South Derbyshire District Council

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

Version: 1.5

Date: April 2018

Contents

Version Control 2
Approvals 2
Associated Documentation 2
1.0 Introduction 3
2.0 Access to Authority ICT Systems 4
3.0 Hardware Issued by the Authority 4
4.0 Internet Usage and External E-Mail 5
5.0 Use and Care of the Equipment 6
6.0 The Law 11
7. Responsibilities 13
APPENDIX A 15
APPENDIX B 16
APPENDIX C 19
APPENDIX D 21

Version Control

Version	Description of version	Effective Date
1.5	Updated to reflect new ICT equipment, member requirements and best practice	April 2018

Approvals

Approved by	Date

Associated Documentation

Description of Documentation	

1.0 Introduction

The ICT 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 ICT equipment procedures, giving users a faster response to faults.
- To enable Members to carry out their duties safely and more effectively.

The ICT Protocol is a tool to help all users of Information Technology and is not intended to restrict you in carrying out your normal Council activities. South Derbyshire District Council provides Members with ICT equipment to reduce costs and improve productivity.

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

In order for access to be granted to the Councils ICT infrastructure a Member must understand and accept this protocol. Failure to agree or and subsequent breach will result in withdrawal from the environment.

The following Protocol must be read and understood and Members must sign to acknowledge that they abide by the requirements of this Protocol before any Council owned ICT equipment is supplied to them or any access to ICT systems enabled.

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

If you require clarification of any issue about the use of ICT, please contact ICT Services on 01283 595705, who 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 or when access to ICT systems is enabled.

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

All other South Derbyshire District Council District Council codes, guidelines and policies apply in addition to the ICT Protocol

2.0 Access to Authority ICT Systems

In order to gain access to the SDDC systems, such as outlook, networked drives and exempt information in CMIS it is necessary to have a valid username and password. Your username and password will be provided upon completion of Appendix D. The password generated and assigned to a user account will follow strict protocol on its composition as documented in the ICT Security Policy. This will need to be changed upon first logon, equally there will be specific requirements as to the composition of your chosen password for security purposes. The password (Active Directory) will need to be changed every 60 days.

Any equipment provided by the Council must not be used for illegal purposes or in any way which could bring the Council into disrepute and must not be used to operate a private business.

The Council Member must not allow any unauthorised person to access the Council's systems using their network credentials or equipment and must keep all passwords secure. For more information on good practice on password control, please refer to Appendix A.

It should be noted that anything stored locally on Council equipment, that is to say, not on the network drives is not backed up by the Council. Members must only save documents to their U drive. Saving files to the desktop is strictly prohibited.

Where additional 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. If you have had a separate broadband line installed, this line should not be used for voice calls.

3.0 Hardware Issued by the Authority

All ICT equipment and applications and data belong to and remain the property of the Council.

ICT equipment will be expected to be used for all democratic work, including use at Council meetings and reading/annotating agendas, reports, minutes and accessing SDDC emails.

The Member will take all reasonable steps to ensure ICT equipment is kept secure and protected from theft/damage. Particular care should be taken with regard to ensure ICT equipment is not left on view in cars or on public transport etc.

The Member will grant access to ICT 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, all equipment must be returned to the Council within 10 working days.

The storage or processing of personal data (e.g. details of names and addresses) may be unlawful in certain circumstances, advice is available from the Data Protection Officer.

Malfunctions with the ICT equipment should be reported to the ICT Service desk on 01283 595705. Under no circumstances should arrangements be organised for repairs to be undertaken.

In the event of damage to any part of the equipment, you should inform the ICT Service Desk immediately on extension 5705 (01283 595705).

In the event of theft or loss of ICT equipment the Member must report the incident to the Police to obtain a crime reference\lost property number and then provide this information to the ICT Service Desk on extension 5705 (01283 595705).

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

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 Member suspects a virus is affecting the operation of software and/or hardware, they shall switch off the hardware affected. Phone the ICT Service Desk immediately, who will advise 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, and potentially other users of the network.

4.0 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:

- 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 ICT Service Desk. 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 instructions above.

- 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. It should also be noted, 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.

5.0 Use and Care of the Equipment

All ICT equipment and system access supplied to you is primarily for your use as an elected Member of South Derbyshire District Council.

This includes all the work you do as a Councillor, 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.

5.1 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, 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 ICT 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.

5.2 Personal Use

The ICT equipment or services 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 setup 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.
- Using 4g for personal use
- The use of proxy sites.

This is not an exhaustive list.

5.3 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.

5.4 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.

5.5 Care of the Equipment

Members are required to take all reasonable care of the Authority's equipment. Members should not eat, drink or smoke over the equipment.

Lending ICT equipment to any third party is strictly forbidden

Elected Members should never attempt to delete software packages from ICT equipment. It should be noted that these will be updated or changed over time and ICT can do this remotely.

Members are allowed to connect their ICT equipment to their home or third party Wi-Fi networks, and this should be done where appropriate to minimise the cellular usage.

ICT equipment has been selected with robustness in mind however screens are made of glass and therefore are subject to cracking and breaking if misused. Never drop nor place heavy objects

(books, laptops, etc.) on top of the equipment. If provided upon delivery, the equipment should be kept in the case or cover at all times when not in use.

Only a soft cloth is to be used to clean screens.

To extend battery life, users should always turn off and secure their ICT equipment after work is completed.

Do not subject the ICT equipment to extreme heat, cold or moisture (do not store in vehicles).

When carrying ICT equipment in a vehicle or on public transport every effort should be made to keep the device secure i.e. do not eave on display.

The whereabouts of the ICT equipment should be known at all times. It is the user's responsibility to keep their equipment safe and secure.

One charger will be issued with each item of ICT equipment. If lost Members will be expected to replace these at their own cost. This also applies to peripherals supplied with the equipment such as a stylus.

5.6 Strictly forbidden Activity

Illegal installation and transmission of copyright materials.

Users are not allowed to send, access, upload, download, or distribute offensive, profane, threatening, pornographic, obscene, or sexually explicit materials. Downloading other browsers is not permitted. Proxy sites are also prohibited.

Use of South Derbyshire District Council District Council's internet/E-mail accounts for financial or commercial gain or for any illegal activity.

5.7 Malfunction of Equipment

Malfunction or any other technical problem with ICT equipment should be reported to the ICT service desk 5705 (01283 595705), under no circumstances should repairs be organised without consultation with ICT.

5.8 Cameras

Users must use good judgement. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Cameras must not be used in meetings without the permission of the chairman.

5.9 Messaging

Messages must not be sent during meetings. The device should only be used during meetings to access CMIS unless express permission is given by the chairperson to use for research during the meeting.

ICT equipment provided to Members should not be used to access personal social media sites such as Facebook and Twitter. It is however permissible for Members to use equipment provided for social media for legitimate business reasons such as communicating with residents or maintaining SDDC corporate sites. It is recommended that Members have separate social media accounts for Council business

5.10 Excessive Usage

ICT equipment cannot be used abroad. Usage charges are not covered by UK tariffs, are expensive and insurance cover does not stretch out of the UK.

Cellular data is provided to meet the business needs of the Council and appropriate usage tariffs will be selected accordingly.

The Council provides a mobile data contract which allows for up to 1 GB of data per month to be downloaded through the mobile network. This should be sufficient to cover all work requirements. Unless there are exceptional work requirements that cause the limit of 1 GB to be exceeded then data usage above that level will be charged to the individual member concerned.

Wi-Fi connections should be used wherever possible to avoid additional usage charges. The Civic Offices (in Council Chamber & Members room) Wi-Fi will be preconfigured and equipment can easily be setup for home Wi-Fi or where this is provided in other locations such as Café's, hotels. If assistance is required please contact ICT Services on 01283 595705.

5.11 Malicious Use/Vandalism

Any attempt to destroy hardware, software or data is forbidden.

Defacing of ICT equipment, including the SDDC ID tag, in any way is prohibited (stickers, markers, etc.).

6.0 The Law

6.1 Data Protection

You are responsible for complying with the General Data Protection Regulation (GDPR) 2018 and any consequential data protection legislation as updated, amended or replaced from time to time which concerns the direct use of personal data, whether that information is held in electronic or paper-based form.

The GDPR introduces a duty on the Council to report Personal Data breaches to the Information Commissioners Office ("ICO") within 72 hours of becoming aware of the breach. You must therefore report the breach without undue delay to the Council's Data Protection Officer. If the breach is likely to result in a high risk of adversely affecting the individual's right and freedoms, the Data Protection Officer will inform the individual.

The GDPR applies to Personal Data meaning any information relating to an identifiable person who can be directly or indirectly identified, such as the name, identification number, location data or online identifier. It also applies to sensitive personal data such as genetic data and biometric data. The GDPR itself has 8 principles, all of which must be adhered to when handling personal data.

You should ensure that the Personal Data held for Council purposes should not be used for political purposes.

You should be aware that the unauthorised processing or disclosure of such data is prohibited under the GDPR, you are responsible for ensuring that there is no such unauthorised disclosure of data. If the Council fails to abide by the GDPR, it could be prosecuted and fined up to 20 million Euros (17 million pounds) or up to 4 per cent of the Council's turnover. The GDPR also imposes legal liability if you are responsible for a breach. In addition the Council or the individual officers may be liable to pay compensation to any individual who has suffered material or non-material damage as a result of such a breach.

You must comply with the GDPR and the Council's GDPR policies, procedures and guidelines. It is your responsibility to be familiar with and adhere to the requirements of GDPR.

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 Strategic Director of Finance & Corporate Services has copies of all the Council's Data Protection registrations and can give you advice.

6.2 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.

6.3 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 and the Equality Act 2000. 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.

6.4 Obscene Material

Publishing legally 'obscene' material is a criminal offence under the Obscene Publications Acts 1959 and 1964. This includes electronic storing and/or transmitting obscene materials that would tend to deprave and corrupt or paedophiliac material.

6.5 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 in accordance with the Defamation Act 2013 for causing or likely to cause serious harm 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.

6.6 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.

6.7 Contracts

Electronic communication, such as 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.

6.8 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.

7. Responsibilities

Violation of the Acceptable Use Policy may be subject to but not limited to; action under the Member Code of Conduct, repossession, removal of content.

7.1 Member

Violation of the Acceptable Use Policy may be subject to but not limited to; action under the Member Code of Conduct, repossession, removal of content.

All material viewed and stored on ICT Equipment must be in accordance with the ICT protocol and values of South Derbyshire District Council.

Users must exercise the same prohibited uses as the use of South Derbyshire District Council computers and laptops.

7.2 Corporate ICT

Provide SDDC supplied ICT equipment to a recognised standard build that can access the Internet and emails to the device from the users SDDC email account.

Ensure any incidents in relation to ICT equipment acceptable use protocol are referred to Democratic Services and investigated

Provide support and maintenance of ICT equipment in keeping with the corporate ICT service standards.

Providing basic training and instruction on their use

Providing advice and support to staff and Members regarding ICT equipment

Investigation of any suspected misuse of devices

APPENDIX A

GOOD PASSWORD GUIDELINES

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

1. Keep passwords confidential.
2. Do not keep a paper record of passwords.
3. Take care in the siting of keyboards to minimise casual observation.
4. 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.

APPENDIX B

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 ICT Services

APPENDIX C

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 ICT 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 ICT Service Desk.

APPENDIX D

Important

Please sign and return to Strategic Director Corporate Resources

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.

I have received a tablet PC, asset number ……

SIGNED _____

PRINT NAME _____

DATED _____