Appendix 19 - Protocol for use of ICT by Members/Use of Resources

1. Introduction

The protocol sets out to support Members to carry out their role effectively with the Information Communication Technology (ICT) provided whilst protecting the Authority and its Members from the risks associated with its use.
The Protocol helps Members to stay compliant with the law and good security practise and is intended to assist and enable them in carrying out their Council activities.
This protocol must be used in conjunction with agreed policies and procedures around ICT security and use of systems such as internet and email.
Any breach of the requirements of the protocol or the agreed policies and procedures may amount to a breach of the Members' Code of Conduct and the removal of access to the Council's assets and systems.

2. ICT Equipment

Members are provided with equipment to support their needs. Each Member is able to choose from a standard list of equipment detailing the type of use supported and cost of each item. Support is available from the Finance and ICT Division to help Members understand what each item can and can't support and to match the device to the Member's individual requirements. Members will be able to choose either a laptop, tablet or hybrid and a smart phone. Printers will not be supplied as standard.
All items are procured through the standard DCC procurement process and are covered by standard warranty and insurance policies.
Any equipment issued belongs to, and remains the property of the Council.
The equipment is provided to be used for all democratic work, including use at Council meetings, reading/annotating agendas, reports, minutes and accessing DDC emails and for constituent work related to the Council. It is not to be used for purely political purposes or private business purposes. Where Members are also elected to other Derbyshire bodies arrangements may be able to be made to share equipment.

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

The Member will only grant access to the equipment to an authorised employee or agent of the Council for the purpose of service, repair or audit and will make the equipment available at reasonable notice and in working hours. Use by family / friends and the like is not permitted however family members can

provide assistance to Members in the use of the equipment as long as the Member remains in overall control and does not divulge their user name or password.

If a Member ceases to be a Member of the Council, the equipment must be returned to the Council within 10 working days and in such an event access to Council systems will be disabled within ten working days.

In the event of theft, loss or damage to any part of the equipment, you need to inform the ICT Service Desk immediately on 016295 37777 or complete a Security incident form using the Service Desk Online icon on the desktop.
In the event of theft of the equipment, report the incident to the Police to obtain a crime reference\lost property number and then provide this information to the ICT Service Desk

Lending any equipment to any third party is strictly forbidden.

3. Software

Members ICT equipment is configured to comply with the Council's ICT Security Policy and to meet the requirements of the Governments Code of Connection to the Public Services Network. Any unauthorised changes may contravene these policies therefore configurations must not be changed and Members must not attempt to add additional hardware or software.
If any additional applications are required, these can be requested via Democratic Services initially, to establish the need on an individual and collective basis, subject to the necessary funding to cover any applications. Each request will be evaluated on its merits.

Elected Members should never delete any of the Council supplied software or Apps. It should be noted that these will be maintained, updated or changed over time and ICT can do this remotely.

If there is a suspicion of a virus infecting the equipment or any notifications of untoward activity this must be reported **immediately** to the ICT Service Desk.016295 37777. Do not ignore warnings as this could lead to more widespread infections and serious disruption to Council ICT systems.

All software provided by the Council with the computer, or subsequently, remains the property of the Council, or the licensing organisation as appropriate, and may not be shared or copied to another computer/device without written authorisation from the
Director of Finance and ICT.

4. Access to Systems

Access to the Council's systems is via a username and password and individual applications may need their own username and password. Members are required to abide by the Council's password policy and persistent failure to use a sufficiently secure password may be deemed to be a breach of the Member's Code of Conduct. Regular audits of all DCC passwords are undertaken as part of the security audits of the authority.
Care must be taken to keep passwords secure and passwords must not be disclosed to anyone.
Systems and equipment must only be used for Council business. ICT equipment left unattended must be locked or logged off. Members are responsible for all activity undertaken when logged onto the equipment and must not allow any unauthorised person access to the Council's systems.

Members are allowed to connect their equipment to their home or third party Wi-Fi
Networks.

5. Storage

Various places are available to store electronic data and specific guidelines will be provided as part of Member induction. All Council meeting papers will be accessible by Modern.gov and Members are discouraged from printing off meeting papers.
Any data stored locally on equipment is not backed up and will be lost in the event of loss or damage to the equipment. All data that you need to retain should be moved when possible to central storage such as EDRM. Council data should not be transferred to removable media, should it be necessary only DCC provided items that are encrypted are to be used and this must not then be transferred to personal or third party equipment without the necessary permissions.
Members are encouraged to go paperless and should print only essential material.

6. Internet access

Do not access any area that could be construed as unfit, obscene or would otherwise, be considered as inappropriate for a Member of the Council. All internet sites visited by any user (Member or officer) when connected via Council equipment are recorded, monitored and if necessary will be available for audit purposes.
If you accidentally visit any area that could be construed as, unfit, obscene or inappropriate you must leave it immediately and inform Democratic Services.

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 equipment and the Council's systems. If in doubt, do not click on links or download files.

The equipment provided to Members must not be used to access personal social media sites such as Facebook and Twitter. It is however permissible for Members to use the equipment provided for social media for legitimate Council reasons such as communicating with residents or maintaining corporate sites. It is recommended that Members have separate social media accounts for Council business. Members are required to adhere to the Acceptable use of Social Media policy.

Any personal views expressed using Council provided equipment and access must make it clear that the views expressed are personal and may not necessarily reflect those of the Council.

7. Email

Members will be allocated a Council email address for use on Council business. This email must not be used for personal or political purposes.

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

You must not use anonymous mailing services to conceal your identity when sending emails, 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.

Members can not automatically forward email from a Council email account to a web mail account hosted on the Internet by a third party, for example Google, Yahoo, Hotmail etc. and should not manually do so as a matter of course as this could lead to Council data on insecure domains.

The full Internet and Email Acceptable Use Policy will be provided to Members and is available on the Council website. This policy must be adhered to at all times.

8. Cameras

Any camera on ICT equipment must not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor be used to embarrass anyone in any way .Members must use their judgement on appropriate use of cameras. Good practise is to ensure that any person to be photographed has given their consent.

Cameras must not be used in meetings without the permission of the chairperson.

9. Monitoring

The Council has the capability to monitor all use of the internet and intranet, maintain logs and retains the records. The reason that monitoring takes place is to ensure compliance with legislation and the standards and rules set by the Council. 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 e-mail and internet traffic being sent or received by the Council's systems are scanned for potential viruses.

10. Complying with legislation

The following is a summary of areas to be aware of but cannot give full detail of all aspects of relevant legislation.

- **Data Protection**

You are responsible for complying with the Data Protection Act 2018, 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 ICT equipment unless the use is registered with the Data Protection Registrar. The Director of Legal & Democratic Services has copies of all the Council's Data Protection registrations and can give you advice.

- **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**

The Protection from Harassment Act 1997 covers harassment either by using e-mail to 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 (Amendment) 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, written communication can be misinterpreted and offence may be caused where none was intended.

- **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.

- **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**

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.

- **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.

11. ICT Points of Contact

The IT helpdesk is the first point of contact for all ICT enquires, queries and support problems. Calls can be logged via the desktop icon Service Desk Online
Operating hours: Monday –Friday 08:00 – 18:00
Contact Details Tel: 01629 537777
Email: service.desk@derbyshire.gov.uk
Alternatively contact the Member ICT Support officer..