C

CABINET - 7 MARCH 2012 **PORTFOLIO: FINANCE & EFFICIENCY**

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECURITY POLICY

1. PURPOSE

1.1 The ICT Security Policy has been reviewed and updated as part of the implementation of the ICT Strategy 2009-2013. The ICT Security Policy must be approved by Cabinet and full Council.

2. INTRODUCTION

2.1 The ICT Security Policy is a key component of the overall ICT security framework in operation at New Forest District Council. The ICT Security Policy has been reviewed and updated to take account of changes to the council's ICT infrastructure, ongoing requirements to comply with strict public sector ICT security standards and to recognise the opportunities and threats rising from new technologies such as smart phones and new ways of working such as using social media facilities like *Facebook* and *Twitter.*

3. MEMBERS' USE OF ICT

3.1 Members of the council can claim an allowance to provide up-to-date ICT facilities to assist them in their role and to assist the council organisation to operate as efficiently as possible e.g. reducing the distribution of hard copies of documents and related postage costs by using e-mail and the internet. Members' own ICT equipment is not directly attached to the council's network and the security risks are therefore minimised. For this reason the members' use of ICT is being developed in the form of a simple guidance note highlighting best practice and is **not** covered by this ICT Security Policy.

4. FINANCIAL IMPLICATIONS

4.1 The day-to-day operation of the ICT security function is funded through the operational budget for ICT Services. No specific funding is sought in respect of the updated ICT Security Policy.

5. ENVIRONMENTAL / CRIME AND DISORDER AND EQUALITY AND DIVERSTY IMPLICATIONS

5.1 The ICT Security Policy is intended to underpin various measures aimed at minimising all potential threats to the Council's information and information systems. There are no other direct implications.

6. RECOMMENDATIONS

6.1 That Cabinet recommends to the Council the ICT Security Policy at Appendix 1 is approved.

For Further Information Please Contact:
Ken Connolly
Head of ICT Services
Tel (023) 8028 5588
Email ken.connolly@nfdc.gov.uk

APPENDIX 1

New Forest
DISTRICT COUNCIL

INFORMATION, COMMUNICATIONS & TECHNOLOGY

SECURITY POLICY & GUIDANCE

February 2012
(Version 2.1)

New Forest District Council

ICT Security Policy

CONTENTS

Foreword:

Why have a security policy?

The massive growth in the use of computers at work has brought with it issues of computer security. There have been some highly publicised cases in the national media of loss of data or data falling into the wrong hands. The Council has to abide by some very strict government rules about the handling of restricted information. Working and sharing data with other agencies must also be done under controlled conditions.

The ICT Security policy will ensure the confidentiality, integrity and availability of information needed to do the Council's business.

Isn't our network secure then?

Our network is very secure. This policy ensures that we keep it that way.

Who's it for?

The ICT Security policy lays down this Council's rules for using ICT facilities and must be followed by all staff, as well as any contractors, software suppliers and anyone else having access to the Council's ICT systems.

Strict rules are needed but hopefully you will find that this document presents them in a readable style, using plain English.

Won't it stop me doing my job?

It is not our intention to prevent you accessing the programs and data you need to do your job. The intention is to give you that access but under well-controlled conditions.

New job?

Your manager will tell ICT Services about any new member of staff and what systems you need to use.

You need to sign up to the Security Policy

Firstly, you'll get security policy training, then you'll sign to say you understand the policy. No-one gets access to ICT systems without it.

Then you'll need to **apply the policy in your everyday work.**

As ever, ICT Services staff are here to help you; if you have any queries on this document or on ICT Security generally, ring the ICT Service Desk (ext. 5300) and select Option 6.

Ken Connolly - Head of ICT Services

SECTION 1: INTRODUCTION

1.1 Policy Statement

1.1.1 This Policy aims to:

- Ensure that information will be protected against unauthorised access and the confidentiality of information will be assured.
- Ensure that information is accurate, complete and available.
- Minimise Information Security Incidents.
- Ensure the Council gets maximum benefit from technology.
- Ensure technological resources are managed effectively.
- Prevent inappropriate use of the Council's equipment and data.
- Help the Council meet legislative requirements, including the Government Connect Code of Connection.
- Maintain the security of data handling.
- Define how the use of ICT systems will be monitored and how security breaches will be dealt with.

1.1.2 This Policy applies to:

- Employees engaged in work for the Council while working from home, in the Council offices or any other location.
- Other individuals engaged in work for the Council, such as agency personnel, contractors, students on work experience /placement and employees from partner organisations or using Council equipment and/or networks and data.
- Work carried out using privately owned computer equipment when a connection is made to the Council's network.
- Use of Council equipment by any individual for personal reasons or any other use by an individual, which identifies the user as a Council employee, that may bring the Council into disrepute.

1.1.3 The policy applies, in full, to business use, formal home use, remote or mobile working and personal use of the Council's ICT resources.

1.1.4 A separate ICT Security Policy is applicable to NFDC Councillors.

1.2 Signing up to the Policy

1.2.1 Everyone using the Council's information systems and network facilities is required to complete online security training and sign a memorandum of understanding. By signing the memorandum of understanding, you are agreeing to adhere to this Policy.

1.2.2 Adherence to this Policy is a condition of using the Council's equipment and networks. Failure to do so is considered a serious offence. This could lead to disciplinary action and dismissal for employees or immediate termination of work for contractors. It could also lead to criminal or civil action if illegal material is involved or legislation is contravened.

1.2.3 Equipment is provided to staff to enable them to perform their Council duties. This equipment shall remain the property of the New Forest District Council and shall be returned when staff are no longer entitled to the equipment under the Council's policies, procedures or decisions.

1.2.4 All managers are responsible for ensuring that staff are familiar with and regularly reminded of their obligation under the policy.

1.1 History of this Policy

1.3.1 The history of this policy is detailed below.

Version	Author	Date	Comments
V1	Janet Clarke ICT Security Officer	2000	
V1.1	Janet Clarke	2004	
V2.1	Janet Clarke / Keith Kensley ICT Records Manager	January 2012	This policy supersedes the ICT Security Policy that was originally issued in 2000 and revised in 2004

1.3.2 This policy has been produced in consultation with the following Services and Groups:

- ICT Services
- HR Services
- Legal Services
- Executive Management Team
- Unison

1.3.3 This policy has been ratified by Cabinet on 7th March 2012 and has the full support of the Executive Management Team.

1.3.4 This Policy will be reviewed annually by the ICT Security Manager, or more regularly to meet legislative requirements and technology developments, to ensure its content is relevant. Updates will be communicated directly to staff and also made available on Forestnet.

SECTION 2: USE OF TECHNOLOGY

You have been provided with the appropriate IT hardware and software to enable you to do your job. It is important that you understand the various types of IT facilities available to you and that you use them in accordance with this policy.

2.1 Types of information technology

The ICT Security Policy applies to all types of information technology, including:

The Internet and Intranet (ForestNet)

Desktop applications (Word, Excel, PowerPoint, etc.)

Outlook (e-mail and calendar)

Line of business applications, e.g. Orchard (Housing), Acolaid, Anite, Northgate Tax & Benefits, etc.

Corporate systems (Agresso, ICT Service Desk, Complaints, ForestMap, ForestNet, NFDC Website,Telephone Payments, Travel Claims, Meridio EDRMS, etc.)

2.1.1 Internet

2.1.1.1 Access to the Internet is provided where you need it to carry out your work.

2.1.1.2 Your Director or Head of Service will be responsible for authorising your connection to internet services. Authorisation cannot be delegated to any officer below Head of Service level. Access will not be provided without this authorisation.

2.1.1.3 Before you can be connected to the Internet, you must complete the online ICT Security Training, details of which are available from your manager.

2.1.1.4 Your connection to the Internet will be controlled by management software. This software will provide an account of all your incoming and outgoing network connections.

2.1.1.5 Access to the Internet must only be via the Council network to ensure maximum protection. The use of a modem to make a direct connection with the Internet is not allowed, as this would bypass the necessary protection. However, you should contact your manager and the ICT Service Desk if you believe that there is an appropriate business reason to make a direct connection.

2.1.1.6 You should be aware that, as with paper sources, not all information on the Internet is accurate, complete or reliable. You should evaluate its validity, as you would a printed publication, before using it.

2.1.1.7 Personal Use

Occasional personal use of the Internet is allowed in your own time at the discretion of your manager, provided:

- It does not interfere with Council business.
- It is not related to a personal business interest.
- It is not misuse as detailed in this policy.
- Personal use of the Internet is not allowed during working hours*.

*You may have different working patterns to "normal office hours". For the purpose of this policy, "working hours" will mean "paid hours".

Your manager is responsible for controlling time spent on personal use.

If you wish to spend significant time outside working hours using the Internet (e.g. for study purposes) you should obtain specific approval from your manager.

2.1.1.8 Offensive Material

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 you know, or could have been 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.

The Internet contains volumes of useful information. It also contains some offensive material. Any individual using Council facilities for viewing or downloading such material will be in breach of this policy. If you access illegal material the Council will inform the Police and criminal prosecution may follow.

You should be aware of the risk of inadvertently accessing inappropriate sites. If you accidentally access offensive material you must inform your manager and the ICT Security Manager immediately. Accidental access will not result in disciplinary action, but failure to report it may do so.

2.1.1.9 Inappropriate sites

Many sites are made unavailable to you since they have no relevance to the business of the Council. These include:

- Gambling sites
- Auction sites
- Video sharing websites (e.g. YouTube)
- Film and music download sites
- Pornography sites

You must not attempt to access any sites of this nature on the Council's equipment.
A good test is whether, with hindsight, your actions could be justified to your manager or to a member of the public.

2.1.1.10 Social Networking sites

As part of a strategy to provide easy access to services for customers, NFDC will utilise appropriate Social Media tools to promote its activities and to engage with customers and visitors. Initially this activity will be confined to *Facebook* and *Twitter.* Given the unstructured nature of these social media tools it is necessary to provide some flexibility in the council's ICT Security framework to make the best use of these tools.

It is necessary to permit the limited sharing of passwords in order to access and update some of our *Twitter* and *Facebook* accounts. The sharing of passwords by authorised users will be limited to sharing the password between two users only for each account. For example:

Housing Needs – "New Forest Homesearch" *Facebook* account
Password shared between the primary and secondary account holder.

The use of Social Media tools by authorised users can be monitored and analysed and this limited permission to share passwords when using these tools will be regularly monitored to ensure compliance with best practice.

Access to social networking sites is strictly restricted to those individuals who require it for the purposes of their employment with the Council. Each request must have the support of the appropriate Head of Service and meet the Council's criteria set out in the Social Media Protocol (Appendix A). The Head of ICT Services will review all requests.

2.1.1.11 E – Safety – Children and Young People

In an age when electronic communication is ever more to the fore and is increasingly used by the Council, there is a responsibility to ensure that children and young people are safeguarded in the "virtual" environment. E-safety is the process of limiting risks to children and young people when using Information and Communications Technology. It relates to the use of all ICT (fixed or mobile); current and emerging.

The use of ICT is a significant benefit to our communities and the Council is encouraging its use for service delivery. It can be an attractive medium which helps children and young people engage with Council services. However, in moving in that direction we have to be aware of the potential risks. For services aimed at children and young people, the guidance of the Four Local Safeguarding Children's Boards is used. This guidance also contains useful links to training and support materials. This subject is also included in the Council's training programme.

2.1.2 E-Mail

2.1.2.1 E-mail is available to all employees with access to a PC. It is accessible from desktop PCs and available to assist in legitimate Council business. It is subject to all aspects of both this Policy and the Email Charter. The Council has developed the E-mail Charter and Corporate Standards for Communications, which you should make yourself familiar with. Both are available on ForestNet,

2.1.2.2 You should have regard to what is deemed misuse at Section 2.2 of this policy.

2.1.2.3 Personal Use

You should not use e-mail for personal use during work time. However, it is recognised that, as with telephone calls, a certain amount of private usage is acceptable. Personal usage must be agreed with your line manager, kept to a minimum, not interfere with work, should not be regarded as private and will be monitored.

You are not permitted to use the Council's internet access for connecting to any Internet e-mail sites and must only use the e-mail system provided by the Council. (An example of this could be personal email accounts at btyahoo or hotmail).

2.1.2.4 Offensive Material

If you receive an offensive or sexually explicit e-mail, you must inform your manager and the ICT Security Manager immediately. Such material may not be identifiable until an e-mail is opened and in these circumstances you will not be held responsible provided it is promptly reported.

2.1.2.5 "*Spam" and "Phishing" emails*

Spam is email that is unsolicited and unwelcome. Sometimes it is also designed to spread computer viruses.

The Council's internet service provider has an effective spam filter that intercepts most spam messages. However, you may occasionally receive obvious spam messages, in which case, preferably without opening the item, use the Junk E-mail / Add sender to Blocked Senders List option in Outlook or simply delete the email making sure your 'deleted items folder' is also cleared. If you think the spam may be harmful to the network, you must report it to the ICT Security Manager.

Phishing is an illegal way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy person or organisation. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

You will **never** receive a legitimate email asking for your security details (private or work related) and you should **never** reveal them either by email or phone. If you are asked for this information then please forward the emails to the ICT Security Manager.

2.1.3 Telephones

There is guidance on the Council's Corporate Standards when communicating via the telephone which you should make yourself familiar with.

2.1.4 Personal Digital Assistants (PDAs) and Smart phones

The Council provides PDAs and Smart phones to employees who require them to carry out their work. The appropriate Head of Service agrees the need and the Central Purchasing Unit purchase the devices. Their use is subject to all aspects of both this Policy and the Remote Working Policy (Appendix B). If you purchase your own PDA or Smartphone, ICT Services are not permitted to enable synchronisation with the Council's network.

2.1.5 Computer Equipment

2.1.5.1 You may only use the Council's computer equipment for personal use with the express permission of your manager and in your own time. This includes the creation of CVs, letters and spreadsheets and the playing of pre installed Microsoft games (no other games are permitted).

2.1.5.2 You must not use the Council's equipment 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 or registering NFDC's contact details e.g. telephone number or email address.

2.1.5.3 To ensure that electronic storage space is not compromised, you must not store personal material (e.g. personal letters, CVs, photographs, etc.) 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. The ICT Security Manager will monitor the Council's Information Systems Network and local drives of the computer equipment and address any issues directly with users.

2.1.5.4 Only Council provided equipment can be used or physically connected directly onto the Council's equipment and Information Systems Network. Under no circumstances is the use of privately owned portable media, including detachable hard-drives, CDs, memory cards and USB flash drives/memory sticks permitted, not even for festivities at Christmas, birthdays or other celebrations. Only Council owned portable media can be used in approved circumstances. You must without exception submit all removable media including disks, CDs and memory sticks to ICT Services for virus checking before you use them. Their use is subject to all aspects of both this Policy and the Remote Working Policy (Appendix B).

2.1.5.5 The loading of any software, including shareware or freeware, is restricted to ICT Services and other authorised persons only. You must not try to install executable programmes or download them from the Internet. If you get an on-screen message saying that a software update is available (e.g. to Adobe viewer) you must take no action to install it and refer it to the ICT Service Desk.

2.1.5.6 In respect of wallpapers or screensavers 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 4.6 of this policy. PC wallpapers must not be downloaded from the Internet.

2.1.5.7 If, to ensure work can continue, access to data is required while another user is on leave or unexpectedly absent, a temporary access request form – available on ForestNet - must be completed by your manager; if your manager is not available, access can be requested via the ICT Security Manager.

2.1.5.8 For areas in the view of the public, consideration must be given to the location of monitors to ensure that members of the public cannot view the screen.

2.1.5.9 To ensure security of the hardware, software and data, all moves relating to hardware and software must only be undertaken by ICT Services.

2.1.5.10 Laptops and Portable PCs

The use of laptops and Portable PCs is subject to all aspects of both this Policy and the Remote Working Policy (Appendix B) and to the following additional provisions.

2.1.6 Home working and Remote Working

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 Human Resources for advice.

Access to the Council's data and information systems network from a remote location including home is only permitted via the secure remote access system. Before individuals are issued with an authentication token for the system, they must first obtain approval from their Manager. Details of the cost (software licence, etc.) and enrolment process can be found on ForestNet.

Home and Remote Working is subject to all aspects of both this Policy and the Remote Working Policy (Appendix B).

2.1.7 The Council's Website and Intranet

The Council's web site and internal Intranet site are important parts of the communication framework.

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, subject to a compelling business case. Any such site must be approved by EMT and follow standards set by ICT Services.

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 Web Content Manager.

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

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.

There is an established review programme to ensure all information on the Website and Forestnet is reviewed on a regular basis. In addition, all information made available to the public in printed form should be published simultaneously on the web site.

All associated websites must be designed in line with the Corporate Website Standards and in liaison with the Web Content Manager.

For further information using the Intranet and the Council's website contact the Web Content Manager.

2.2 Misuse of technology

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

A good test is whether, with hindsight, your actions could be justified to your manager or to a member of the public.

2.2.1 The following comprehensive but not exhaustive list constitutes misuse of Computer and Internet Access :

- Revealing your log-in name and password to another person
- Using another person's log-in name and password
- Creation, use, transmission or encouragement of material that 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.
- Causing nuisance or distress.
- Harassment.
- Participating in instant messaging using applications like windows messenger.
- Participating in chat rooms, blogs, social networking sites etc. without your manager's permission
- Online banking facilities other than the business of the Council.
- Any online sale or purchase of goods and services for personal purposes or undertaking personal commercial activities.

- 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.
- Downloading music, films, games or any other entertainment media from the internet
- Unauthorised downloading of material including copyrighted or confidential information.
- Downloading software from the internet
- Importation or downloading of executable program files without the express permission of ICT Services.
- Hacking.
- Accessing "offensive" sites.
- Putting the Council's reputation at risk.
- Connecting to Internet e-mail sites; only the e-mail system provided by the Council must be used
- Registering with another Internet service provider.
- Using the Council equipment, network and services for any type of personal gain.
- Failing to adhere to any aspect of this policy.

2.2.2 Email

The following comprehensive but not exhaustive list constitutes misuse of e-mail:

- Excessive personal use
- Illegal activities.
- Undertaking personal commercial activities.
- Causing nuisance or distress.
- Harassment.
- Creation and transmission of "offensive" material (definition of "offensive" in section 2.1.2)
- Sending Data Classified as RESTRICTED or above via the @nfdc.gov.uk email system using Microsoft Outlook
- Sending contentious or libellous electronic communication.
- Sending threatening, defamatory, offensive material, including jokes, on the Internal and External e-mail system.
- Registering with e-mail providers.

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).

Should an email be received that falls into the category of misuse, the user should advise their Manager and only retain the material if the user or the manager wish to take further action on the issue. Otherwise, the e-mail must be deleted immediately.

2.2.3 Computer games

Standard Microsoft computer games, for example Solitaire, can be played in users' own time (at the discretion of their line manager). If games are allowed, they must never be used in areas that may be viewed or are accessible to the public.

Any other games used on the Council's equipment are regarded as misuse.

2.2.4 Action on misuse

Misuse will be investigated and acted upon in accordance with this policy and the Councils disciplinary procedures.

All managers are responsible for regularly reminding staff of their obligations under this Policy. Section 8 of this Policy deals with how to report a security breach and how it would be investigated.

SECTION 3: MONITORING THE USE OF TECHNOLOGY

3.1 Why is monitoring taking place?

3.1.1 The Council has the ability to monitor electronic data and communications. The reasons for monitoring communications is to:

- Ensure standards of behaviour from employees and others working for the Council meet the requirements laid out in this, contracts of employment and other policies.
- Help avoid criminal activity.
- Help identify criminal activity.
- Safeguard the Council's network and providing protection for the organisation and its employees.

3.2 What will be monitored?

Users should not expect activities detailed in this section to be considered private.

3.2.1 The following activities will be monitored:

- Internet
- E-mail

- Software on PC
- PCs
- Network storage areas
- Office telephones
- Mobile phones
- Approved Social Networking activity

3.3 How will it be monitored?

3.3.1 Internet

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 Manager will be able to determine Internet usage, including details of which sites have been accessed, the number of visits, services used and time spent at each site by individual users.

This monitoring software automatically blocks access to specific categories of websites, for example gambling and pornography.

The blocking software is not infallible. If you are unable to access a web site that you believe is legitimate for work purposes, you should contact the ICT Service Desk.

The ICT Security Manager will produce reports for Heads of Service on Internet usage in their service. These reports detail the number of recorded browsing hours, where there are concerns about the number of hours browsing by an individual, their Head of Service will make a formal request to the Audit Manager for further investigation.

Investigations whether at the request of Management or where a breach/misuse has been reported will include detailed analysis of the sites that have been accessed, the number of visits, services used and time spent at each site by the individual under investigation.

3.3.2 E-Mail

The Council has an e-mail management system, which can report on in and out bound traffic to the mail servers. These reports detail information such as: Sent to/ Received from/Subject /Attachment type/Date and Time.

The management system automatically filters e-mails for inappropriate or “offensive” material such as offensive language and viruses.

All emails sent and received via the Council’s network are the property of the Council and should not be perceived as private. Although not regular practice, emails may be reviewed as part of an internal investigation. In such cases steps are taken to only review relevant communications, but it cannot be guaranteed that private emails will not be read.

3.3.3 Software on PC

All software being run on Council owned PCs must be authorised by ICT Services and properly licensed. To ensure the Council meets the legal requirements of any licence, continuous monitoring of software being run on PCs will be undertaken. The computer normally undertakes this monitoring automatically, but ICT Services regularly review the data.

3.3.4 Office Phones

Managers are responsible for monitoring levels of usage on a day to day basis.

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, e.g. 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.

3.3.5 Mobile Phones

Detailed mobile phone statements are received from the network supplier for each mobile phone and will be checked by your Manager and periodically by Internal Audit. Any misuse will be fully investigated and may result in disciplinary action being taken, which could result in dismissal.

3.4 Legal Considerations

All monitoring is carried out in line with the relevant legislation, which primarily includes the Data Protection Act 1998 and Lawful Business Practices Regulations 2000.

SECTION 4: SECURITY OF DATA

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.

The Act also provides individuals with a right to access information held about themselves. To ensure compliance with Act the Council has a formal set of procedures for the dealing with these types of requests. All employees must adhere both to these procedures and the eight data protection principles. More information including the Council's Data Protection Policy and the eight principles of the Data Protection Act can be found on Forestnet.

You should bear in mind that in your day to day work, much of the information you deal with will contain personal data. You should be aware of your personal responsibilities in dealing with personal information, and the fact that you could commit a criminal offence if you don't deal with personal information in accordance with the Act. In particular, the Data Protection Act restricts what personal information

you can disclose to colleagues, third parties and members of the public. If in doubt, you should contact the Data Protection Officer in Legal and Democratic Services.

Display screen equipment must not be located in such a position that screen displays are visible to unauthorised users or members of the public.

Before committing personal data to newsgroups, social networking sites or any other web-sites, you must ensure the Data Protection Principles are adhered to.

4.2 Types of Data

4.2.1 Personal data

Personal data is information about a living person, which by itself or with other information held by the Council would enable them to be identified (not necessarily by name). The information may relate to the person's personal life, business or profession and include information about their activities. For example:

- Name, address, age, marital and employment status, their photo and signature.
- Personal finances.
- Personal contact details.

4.2.2 Sensitive personal data

Sensitive personal data is a type of personal data that can only be held or used if stringent requirements are met, and access is strictly controlled. For example:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences/record

4.2.3 Business sensitive data

Business sensitive data is a type of data or information that is not in the public domain and could be damaging to the authority, a company, business or individual. For example:

- Building plans
- Security details
- Contact information
- Minutes of some meetings

4.3 Data Classification

The Government has a Protective Marking System comprising five markings. In descending order of sensitivity they are:

- Top Secret
- Secret
- Confidential
- Restricted
- Protect

Local Authorities are encouraged to follow the Protective Marking System.

The criteria for marking data are detailed in Appendix C.

The Council network is cleared up to the level of RESTRICTED. Data Classified by Government as RESTRICTED or above must not be saved to mobile devices or removable media under any circumstances. Only approved NFDC equipment will be enabled to access and transmit (which includes emailing) data classified at these levels via the Government Secure Intranet (GSI). Details can be found in section 12 of this document.

4.4 System access

4.4.1 Giving access to Council systems

Everyone using the Council's data, information systems and network facilities is required to complete online ICT Security Training and sign the memorandum of understanding.

Line Managers should advise ICT Service Desk of the need for access for an employee at least 5 working days prior to the access being needed by completing a new starter or access request form, both of which can be found on ForestNet.

All ICT users will be set up with an individual User ID and password. They identify users on system logs and audit trails which are reviewed by system administrators on a regular basis and will be used by the ICT Security Manager in the event of a breach or suspected breach of security. Group working will be permitted utilising shared drives and systems areas. However, access to such group work areas will only be granted via (personal) User ID and password to provide an adequate audit trail of activity on an individual user basis.

Access to the Council's computer systems is authorised by managers and is set to the requirements of the job. Some employees are given appropriate access levels to allow them to carry out specific tasks. **It is very important that users do not share passwords or log on details – this would constitute computer misuse by both parties.**

System administrators are employees responsible for the management of a computer system. It is their role to ensure that access is given only to those that need it and at the correct level. Periodic reviews of access to systems must be undertaken by the systems administrator to ensure only current employees and authorised people have access.

4.4.2 Removing access from Council systems

To request removal of access for individuals, line Managers should advise the ICT Service Desk by completing an ICT leaver's form (e-form) which can be found on ForestNet. This is required when a person leaves the Council's employment or there is a change of duties.

Before an employee leaves the Council, managers should ensure data stored on their network drive is transferred to an area colleagues can access, where appropriate. When the person has left, their network account will be suspended. Data will be held for a further month, but access will only be available through ICT Services. After the month data will be deleted from the network and therefore irretrievable.

4.4.3 Logging off

Computers should not be left unattended when you are logged on. If you need to leave your computer or laptop for any length of time you should ensure that current data is saved and access is prohibited, by logging out of all major applications and using the "lock workstation" option that Microsoft Windows offers. Before leaving your desk for the day, you must ensure that your PC and monitor have been turned off.

4.5 Passwords

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

Passwords are a means of preventing access to systems or parts of systems by unauthorised users. The password should be made up from a minimum of 7 characters and numerals as a combination, for example Summer01. It should not have repeated characters and should not be a name or any string that can be easily identified with the user, e.g. surname, other family names, car registration, telephone numbers, etc.

Passwords are case-sensitive

4.5.2 You will be required to change your network log-in password every 90 days.

4.5.3 Do not keep a manual record of individual User IDs and passwords.

4.5.4 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.

4.5.5 Using another person's password is misuse under this policy.

4.5.6 Should you forget your User ID or password or believe that another user knows your User ID and password you should contact the ICT Service Desk immediately.

4.6 Viruses

4.6.1 A computer virus is a computer program specifically designed to spread itself from one computer to others and, in some cases cause annoyance and damage.

4.6.2 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 anti-virus software up-to-date with the latest virus signatures.
- You must without exception submit all removable media including disks, CDs and memory sticks to ICT Services for virus checking before you use them.
- You must not irresponsibly introduce a computer virus into Council computers.
- Anyone recklessly transmitting a virus to or from Council computers will be in breach of this policy.
- Any dangerous file types such as executables and scripts must be validated and virus checked before being loaded onto the Council' computers or network.
- If you suspect that your computer has been infected by a virus, you must call the ICT Service Desk immediately.

Please contact the ICT Service Desk (ext 5300) for advice on the above.

4.7 Portable equipment and removable media

4.7.1 **Portable equipment** includes any piece of electronic equipment that is removed from the Council Offices, such as:

- Personal Digital Assistants (PDAs)
- Laptops
- Netbooks
- Tablets

Removable media includes:

- approved USB memory sticks
- card readers
- cameras
- mobile phone memory storage devices
- CDs
- DVDs.

4.7.2 Data should only be placed on Portable equipment or removable media in exceptional (and approved) circumstances and **must** be protected by encryption (contact ICT Security for further advice)

4.7.3 Storing data on mobile devices (rather than the network) is actively discouraged. Only where the local drives have been encrypted should data be saved locally (Guidance on how to do this is on ForestNet).You should not transfer significant quantities of data simply for convenience; it must be kept to what is necessary for the business requirement and the data should be securely deleted as soon as it is no longer required.

4.7.4 You are responsible for the security of the equipment and the data it contains, while you have taken it away from the offices. Practical steps should be taken, e.g. basic home security, and you must never leave equipment unattended, for example in cars.

4.7.5 If a piece of equipment does go missing, report it immediately to your Head of Service, ICT Services and the Performance Improvement Manager (for insurance purposes).

4.8 Data transfer

4.8.1 Any manual or electronic data being transferred outside of the authority, which could be covered by the Data Protection Act, information that is RESTRICTED (See 4.3 and Appendix C) or could be damaging to the authority if it was misplaced, lost or stolen must be protected.

4.8.2 Electronic data being transferred must be encrypted to recognised industry standards. Where encryption is not possible, you must seek advice from the ICT Security Manager before any data is transferred.

4.8.3 For manual transfer of data a transfer log must be created by ICT Security before despatch and the package sent by recorded/tracked means with a recognised carrier. The package must be signed for at despatch and on receipt to form part of the Audit Trail.

4.8.4 Data that has been classified as RESTRICTED or above can only be transferred electronically via the Government Secure Intranet (GSI). Details on connecting to the GSI can be found in section 12 of this document. Relevant staff will receive GSI training.

4.8.5 Transferring or sending data to private email accounts to undertake work at home is prohibited.

4.8.6 It is the sender's responsibility to ensure that any transferred data, electronic or manual, is secure.

4.9 Data sharing

4.9.1 The term "data sharing" refers to the sharing of personal and sensitive data held by an organisation internally and externally with other organisations.

4.9.2 Where Data is shared this must be done fairly and lawfully in accordance with the Data Protection Act. It is your responsibility to ensure that any data sharing is in accordance with the Data Protection Act. Before sharing data with another service within the Council, or with any external organisation (including the police) you must seek advice from the Data Protection Officer.

4.9.3 Employees using the Government Secure Intranet are required to read and sign up to an additional set of guidelines which complement this Policy. This additional security introduces stringent controls on the particularly sensitive data used in this area. The scheme is managed by the Head of **Customer and Financial Support Services** and the Benefits Manager.

SECTION 5: PHYSICAL SECURITY

In the Council Offices

5.1.1 Personal data in paper format must be locked away when unattended, and only authorised people have access to it.

5.1.2 Portable ICT equipment must also be held securely while in the office.

5.1.3 To ensure that the physical security is not compromised, access to the Council offices is via an electronic door entry system, activated by staff identity cards. Access must only be given to authorised individuals. Approved contractors will be given an access card for the duration of their visit. Visitors must sign in and will be issued with a temporary visitor card detailing emergency information. There will be no access facility with this card and all visitors will be collected from Reception by the meeting organiser. Each Head of Service will be issued with a small number of access cards to be issued at their discretion on a temporary basis for unusual/ad hoc requirements. These must be kept securely. It is the Head of Service's responsibility to ensure these are controlled appropriately. To activate the card, the Head of Service must contact the ICT Security Manager.

5.1.4 Security doors should not be propped open and any unknown people within the secure area of the Council Offices must be approached to confirm they are legitimate visitors.

Outside of the Council Offices

5.1.5 To carry out Council business you may be required to take personal data out of the Council Offices either in paper format or on a portable device. When doing this you must:

- Only take the information needed
- Not leave it unattended
- Not leave it on view in a locked car
- Ensure that, if you are reading it in a public place, nobody can read it over your shoulder

5.1.6 Particular care should be given if passing personal data out of the building. This includes data in a range of formats, but includes paper, e-mail, phone and USB sticks. Each case should be considered individually as it is a form of data sharing. Questions to ask before you send out data include:

- Are there good business reasons for sending out the data?
- How sensitive is the data being sent?
- What volume of data is being sent?
- How can I be sure the correct recipient receives the data sent?
- If lost what impact would that have for the individuals affected and the Council as an organisation?
- What options are there to ensure the security of data in transit?
- Are there any other alternative more secure options to passing on the data?

SECTION 6: BACKING UP OF DATA

6.1 Backing up of all computer data ensures that it can be retrieved should the network or server fail. ICT Services undertake comprehensive backing up procedures of all the Council's systems.

6.2 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. Only the work/data on the server will be backed up automatically.

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

SECTION 7: RETENTION AND DISPOSAL OF DATA

How long should I keep data?

7.1 Most records should be retained for various time periods. Some will be subject to statutory retention periods, others will be subject to "common practice".

7.2 Guidance can be found for records retention on the Council's website under Information Management or advice can be sought from your manager or the Council's Records Manager.

How should I dispose of paper files and documents?

7.3 Any hardcopy information containing personal details must be disposed of securely. For disposal options contact the Procurement Manager.

All I.T. equipment that has been used for work must be returned to ICT Services for disposal. An image of all files saved to the equipment can still be retrieved even if users believe they have deleted the information and if not removed could allow sensitive data to be accessed by unauthorised people.

SECTION 8: DEALING WITH SECURITY BREACHES (INCIDENTS)

8.1 What is a security incident?

8.1.1 A security incident is:

- an event that has resulted, or could have resulted in the loss of or damage, to the Council's information.
- an action that is in breach of the Council's ICT Security policies and procedures.

8.1.2 Security incidents can happen for a number of reasons:

- Misuse of technology.
- Loss, misplaced or theft of data or equipment on which data is stored.
- Unauthorised access to data.
- Equipment failure, weakness or malfunction.
- Human error or negligence.
- Hacking.
- "Blagging" where information is obtained by deceit.
- Unforeseen circumstances such as fire or flood.

The scope includes potential loss, damage or disclosure to manual records as well as electronic ones.

8.2 Reporting a security incident

8.2.1 All incidents (large or small), or suspected incidents, are taken seriously and should be reported immediately to Managers or the ICT Security Manager, who may discuss or escalate these breaches to the Head of ICT Services for further investigation.

8.3 Investigations

Investigations will be undertaken at the direction of the Head of ICT Services and will be conducted in line with the severity of the breach.

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

All other investigations will be conducted in accordance with the Council's disciplinary rules. This could lead to dismissal for employees or immediate termination of work for contractors.

8.3.1 In some cases access by the investigators to email, network drives, PCs and system logs may be required. A clear process for this has been set out and is attached as Appendix D. It ensures that all employees are treated fairly and in line with relevant legislation.

SECTION 9: PURCHASING AND INSTALLING TECHNOLOGY

9.1 Purchase and installation

9.1.1 All ICT equipment and software must be purchased through ICT Services in accordance with the Council's ICT Asset Management Policy and the Financial Regulations. The reasons for this are that ICT Services will:

- help to identify the best solution for the job.
- ensure all hardware and software is compatible.
- Add / remove equipment to / from the hardware maintenance schedule.
- ensure adequate storage space and optimum configuration of any software
- register equipment and software on the ICT inventory and schedule for replacement

9.2 Software licensing

9.2.1 All software operated on the Council's network and equipment must be correctly licensed to meet legislative requirements.

9.2.2 As noted in section 3, the use of software on the network is continuously monitored. If unlicensed software is identified on any PC, the user will be given 5 working days to either produce a valid licence or ICT Services will remove the software.

9.3 Registering Council equipment (assets)

All equipment purchased through ICT Services is allocated an asset tag and recorded electronically. This allows support to be given without users having to supply hardware and configuration details and allows all items to be tracked throughout their life-cycle.

SECTION 10: TRAINING AND SUPPORT

10.1 New starter induction

ICT users will be made aware of ICT Policies as part of their induction package and will be required to complete the on-line training (see 4.4.1). Managers will be responsible for ensuring that employees are trained on ICT systems applicable to their job role and service.

10.2 ICT Service Desk

The ICT Service Desk is the first port of call for all ICT queries and support. Contact them on extension 5300.

SECTION 11: OTHER RELATED LEGISLATION AND GUIDANCE

11.1 Related legislation and guidance include:

- Lawful Business Practices Regulations 2000
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Criminal Justice and Immigration Act 2008
- Freedom of Information Act 2000
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Data Handling Procedures in Government June 2008
- Communications Act 2003

11.2 Other related Council Policies and Procedures

Related policies and procedures include:

- ICT Security Policy for Councillors
- Disciplinary Procedure
- ICT Strategy
- Members Code of Conduct
- Employee Code of Conduct
- Remote Working Policy
- Government Connect Code of Conduct
- Corporate Risk Management
- ICT Asset Management Policy
- Financial Regulations
- Communications Corporate Standards
- Email Charter
- Whistleblowing Policy
- Road Safety Procedures

SECTION 12: GOVERNMENT SECURE INTRANET

The Government has established a project to develop a secure ICT infrastructure for shared services. The idea is to have a fully secure system known as the GSI (Government Secure Intranet) that will enable central and local government to share RESTRICTED electronic data safely.

NFDC is connected to the GSI and compliant to the Code of Connection (COCO) which outlines the minimum set of security standards that organisations must adhere to when joining the GSI.

Systems that are Live on the GSI	
System	***NFDC***
DWP Customer Information System	*Council Tax and Benefits Teams*
GSI Secure email system	*Council Tax and Benefits Teams*
Her Majesty's Court Services	*Electoral Services*

If access is required to a system that is available on the GSI, the user will need to complete the application form which can be found on Forestnet under ICT Security / Government Connect.

SECTION 13: ROLES AND RESPONSIBILITES

13.1 The main contacts and their responsibilities relating to the management of this policy are**:**

Person / Group	**Responsibilities**
Council	To agree the policies
EMT	To endorse and fully support the application of the policy across the authority.
Head of ICT	To manage the Council's ICT environment.
	To ensure that ICT Services maintains a Disaster Recovery Plan.
	To ensure ICT employees only install software for which a valid licence is held.
	To ensure that all suspected breaches are investigated.
	To ensure that appropriate "housekeeping" of systems, including the regular backing up of data, is undertaken.
Head of Legal & Democratic Services	To advise on associated legislation as required.
	To manage Data Protection and Freedom of Information
	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.
ICT Security Manager	To monitor employees' use of systems and recommend disciplinary action when required.
	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 provide information to the Head of ICT Services 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.
ICT Security Manager (contd)	To co-ordinate the ICT Disaster Recovery Plan in relation to technology based services across the Council's sites and verify its adequacy.
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 Service Desk promptly about employees joining and 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 suspected computer misuse to the Head of ICT Services.
	To control time spent by employees on personal use of email and the internet.
	To create relevant business continuity plans prioritised across the business unit.
	To ensure that all employees receive training on computer systems applicable to their job role and service.
Systems Administrators	To ensure that access at the correct level is given to systems for those who need it
	To undertake periodic reviews of access to systems to ensure only current employees and authorised people have access.
Records Manager	To advise on good Information Management practice and records retention periods.

Employees	To comply with the Policy, Standards and Legislation.
	To report any breaches of ICT Security to managers or to the ICT Security Manager
Employees (contd)	To ensure that any software to be installed is registered with ICT Service Desk for installation by ICT employees.

Social Media Protocol

This protocol is for the use of New Forest District Council employees, and aims to help them make responsible decisions and get the most out of social media tools i.e. Facebook and Twitter.

'Social media' is the term commonly given to websites and online tools allowing users to interact with each other in some way – by sharing information, opinions, knowledge and interests.

The use of social media presents new and interesting opportunities for the council to reach out to its residents and service users.

Alongside these opportunities it must be recognised that there are risks attached to the use of social media. Distribution of material cannot be controlled. Once posted to an initial target audience, material can be posted anywhere through the networks of each individual in that audience and beyond. It is therefore important that users of social media understand the pitfalls as well as the benefits of the technology.

These guidelines have been introduced to ensure appropriate legal and effective use of social media as a communication channel for New Forest District Council. It will interact with other council guidance in this area of work, including the ICT Strategy 2009 - 2013, the ICT Internet Security Policy and Email Charter.

Content

Objective

The objective of this protocol is to protect the reputation of the council by providing a framework for the effective and safe use of social media to promote and develop the council's vision, services and achievements.

Scope

This protocol on how to use social media applies to all council employees.

Further information regarding conduct and Internet usage can be found in the Council's ICT Security Policy for Employees.

Failure to comply with this protocol may result in disciplinary action.

Exceptions

If the nature of your project requires you to operate outside the protocol, you must not do so without requesting an exception.

Exceptions can only be granted by the Executive Management Team (EMT).

Definitions

In the following protocol, the term "**profile**" refers to an account, page or website representing the council, one of its services or an officer.

Protocol

Creation

1. New profiles should only be created following agreement by the Head of Information and Communication Technology (ICT) Services.
2. Before creating a new profile, check whether one already exists serving the same audience. It may be more appropriate for the council to join an existing group than create a rival group.
3. New profiles will only be agreed if a clear business need can be proven, and sufficient resources by the relevant services are made available to maintain it, and respond to feedback generated by the service or project lead.
4. ICT Services (via the Service Desk, where they can be logged) will set up all new profiles.
5. The profile will be the responsibility of the service area in terms of content management and must be updated on a regular basis to ensure content is fresh and relevant.
6. A single, named person in the service area requesting the site must be responsible for maintaining the profile. Other approved employees may also be nominated to assist them.
7. Any such approved employees must also comply with this protocol.

Operation

1. Know and follow New Forest District Council's Codes of Conduct for Employees in Section 6a of the Employee Handbook **-** Gifts and Hospitality; Financial and Personal Interests; Local code for Member/Officer Relations and the ICT Security Policy for Employees.
2. When using third-party websites (such as Facebook), know and follow their terms of use.
3. No content should be published unless already added in some way to the council's corporate website – www.newforest.gov.uk. Do not publish any information which is not already in the public arena.
4. Assess any risks and make sure you have plans in place to manage and mitigate them – refer to Risk management guidelines.
5. You must clearly identify yourself and your role within the Council. Make it clear that you are acting in a professional capacity. Your comments will affect the way the Council is perceived and therefore brings responsibilities.
6. Make sure that social media is the appropriate way to engage with customers for the particular purpose you are intending to use it for. Respect your audience; be aware of any language, cultural or other sensitivities you may need to take account of. You should be particularly mindful of any interaction with children and/or vulnerable people and observe the Council's policy on Safeguarding Children, Young People and Vulnerable Adults
7. Do not publish anything that would not be acceptable in the workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory, such as politics and religion.
8. Be accurate, fair, thorough and transparent.
9. Be mindful that what you publish may be public for a long time
10. Respect copyright laws if linking to other online material, including images.
11. Always stay within the legal framework and be aware of Data Protection regulations.
12. Do not publish or report on conversations that are meant to be private or internal to New Forest District Council without permission. Do not cite or reference customers, partners or suppliers without their approval. When you do make a reference, link back to the source where possible.
13. Write in the first person ("I" or "we").
14. Wherever possible, disclose your position as a representative of your service, business unit or team.
15. Remember that you are an ambassador for the council and be cordial at all times

16. Think not only about whom you are engaging with but how you wish to engage. Having a purpose in mind, allows you to maximise the efficiency of the contact / communication. Turn around conversations wherever possible pointing customers to web content and / or appropriate online service to complete a transaction.
17. Encourage constructive criticism and deliberation.
18. Do not correct contributors' spelling or grammar.
19. Edit other people's contributions only when necessary. Instead of editing or removing significant factual errors, you should either make a public response or directly contact the person who made the original comment, or both.
20. If a contributor makes a comment that is defamatory or likely to cause extreme offense, edit or remove it where possible. If this is not possible, report it to the operator of the website. Contact the user to explain why you took this action, and if appropriate ask them to post the comment again without the offensive content.
21. All feedback to the council through social networking sites should be monitored by the responsible service. Feedback that requires a response must be acknowledged within one working day. Where action is required, bear in mind that excessive delay will have a negative impact on the council's reputation.

Review

1. The ICT Security Officer will monitor social networking in line with ICT Security Policy.

2. The Web/Intranet Content Manager will carry out periodic reviews of the Council's Social Networking sites. This will include reviewing content and feedback.

Closure

1. Profiles must not be deactivated without prior approval from the Head of Information and Communication Technology (ICT) Services.

About this document

This protocol was approved by the Executive Management Team (EMT) on 22 November 2011. It was written by the Intranet/Web Content Manager (Web Team) on behalf of the Social Media Project Team.

Related information / websites

Social Media Management Advice Note
Blogging Quick Guide (Standards for England website)

DECLARATION
Terms and Conditions for access to social networking on behalf of New Forest District Council.

I confirm that:

I have read and understood the NFDC Social Media Protocol.

I have received training and have had the opportunity to ask any questions regarding the Protocol that I felt were unclear.

I agree to abide by the Protocol.

NAME: ……

SERVICE: ……

DATE: ……

SIGNED: ……

A copy of this agreement will be held on your personnel file.

Monique Conley
Intranet/Web Content Manager
ICT Services
January 2012

New Forest District Council

Remote Working Policy

Ver	Date	Team / Author	Overview of Changes
1.0	July 2011	Janet Clarke	
1.1	January 2012	Kim Grey / Keith Kensley	Amendments to original draft

CONTENTS

Introduction

Remote working enables individuals to work from any appropriate environment. It can be thought of as working anywhere other than the traditional office. This may include remote access to data and the Council's information systems. For the avoidance of doubt remote working will include:

- Home working;
- Working when "on the move" (e.g. on the train);
- Working at rest, including in hotels and coffee shops;
- Working in the office but using remote access technologies;
- Working from the premises of customers, delivery partners, contractors, or any other organisations.

The Council's secure remote access system allows controlled access to the Council's data and information systems.

Document Purpose

This document provides the detailed policy statements for working remotely and accessing NFDC data and information systems. It supports the Council's ICT Security policy.

Policy Overview

Information & Communications Technology (ICT) systems must be used responsibly and legally. Maintaining the confidentiality, integrity and availability of data and information systems is critical to the effective operation of the Council. 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.

Adherence to both this Policy and the ICT Security Policy is a condition for using the Council's data and information systems remotely. Use may be monitored and any breach of this policy (actual or suspected) will be reported to and investigated by ICT Security. The ICT Security Manager, in consultation with management, may recommend 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.

This policy details how remote working, the Council's secure remote access system and mobile devices should be used which includes the following:

- Working with manual records and files;
- Working with removable media, to include approved USB memory sticks, card readers, cameras and mobile phone memory storage devices;
- Working with a Personal Digital Assistant (PDA) or Smartphone;

- Accessing the Council's data and information systems network remotely using personally-owned equipment;

- Accessing the Council's data and information systems network remotely using Council owned equipment;

Before being enabled for remote working individuals will receive training on and be required to sign up to this policy.

Policy Applicability

This policy applies to:

- Individuals using Council equipment, data and information systems network remotely from whatever location, including home.

- Individuals accessing the Council's data and information systems network remotely using personally-owned equipment from whatever location, including home.

- Other individuals working for the Council, agency personnel or contractors, sub-contractors, third parties with remote access to NFDC information and information systems and services whilst engaged on Council business or using Council equipment and/or networks.

- Any other remote use by Council employees, which identifies the individuals as an employee, working on behalf of the Council or which could bring the Council into disrepute.

4 Policy details

The confidentiality and security of personal, sensitive or classified data is paramount. This applies to data whether held in either electronic or manual form. Individuals should take regard to the appropriateness of working with this type of information remotely. All reasonable precautions must be taken to safeguard both data and equipment.

When working remotely, individuals are subject to the same rules governing the use of personal, sensitive or classified data as if they were working from the Council offices. Individuals must be aware of the personal responsibilities, including criminal liability that this brings together with a full understanding of the Council's ICT Security Policy. **Sensitive information and data** includes both personal data and business sensitive data (i.e. building plans or information that is not in the public domain and could be damaging to the authority or an individual)

Storing data on mobile devices (rather than the network) is discouraged. Normally when working remotely data should be accessed via our approved remote connection (contact ICT Service Desk for details).

Exceptionally data may be saved using the 'briefcase' method onto a local drive that has been encrypted (contact ICT Service Desk for details). Individuals should not transfer significant quantities of data simply for convenience it must be kept to what is necessary for the business requirement and the data should be securely deleted as soon as it is no longer required.

Data that has been classified as RESTRICTED or above must not be saved to mobile devices or removable media under any circumstances. Only approved NFDC equipment will be enabled to access data classified at these levels.

Individuals need to consider the security of the surroundings they are working in. Care should be taken when working in public places to avoid the risk of being overlooked by unauthorised persons.

Access to the Council's data and information systems either electronic or manual by unauthorised individuals, third parties, family members or visitors etc. is not be permitted.

Council owned equipment (PCs, Laptops or PDAs) must not be connected directly into an untrusted network i.e. only on the Council's network.

4.1 Working with data in manual form

When travelling, manual records and files should not be left unattended and when not in use should be secured out of sight.

Waste produced as a result of your work, must not be disposed of in normal domestic waste. It should be brought into the Council offices for secure disposal.

4.2 Working with removable media, which includes approved USB memory sticks, card readers, cameras and mobile phone memory storage devices and CDs:

Data should only be placed on removable media in exceptional (and approved) circumstances and **must** be protected by Encryption.

Data that is sensitive or classified should not be loaded on removable media. Secure file transfer or remote access arrangements will be made available in these circumstances.

Only official NFDC USB devices will be able to be used on the Council's equipment and network. Non NFDC USB devices are blocked. If the use of a memory stick or similar device is required then the device will be issued under a controlled process co-ordinated by the ICT Service Desk. The individual requesting to work on portable data, the device type, duration of the loan and type of data will be recorded and the user will be required to sign a request register.

It is recognised that information may be received by third party on removable media, Individuals must without exception submit all removable media including disks, CDs and memory sticks to ICT Services for virus checking before using them on the Council's equipment and network.

If the user frequently requires access to sensitive data away from the office the individual will be encouraged to enrol for secure remote access. This will attract a cost and a manager would need to approve this type of access. In cases of regular requests for the loan of portable media from the same user or business unit, the Service Desk will contact the manager to review the need for a more permanent solution.

4.3 Working with a Personal Digital Assistant (PDA) or Smartphone

Only Council provided PDAs or Smart phones can be enabled to connect to the Council's data and information systems. All devices will be setup with a password. This password must be kept secure and is not to be divulged to anyone else.

The security of the mobile device and the data held is the individual's responsibility and all reasonable precautions must be taken to safeguard both data and equipment.

You Must:

- Activate a password when the device is idle to ensure that access to it is prohibited;
- Ensure that the mobile devices are put securely out of sight when not in use;
- Be aware of the security of your surroundings when using the device

You Must Not

- Leave the mobile device unattended;
- Make any changes to the setup of the device;

Provided that you have taken all reasonable care to prevent such loss or damage, the business units will bear the costs of loss or damage to equipment.

If the equipment is lost or stolen it must be reported to the ICT Service Desk as soon as possible, at which point the device will be reset and all data will be erased, rendering it unusable.

4.4 Remote Access

Access to the Council's secure remote access systems, which enables individuals to remotely access data and information systems, is via an enrolment process. This does attract costs and a manager would need to approve this type of access. Details on the enrolment process and cost can be found on ForestNet under IT then Homeworking.

The system operates with two factor authentication, which is made up of a user name and password together with a pin and a number generated by a token.

The PIN for two factor authentication or the token must not be shared, written down or left with the device. Unless by prior agreement for support purposes, if needed for support the PIN will be reset afterwards.

Any two factor authentication token supplied remains the property of NFDC and must be returned upon request.

Individuals should be aware that remote printing is not currently supported.

Systems containing sensitive or classified data must not be used in, or accessed from, public places (e.g. airports, trains, internet cafés).

Remote access sessions are terminated after 120 minutes (2 hours) of inactivity. The maximum remote access session is 450 minutes (7 hours 30 minutes). Session details will be logged. These logs will be reviewed as part of the system management and support process and as part of an investigation.

4.5 Accessing the Council's data and information systems network remotely using personally-owned equipment

Remote access using this type of equipment will only be provided via the Council's secure remote access system and will be restricted to the following systems:

- Web mail (which is a limited version of the Council's email system) enabling access to email and calendar.

- ForestNet, which enables access to Agresso Web Services, and Envoy Travel System.

Individuals must not leave personally-owned equipment unattended while logged on to the remote access system. 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 using a screen saver with a password or using the "lock workstation" option that Microsoft Windows offers.

Access to the Council's data and information systems by unauthorised individuals, third parties, family members or visitors etc must not be permitted. Care should be taken when working in public places to avoid the risk of being overlooked by unauthorised persons.

Sensitive or classified data should not be printed. However where printing is unavoidable printed matter should be brought into the Council offices for secure disposal.

ICT Services must be consulted before individuals dispose of personally-owned equipment that has been used to undertake Council business.

4.6 Accessing the Council's data and information systems network remotely using Council owned equipment (PCs, Laptops or PDAs).

Remote access using this type of equipment will only be provided via the Council's secure remote access system and will be restricted to the following systems:

- Outlook, enabling full access to email and calendar;
- ForestNet, which enables access to Agresso Web Services, and Envoy Travel System;
- Applications that have a Web or Citrix based client which have been approved for remote working by ICT Services;
- The ability to retrieve, create, amend and save documents to a network drive;
- Internet access for browsing.

Sensitive or classified data should not be printed. However where printing is unavoidable printed matter should be brought into the Council offices for secure disposal.

Access to the Council's equipment, data and information systems by unauthorised individuals, third parties, family members or visitors etc must not be permitted. Care should be taken when working in public places to avoid the risk of being overlooked by unauthorised persons.

Individuals must not leave equipment unattended whilst logged in. 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 using a screen saver with a password or using the "lock workstation" option that Microsoft Windows offers.

When travelling with a laptop or when they are not in use, users must ensure that it is secured and where possible 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.

If the equipment is lost or stolen it must be reported to ICT Service Desk on 023 8028 5300 as soon as possible.

4.7 Dealing with a breach of this policy

Misuse will be investigated and acted upon in accordance with the ICT Security policy and the Council's disciplinary procedures.

Section 8 of the ICT Security Policy deals with how to report a security breach and how it would be investigated.

Criteria for Protective Markings

The Government protective marking system is designed to help individuals determine, and indicate to others, the level of protection required to help prevent the compromise of valuable or sensitive assets. The markings are a means of signalling quickly and unambiguously, the value of an asset and hence the level of protection needed.

The underlying principle is that the consequences of compromise are clearly indicated by the protective marking applied to documentary assets held on paper or electronically.

The criteria below provides a broad indication of the type of material at each level of protective marking.

Criteria for assessing TOP SECRET assets:

- threaten directly the internal stability of the United Kingdom or friendly countries;
- lead directly to widespread loss of life;
- cause exceptionally grave damage to the effectiveness or security of United Kingdom or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations;
- cause exceptionally grave damage to relations with friendly governments;
- cause severe long-term damage to the United Kingdom economy.

Criteria for assessing SECRET assets:

- raise international tension;
- to damage seriously relations with friendly governments;
- threaten life directly, or seriously prejudice public order, or individual security or liberty;
- cause serious damage to the operational effectiveness or security of United Kingdom or allied forces to the continuing effectiveness of highly valuable security or intelligence operations;
- cause substantial material damage to national finances or economic and commercial interests.

Criteria for assessing CONFIDENTIAL assets:

- materially damage diplomatic relations (i.e. cause formal protest or other sanction);
- prejudice individual security or liberty;
- cause damage to the operational effectiveness or security of United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations;
- work substantially against national finances or economic and commercial interests;
- substantially to undermine the financial viability of major organisations;
- impede the investigation or facilitate the commission of serious crime;
- impede seriously the development or operation of major government policies;

- shut down or otherwise substantially disrupt significant national operations.

Criteria for assessing RESTRICTED assets:

- affect diplomatic relations adversely;
- cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness or security of United Kingdom or allied forces;
- cause financial loss or loss of earning potential, or to facilitate improper gain or advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- impeded the effective development or operation of government policies;
- to breach statutory restrictions on disclosure of information;
- disadvantage government in commercial or policy negotiations with others;
- undermine the proper management of the public sector and its operations.

Criteria for assessing PROTECT assets:

- cause distress to individuals;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- breach statutory restrictions on the disclosure of information;
- cause financial loss or loss of earning potential, or to facilitate improper gain;
- unfair advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- disadvantage government in commercial or policy negotiations with others.

NFDC ICT Incident Response Procedure