PROTOCOL FOR THE USE OF INFORMATION TECHNOLOGY BY MEMBERS OF SOUTH DERBYSHIRE DISTRICT COUNCIL

PROTOCOL FOR THE USE OF INFORMATION TECHNOLOGY BY MEMBERS OF SOUTH DERBYSHIRE DISTRICT COUNCIL

CONTENTS

Section 1

Introduction

The I.T. Protocol, which follows, is in force for a number of reasons, the most important of which are:-

- To protect the Authority and its Members from prosecution. This can involve Data Protection, software usage, security and virus issues.

- To protect the assets owned by the Authority. These assets include not only software and hardware but also data.

- To standardise the working environment. This will allow every computer to operate the same, wherever you are located.

- To streamline laptop support procedures, giving the user a faster response to faults.

- To enable Members to carry out their duties safely and more effectively.

Remember that the I.T. Protocol is there to help all users of Information Technology and is not intended to restrict you in carrying out your normal Council activities.

The Protocol will be widely distributed either electronically or via hard copy.

From a Member's point of view it must be understood that until you have accepted the Protocol, you will not be allowed to use Information Technology belonging to the Authority.

The following Protocol must be read/understood and Members must sign to acknowledge that they abide by the requirements of this Protocol before any Council owned I.T. equipment is supplied to them.

Any breach of the Protocol may amount to a breach of the Members' Code of Conduct and could lead to the equipment being recovered by the Council.

If you require clarification of any issue about the use of I.T., please phone the I.T. Helpdesk on 01283 595705, which will be more than happy to assist.

When you are clear that you understand the requirements of the Protocol and agree to abide by it, you will be requested to sign the declaration at Appendix D upon collection of the equipment.

The Protocol will be monitored and reviewed periodically to consider any appropriate amendments necessary.

Section 2

Hardware Issued for External Connection to the Authority

The laptop and all associated equipment and software belong to and remain the property of the Council.

You must take all reasonable steps to ensure the equipment is kept secure and protected from theft/damage. Particular care should be taken with laptop computers to ensure that they are not left on view in cars or on public transport etc.

The laptop and all associated equipment must not be used for illegal purpose or in any way, which could bring the Council into disrepute and must not be used to operate a private business.

The Member will grant access to the laptop and other equipment to any authorised employee or agent of the Council at reasonable times for the purpose of service, repair or audit.

If a Member ceases to be a Member of the Council, the laptop and all equipment must be returned to the Council within 10 working days.

The Council Member must not allow any unauthorised person to access the Council's Network using their laptop and must keep all passwords secure. Passwords should be changed monthly and should not be in a form that could easily be guessed by a third party. For more information on good practice on password control, please refer to Appendix A.

No personal software should be installed on the laptop under any circumstances by Members. If any additional software is required, this can be requested via the I.T. Helpdesk subject to the necessary funding to cover any software licence implications. Each request will be evaluated on its merits.

For back-up purposes, data can be saved on diskettes and/or a Network Drive. The I.T. Section will provide information on the Network Drive to be used by Members.

The storage or processing of personal data (e.g. details of names and addresses) may be unlawful if not notified to the Data Protection Commissioner. Members should refer any queries on Data Protection issues to the Head of I.T. and Customer Services, Nigel Glossop, who is also the Council's Data Protection Officer.

In the event of theft, loss or damage to any part of the equipment, including data or diskettes, you should inform the I.T. Helpdesk immediately.

Where additional BT lines have been installed at home locations, you will be responsible for all call charges not relating to connection with an Authority based host system.

In respect of hardware issued for external connection to the Authority, the Council will insure and keep insured the hardware concerned.

2

In the event of the installed virus protection software discovering a virus on the hardware, you should follow the virus procedure as laid out below:-

Reporting the Action on Finding a Virus

- If a user sees or thinks that a virus is affecting the operation of software and/or hardware, switch off the hardware affected. Phone the I.T. Helpdesk immediately, which will advise you what action to take.

- Do not try to ignore the fact that a virus may be affecting your files – it will not clear itself and will continue to infect other software files/hardware.

Section 3

Internet Usage and External E-Mail

Any Member accessing the Internet for search/browsing or e-mail must ensure they adhere to the following rules:

- Your use of the Internet must be restricted to areas connected with your role as a Member of South Derbyshire District Council.

- Do not access any www area that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council. www sites visited by any user (Member or officer) when connected to the Council server are recorded, monitored and will be available for audit, if necessary.

- If you accidentally enter any area which could be construed as unfit, obscene or inappropriate you must leave it immediately and inform the I.T. Helpdesk. Be aware that your computer records which sites you have accessed.

- Care must be taken when downloading files via the Internet. Computer viruses may be contained in files and/or e-mails and can severely damage the operation of the laptop. If the installed virus protection software detects any viruses, please follow the instruction on page 3.

- If you receive unsolicited e-mail (e.g. junk or chain mail), do not forward such items to other recipients.

- Never leave the computer unattended whilst you are using the Internet. The session will be your responsibility. Also, the computer should not be left switched on and unattended for security purposes.

- Use the Internet and its facilities in a responsible way.

- Detailed E-mail guidelines and Internet guidelines are attached at Appendices B and C respectively.

Section 4

Use of the Equipment

The laptop and associated software supplied to you is for your use as an elected Member of South Derbyshire District Council.

This includes all the work you do as a Councillor at present, for example:

- Communicating with officers and other Members.
- Dealing with official correspondence.
- Researching issues relevant to your work as a Councillor.

Use for Party Political Purposes/Party Political Publicity

There is a clear statutory ban on the use of Council property (including PC's, laptops, copiers, scanners, printers, paper and software) **for any purpose connected with party political publicity**, either at election time or at any other time. At election time there are also detailed restrictions on the use of Council property for other party political purposes as well as publicity. The safest course is to avoid the use of Council I.T. equipment for any purely **party political purpose** at **any** time.

This does not prevent Members from using Council property for **general** "political" purposes, including for example researching an issue which concerns you as a Councillor, even though that issue may be politically controversial. Also, this does not prevent you from using Council property to work on matters raised by a constituent in your Ward. However, Council property should not be used for processing names and addresses of your constituents for electioneering purposes.

Section 5

The Law

Data Protection

You are responsible for complying with the Data Protection Act 1998 which covers information held in electronic and paper-based form about individuals. It is a criminal offence to collect and process personal data on your laptop unless the use is registered with the Data Protection Registrar. Details of registration should reflect Internet use. The Head of I.T. and Customer Services has copies of all the Council's Data Protection registrations and can give you advice.

The Data Protection Act 1998 considerably increases the obligation on users of personal data, such as:

- banning sending personal data to non-European Economic Area countries with inadequate protection for data subjects;
- prohibition on processing certain 'sensitive data' such as someone's marital status or ethnic origin.

Computer Misuse

The Computer Misuse Act 1990 covers unauthorised or malicious use of any computer system. It is the law used to prosecute hackers and people who write and distribute computer viruses deliberately.

It is a criminal offence to access, or attempt to access, any computer system you are not authorised to access. This law protects against employees and members of the public who deliberately cause damage to systems and data. The Act also makes it illegal for a person to deliberately delete data or sabotage systems to the detriment of the Council.

Harassment

You can commit harassment either by using e-mail or send a harassing message to someone or by downloading and distributing material from the Internet which constitutes harassment because it creates an intimidatory working environment. Harassment and discrimination are unlawful under the Protection from Harassment Act 1997, the Sex Discrimination Act 1975, the Disability Discrimination Act 1995 and the Race Relations Act 1976.

As with any form of harassment under the anti-discrimination legislation, the intention of the parties is irrelevant. The problem with e-mail is that, with the lack of visual clues, offence may be caused where none was intended.

Obscene Material

Publishing legally 'obscene' material is a criminal offence under the Obscene Publications Act 1959. This includes electronic storing and/or transmitting obscene materials that would tend to deprave and corrupt or paedophiliac material.

Defamation or false statements

The liability for defamation or false statements applies to electronic communication just as it does to more traditional forms of communication. Anyone who e-mails a libellous or false e-mail message or posts such a message on the Internet will be responsible for it and liable for any damage it causes to the reputation of the victim.

In addition to the liability of the individual who made the libellous or false statement, the Council may also be held liable. This could be either under the normal principles of:-

- **Indirect** liability because the Council is considered responsible - known as 'vicarious liability'; or

- **Direct** liability as a publisher because of providing the link to the Internet and e-mail system.

An untrue statement that damages the reputation of a person or company by causing people to think worse of them will generally be defamatory. Similarly, a false statement intended to cause damage to a person or their economic interests can bring a claim for damages.

Do not put anything on an e-mail or an attachment, which you would not put in a normal letter on Council headed paper. Treat e-mail as you would a postcard going through the open post.

Copyright

Although any material placed on the Internet or in public discussion areas is generally available, the originator still has moral and, possibly, legal rights over it. You should not copy it without acknowledging the original source and, where appropriate, gaining their permission. This applies even if you modify the content to some extent. Please note that any official material placed on a website is subject to copyright laws.

Copyright laws are different for each piece of software. In general, the copyright to every piece of software run on a system is owned by whichever company or person wrote it. The Council has a legal duty to make sure sufficient licences of the correct type are present to cover the use of all software. You must be aware of these issues and make sure that the Council has correct licences for any software you are using.

Contracts

E-mail is generally regarded as an informal means of communication but it is, nevertheless, capable of creating or varying a contract in just the same way as a written letter. You should be careful not to create or vary a contract accidentally.

Disclaimer

Despite putting confidential disclaimers and, where appropriate, personal disclaimers, on external communications, there is still nevertheless a legal connection to the Council. Always remember that any statement you make may still be construed as representing the Council.

GOOD PASSWORD GUIDELINES

Members should adopt the following guidelines for allocating and managing their passwords:-

1. Keep passwords confidential.

2. Avoid keeping a paper record of passwords, unless this can be stored securely.

3. Change passwords whenever there is any indication of possible system or password compromise.

4. Select passwords with a minimum length of eight characters.

5. Avoid basing passwords on any of the following:-

   • month of the year, days of the week or any other aspect of the date

   • family names, initials, birthdays or car registration numbers

   • company names, identifiers or references

   • telephone numbers or similar all numeric groups

   • user-id, username, group-id or other system identifier

   • more than two consecutive identical characters

   • all numeric or all alphabetic characters

   • simple and obvious strings of characters such as QWERTY or 12345

6. Change passwords at monthly intervals.

7. Change temporary passwords the first time you logon.

8. Take care in the siting of keyboards to minimise casual observation.

9. Do not include passwords (or user-ids) in any automated logon process, for example as part of the AUTOEXEC.BAT FILE or stored in a function key.

E-MAIL GUIDELINES

These guidelines apply equally to internal and external e-mail.

If you use the e-mail system, you must follow these guidelines.

Never . . .

1.   Use the e-mail system for knowingly doing anything illegal under English law, or for unacceptable purposes that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council.

2.   Transmit confidential, personal or other sensitive information on e-mail unless you can apply appropriate 'encryption' - putting messages into code - to protect it.

3.   Abuse others - even in response to abuse directed at you.

4.   Use e-mail to harass or threaten others in any way.

5.   Use anonymous mailing services to conceal your identity or falsify e-mails to make them appear to originate from someone else.

6.   Access anyone else's mailbox unless they have given you proxy or authorisation rights. Unauthorised access is a breach of security.

Don't . . .

7.   Use the 'Reply All' function unless everyone in the original message needs to know your response.

8.   Print out messages unless they are really important.

9.   Send large e-mails or attachments. It's not an economical or sensible way to handle large documents and it can halt the e-mail system. It is better to put the file on the network and direct people to it.

10.   Create e-mail congestion by sending trivial messages or by copying e-mails to those who don't need to see them.

11.   Forward confidential or restricted items on e-mail sent to you personally without the originator's permission.

Remember . . .

12.   E-mails may be read by a far wider audience than originally intended, because of the ease of forwarding messages to new recipients.

13.   E-mail is not guaranteed to arrive at its destination within a particular time, or at all.

14. Not to send a message in capital letters. It is the electronic version of **shouting**.

15. Always put appropriate disclaimers on your messages.

16. Any advice you give on e-mail has the same legal standing as any other written advice.

17. Before sending an e-mail, ask yourself how you would feel if your message were read out in Court.

18. Not to assume that the message has been read just because it has been sent.

19. Avoid sending graphics - it may look nice but it takes up valuable computer storage space and increases processing time.

20. It's easier to change and distribute messages and documents in the e-mail environment than it is in a purely paper-based one. Use these two categories to indicate the confidentiality of the message or document being sent. Put the category at the start of the 'subject' line. Most messages and their attachments don't need a confidentiality status. If no category is given, the assumption is that the message and/or document has no confidentiality status and can be changed and forwarded as required.

    Confidential Message and/or document marked 'confidential'. This should not be freely copied. Distribution should be limited to a 'need-to-know' basis.

    Restricted Message and/or document marked 'restricted'. Printing, copying and distributing of the document should be closely monitored by the originator and the recipient, and should not happen without the originator's consent. Editing should only be done with the originator's consent.

21. Beware of sending "joke e-mails" or chain e-mails. Whilst you may consider the material not to be inoffensive, a different person may not.

Do ...

22. Maintain your e-mail mailbox properly:-

- Open all e-mails at least daily or make sure that a re-direction is set up if you are away for more than a day.
- Only keep messages that are necessary for current business needs.
- Store all e-mail messages necessary for permanent business records in your personal folders, according to current record retention policies.
- Delete insignificant, obsolete and unnecessary messages, return/read receipts and attachments, daily. Clear your 'deletion' folder daily to get rid of unwanted items.

23. Use a password protected screen saver if your laptop is in an area where unauthorised users could easily access it.

24. Make sure you use the correct address when sending mail. If the e-mail fails to reach its destination, it may be lost or fall into the wrong hands. Double-check the address when you send important messages.

25. Always get confirmation of receipt for important e-mails.

26. Make and keep hard copies of very important e-mails sent and received.

27. Reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will or should be sent.

28. Only print an e-mail if you need a hard copy for filing - don't waste paper.

29. Develop orderly filing systems for messages you need to retain.

30. When responding, concern yourself only with your response. Don't reproduce the message sent to you unless it is really necessary. This makes messaging more effective and conserves network resources.

31. Keep messages brief and to the point. Some people find it harder to read from the screen than they do from paper.

32. Always enter a subject title to your e-mail. Make sure that the 'subject' field of the message is meaningful. This helps everyone file and search for his or her messages more effectively.

33. Try to use one message for one subject. Multiple subjects within a single message make it difficult for the recipient to respond effectively, and to file the message.

34. Think whether all your intended recipients really want or need to receive the message and any attachments.

If in doubt . . .

Contact the I.T Helpdesk on 01283 595705

INTERNET GUIDELINES

If you use a connection to the Internet, you must follow the requirements of these guidelines.

Never...

1. Use the Council's Internet access for knowingly doing anything which is illegal under English law, or the law of any other relevant country, or for unacceptable purposes such as accessing any www area that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council.

2. Divulge personal information such as addresses and telephone numbers over the Internet.

3. Use the Council's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

4. Knowingly use the Council's Internet facilities to disable or overload any computer system, network, or equipment or attempt to disable, defeat or circumvent any systems intended to protect the privacy or security of another user, including the Council's 'firewall' security systems.

Don't...

5. Leave Internet connections unattended.

6. Release protected information through a newsgroup or chat line - whether or not the release is inadvertent, it comes under all the penalties under existing data security policies and procedures.

7. Order or pay for personal goods and services using Council equipment on the Internet.

Remember...

8. You must not provide false information to any Internet service which requests your name, e-mail address or other details.

9. If you accidentally access unsuitable material, you must disconnect from the site immediately and inform the senior officer in I.T. Services.

Do...

10. Only use Internet browser software provided and configured by the Council, and only use officially provided access mechanisms.

11. Immediately report any security problems or breaches to the I.T. Helpdesk.

SOUTH DERBYSHIRE DISTRICT COUNCIL

Declaration

I, Councillor _____ acknowledge receipt of the

Protocol for the Use of Information Technology by Members of South

Derbyshire District Council.

I confirm that I have read the Protocol and agree to abide by it.

SIGNED _____

DATED _____

Section 4

Use of the Equipment

The laptop and associated software supplied to you is for your use as an elected Member of South Derbyshire District Council. If you have had a separate broadband line installed, this line should not be used for voice calls.

This includes all the work you do as a Councillor at present, for example:-

- Communicating with officers, other Members, MP's, government officials, partner organisations and members of the public.
- Dealing with official correspondence.
- Researching issues relevant to your work as a Councillor and/or matters raised by a constituent in your Ward.
- Communicating and obtaining information in support of approved personal training and development activities.
- Viewing and obtaining material for discussion by a political group on the Council, as long as that relates to the work of the Council and not the political party.
- Formulating policy and the decision-making process of the Council or other organisation on which you have been formally appointed to represent the Council.

Use for Party Political Purposes/Party Political Publicity

Under the Members' Code of Conduct there is an absolute restriction on Members using or authorising the use by others of the resources of the Council ('resources' includes land, premises and any equipment such as PC's, laptops, copiers, scanners, printers, paper and software and the time, skills and help of anyone employed by the Council) for political purposes.

There is also a clear statutory ban on the use of Council property **for any purpose connected with party political publicity**, either at election time or at any other time. Publicity is defined as any communication, in whatever form, addressed to the public at large or to a section of the public. This will include press releases and letters to the media. At election time there are also detailed restrictions on the use of Council property for other party political purposes as well as publicity. The safest course is to avoid the use of Council I.T. equipment for any purely **party political purpose** at **any** time.

This includes all the work you do in connection with:-

- Constituency party meetings, Ward party meetings etc. or communications to party members collectively in their capacity as party members.
- Processing names and addresses of your constituents for electioneering purposes.

PERSONAL USE – MEMBERS' LAPTOPS

Personal Use

The IT equipment and broadband connection may be used for personal purposes provided that:-

- it is not detrimental to corporate interests
- it does not cause any disruption, disturbance, inconvenience or degradation of the service
- it does not interfere with the work of the Council
- it does not involve unacceptable use of the Council's system
- the set up of the equipment and connection is not changed in any way
- any Council supplied broadband connection can only be used with Council equipment

Examples of unacceptable use are:-

- breach of confidentiality
- breach of security rules/guidelines, e.g. breaking through security controls
- representing values which are contrary to any Council policy
- promoting any private or personal interests such as selling personal possessions, property or promoting a social activity not related to the Council
- deliberate accessing or attempting to access, viewing, downloading, displaying, printing or distributing from the internet of what is considered to be material likely to incite criminal behaviour
- using or transmitting abusive, defamatory, libellous, profane or offensive language
- the importation of computer viruses and similar software through unauthorised downloading of files and programmes from external sources
- running software that is not approved by the Council
- loading software applications directly onto any of the Council's systems without approval
- knowingly causing congestion and disruption of networks and systems
- deliberate accessing or attempting to access, viewing, downloading, displaying, printing or distributing of what is considered to be offensive, obscene, sexually explicit or pornographic from the internet
- sending e-mail messages and/or attachments that cause offence or are considered to be harassment on the grounds of gender, race, ethnic or national origin, disability, family status, age, religious belief, class or sexuality. Examples are messages that contain sexual innuendoes, racially biased jokes or obscene language.

This is not an exhaustive list.

Monitoring of Communications

You need to be aware that the Council has the capability to monitor all use of the internet and intranet and logs and retains the records.

The reason that monitoring takes place is to ensure that the standards and rules set by the Council and legislation are complied with.

We record or monitor:-

- details of websites visited or attempted to be visited
- pages accessed
- files downloaded
- graphic images examined
- any file attachments (e.g. pictures or word documents)

The Council has the capability to monitor, log and retain e-mail correspondence.

Any potential viruses within e-mail and internet traffic passing through or outside the Council's systems are scanned for.

General Issues

Any messages or information you send to someone outside the Council, or statements that reflect on the Council (this is either in a personal capacity or on business use through an electronic network such as bulletin boards, on-line services or the internet) wherever appropriate you must make it clear that the views expressed are personal and may not necessarily reflect those of South Derbyshire District Council.

You must not use anonymous mailing services to conceal your identity when mailing through the internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any internet service which requests name, e-mail address or other details.

U:\JAYNE\DemServ\LaptopsPersonalUse.doc