other Access Controls

2.1 If Members 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 Microsoft Windows offers.

2.2 If Members need help with setting any of the above up they should call the ICT Helpdesk on 02380 285797

3.0 Connecting To The Council's Network via Unknown Computers

3.1 The remote access system enables Members to connect into the Council's network for email and Intranet systems from any computer and location e.g. cyber cafes worldwide. Members will need the "Forestweb" website address and their login and password. Once connected the email system that will be available is Web Outlook.

[Guidance - be aware there are some differences between Web Outlook and standard Outlook. ICT will be able to advise and give training on these differences. Please call the ICT Helpdesk on 02380 285797].

3.2 When connecting to an unknown computer, Members must ensure that they do not save any information to that computer. For example when reading emails with an attachment, the attachment should be opened in a browser window. This will ensure that the data is not downloaded and the integrity of the information maintained.

4.0 Laptops

4.1 When travelling with portable computers Members 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.

4.2 Any sensitive or confidential information that Members have had to save on the local drive of the laptop/notebook must be password protected or saved in an encrypted folder.

THE INTEGRITY OF INFORMATION WILL BE MAINTAINED

5.0 Data Security & Back Up:

5.1 Back-up software is installed and configured on Members computers and is set to take a back-up copy of the data stored in the "My Documents" folder only. Members must ensure that data is saved to this folder if they require a backup copy to be created.

5.2 This process will only run when members connect to the Council's network.

5.3 Members must ensure that they check on a regular basis that any data stored is still required and if not that it is deleted or archived. Members will be trained on archiving routines.

6.0 Virus Protection

6.1 Viruses can seriously disrupt operations. Anti-virus and Internet security software has been installed and should automatically check downloads, floppy disks, CDs and memory sticks inserted into the computer.

6.2 Virus checking software is installed and configured to be updated automatically this process must be allowed to run without interruption or change.

REGULATORY AND LEGISLATIVE REQUIREMENTS WILL BE MET

7.0 Legislation

7.1 All Members are subject to the following legislation. The list is not exhaustive and other relevant legislation would include for example the Obscene Publications Act 1959, Protection of Children Act 1978, Telecommunications Act 1984, Malicious Communications Act 1988, Criminal Justice Act 1988, Human Rights Act 1998, Race Relations Act 1998 and Electronic Communications Act 2000. Further information can obtained on the Intranet, Internet or by contacting the Council's ICT Security Officer.

7.2 Computer Misuse Act 1990

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

7.2.2 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 this act.

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

7.3.1 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.

7.3.2 Loading of unlicensed software is forbidden and may result in action being taken against the offender. In order to ensure compliance with the law and maintain security, software may only be loaded by ICT Services or their agents.

7.3.3 Using the Internet to download or otherwise copy copyrighted software, information or other material without adhering to its licensing conditions is an offence under this act.

7.4 Data Protection Act 1998

7.4.1 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.

7.4.2 Members 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.

7.4.3 Laptops or visual display units should not be located in such a position that screen displays are visible to unauthorised users or members of the public.

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

7.5 Freedom of Information Act 2000

7.5.1 The Freedom of Information Act ("the Act") gives access to information held by public authorities. A member of the public can make a request for such information. Information is only deemed to be held by the authority when it relates to the business of the authority. Whilst personal written communications between members such as e-mails are retained on the authority's server, the Council would not 'hold' this information (for the purposes of the Act) as it has no interest in it. However, where e-mails or other communications between members contain a mixture of council business and personal content, it would be appropriate (subject to a very limited number of exemptions) to disclose those parts of the

e-mail relating to council business. Therefore you should not mix personal or political content with council business in e-mails.

7.5.2 The business of political parties does not form part of the functions of the authority. Information passing (electronically or otherwise) between members on party political matters are not 'held' by the Council and therefore would not be discloseable under the Act. The same general principle applies to information held by Councillors when they conduct constituency business (although it could be subject to the Data Protection Act). However, information held electronically as part of their council duties (e.g. as a Committee or Cabinet member) will be subject to the Act. Members could therefore be asked by officers to search their records and to confirm or deny the existence of information in their possession. It is an offence to destroy information that is the subject of a request for disclosure, unless the information is destroyed in accordance with the Council's policy on destruction of documents. As far as members are concerned, information which would be potentially discloseable under the Act should be kept for at least 28 days. Thereafter it can be destroyed. If in any doubt, Members should contact either Rebecca Drummond, Senior Auditor and Data Protection Officer (telephone: 02380 285785) or Grainne O'Rourke, Head of Legal & Democratic Services (telephone: 02380 285285) for advice.

7.6 Libel & Defamation

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

USING THE INTERNET

8.0 Internet Connections

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

8.2 All Internet access will be through the Council's network management software and Internet Service Provider who protects the Council's network from viruses and unauthorised entry via the Internet.

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

9.0 Access

9.1 Members may only join newsgroups that relate to areas of the Council's work or professional interest.

9.2 Members posting information to newsgroups should not include any information that brings the Council into disrepute.

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

9.4 Members may only use the email systems provided by the Council. Establishing email accounts with other service provider e.g. MSN Hotmail or BT/Yahoo Mail is not permitted.

10.0 Misuse

10.1 It is incumbent on Members not to misuse the Council's Internet facilities. Misuse will include:

- Creation, viewing, use, transmission or encouragement of material, which is illegal, obscene or libellous, offensive or annoying, defamatory or infringes another person's copyright. Obscenity includes all levels of pornography and nudity (see paragraph 11.0 below).
- 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.
- Payment of bills in respect of Council business or personal debts. However, occasional on-line purchase using personal credit cards is permitted at the users' risk.
- Playing games and gambling on-line.
- 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.
- Importation or downloading of executable program files.
- Downloading copyrighted or confidential information without the authors permission.
- Failing to adhere to this policy.

This list is not exhaustive but is an indication of the types of conduct that may result in action being taken against the Member.

10.2 A good test is whether, with hindsight, you could justify your actions to a member of the public.

11.0 Offensive And Illegal Material

11.1 For the purposes of this policy 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 other persons with particular sensitivities, even if it is not explicitly offensive, e.g. religious views or nudity.

11.2 The Internet contains huge volumes of useful information. It also contains some offensive material. Any member using Council facilities for viewing or downloading such material will face appropriate formal action. If illegal material is accessed the Council will inform the Police and criminal prosecution may follow.

11.3 Members should be aware of the risk of inadvertently accessing inappropriate sites. Any member accidentally accessing offensive material should inform the ICT Security Officer immediately. Accidental access will not result in formal action being taken, but failure to report it may do so.

11.4 Members who receive offensive or sexually explicit mail or pop-ups should inform the ICT Security Officer immediately. Whilst Members are required wherever possible to verify authenticity of senders and therefore validity of content such material may not be identifiable until an email is opened and in these circumstances Members will not be held responsible provided they promptly report it.

12.0 Members Web Pages

12.1 Councillors' individual web pages have been constructed and are intended to assist Councillors to communicate with their constituents. While the Council will retain responsibility for maintaining the Councillors' area as a whole, and for each Councillor's home page, Councillors are responsible for editing and maintaining the other pages of their web sites. The Council does not accept responsibility for the content of the sites, with the exception of the home pages.

12.2 In posting information on their web sites, Councillors must comply with all of the security standards set out above. In addition to possible action against members for breaches of security as set out in Section 1 of this policy, or possible criminal proceedings in case of breaches of legislation, the Council reserves the right to suspend an individual Councillor's site for failure to adhere to the principles set out in this policy.

Political Publicity

12.3 Members may not use their sites to promote political campaigns or to advocate political stances on issues. They may not use the site to promote a political party or persons identified with a political party. They may, however, provide links from their sites to those of political parties or other organisations promoting a particular point of view, providing that these links do not otherwise contravene this security policy. Members are referred to the following extract from the Government's Code of Practice on local authority publicity that deals with publicity about individual councillors;

12.3.1 "Publicity about individual councillors may include the contact details, the positions they hold in the Council and their responsibilities. Publicity may also include information about individual Councillor's proposals, decisions and recommendations only where this is relevant to their position and responsibilities within the Council. All such publicity should be objective and explanatory and whilst it may acknowledge the part played by individual councillors as holders of particular positions in the council, personalisation of issues or personal image making should be avoided.

12.3.2 Publicity should not be, or liable to misrepresentation as being, party political. Whilst it may be appropriate to describe policies put forward by an individual councillor which are relevant to his/her position and responsibilities within the council, and to put forward his/her justification in defence of them, this should not be done in party political terms, using political slogans, expressly advocating policies of those of a particular political party, or directly attacking policies and opinions of other parties, groups or individuals."

Restrictions During Election Periods

12.4 During election times (from the publication of the Notice of Election to the date of the election) most parts of the Councillors' web sites will be suspended.

USING EMAIL

13.0 Security & Content of Email

13.1 Email 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.

13.2 Email must not be used for sending offensive, threatening, defamatory or illegal material. The transmission of jokes on the Council's email system is prohibited.

13.3 Members should be particularly careful about what they commit to email as it may be used in actions against them. Sending an email is the same as sending a letter or publishing a document in law, so defamatory comments could result in legal action. Internal email has been used successfully as evidence in libel cases. Members should also reflect on the areas of misuse noted at Section 3 (paragraph10.0).

13.4 The use of email offers the opportunity to send personal information electronically. However due to its nature, members deciding to transmit personal data via email should take regard of the appropriateness of this transmission to ensure that Data Protection Principles are adhered to. Members 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 email advice should be sought from the Council's Data Protection Officer.

[Guidance – please note that information retained or stored electronically may be required to be produced under the Data Protection and/or Freedom of Information Acts].

13.5 Email 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).

13.6 Email must not be used for personal business or gain.

13.7 Members posting information to newsgroups should not include any information that brings the Council into disrepute (see paragraph 9.2).

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

13.9 Circulating general email messages to groups of recipients is a useful way of conveying information. However, it can alienate and offend recipients if they are subjected to frequent irrelevant mail. Senders should carefully select the addressees to whom they wish to send their mail.

13.10 Members should not re-send email chain letters and should exercise caution with any email that asks the reader to forward it to others. If in doubt seek advice by contacting the ICT Security Officer.

13.11 Junk mail (spam) is a hazard of Internet life. To minimise the risk of spamming Members should avoid registering their email address on the Internet wherever practicable.

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

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

13.14 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…".

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

14.0 Monitoring

14.1 The ICT Security Officer will monitor email traffic and file transfers or networks connections, irrespective of whether the use is for Council business or private. The content of email will only be examined as part of an investigation. Members should not expect any Internet related activities to be considered private.

14.2 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. 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.

14.3 The Council also has an email management system, which enables high level reports on inbound and outbound traffic to the Council's mail servers. 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 emails. Again misuse could result in an investigation. Where necessary the ICT Security Officer seek advice on the suitability of material and may seek the opinion of the Police.

14.4 Recipients of external email are informed via the disclaimer that their email may be subject to monitoring.

15.0 Reporting Offences (Whistle Blowing)

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

15.2 Members are asked to refer to the Anti-Fraud and Corruption Policy and the Council's Whistle Blowing at Work policy where any Member who suspects a breach of the Security Policy must inform the S.151 Officer or Audit Manager promptly.

Intranet Link to the Anti Fraud & Corruption and Whistle Blowing at Work policies

16.0 Suspected Breaches of the Security Policy will be Investigated

16.1 Alleged breaches will be taken seriously. Preliminary investigations will be conducted by the Audit Manager and may be referred to the Chief Executive and/or the Council's Monitoring Officer and dealt with in accordance with the Members codes.

16.2 Any potential criminal investigation will be conducted in accordance with the Police and Criminal Evidence Act 1984.

AN ICT DISASTER RECOVERY PLAN WILL BE MAINTAINED AND TESTED

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

Section 4

ROLES AND RESPONSIBILITES

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

Chief Executive	Head of Paid Services. To be consulted on any breach of policy
Monitoring Officer	Democratic and legal advice. Dealing with possible breaches of policy in relation to members
Assistant Director of Resources (ICT Services)	Head of ICT
Assistant Director of Resources (Financial Services)	Overall responsibility for ICT Security, Data Protection and Freedom of Information
Audit Manager	Audit & Investigations
ICT Security Officer	ICT Security Policy & Monitoring
Senior Auditor and Data Protection Officer	Data Protection & Freedom of Information advice
Corporate Health & Safety Risk Manager	Health & Safety advice

2.0 The roles and responsibilities of employees and managers are:

Council	To endorse and fully support the application of the policy across the authority
Chief Executive	To Investigate breaches in the Security Policy. Where the breach is in excess of a minor discretion report it to the Monitoring Officer in line with the Council's Complaints Procedure.
Monitoring Officer	To advise on associated legislation as required. To conduct actions against Members
Assistant Director of Resources (ICT Services)	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.
Assistant Director of Resources (Financial Services)	Overall responsibility for ICT Security, Data Protection and Freedom of Information

Audit Manager	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 Members 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 Members 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
Corporate Health & Safety Risk Manager	To offer Health & Safety advice
Members	To comply with the Policy, Standards and Legislation