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

1. Introduction

1.1 This protocol sets out to support Members to carry out their role effectively with the Information Communication Technology (ICT) provided whilst protecting the Council and its Members from the risks associated with its use. The protocol helps Members to stay compliant with the law and good security practice and is intended to assist and enable them in carrying out their activities.

1.2 This protocol must be used in conjunction with agreed policies and procedures around ICT security and use of systems such as internal 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, systems and resources.

2. ICT Equipment

2.1 Members are provided with equipment to support their needs. Support is available from ICT to help Members understand what each item can and cannot support and to match the device to the Member's individual requirements, such requirements may include a laptop, tablet or mobile phone. Printers will not be supplied.

2.2 All items are procured through the standard ICT procurement process and will be covered by standard warranty and insurance policies. All equipment issued belongs to and will remain the property of City of York Council. The equipment provided must be used for all democratic work, including use at Council meetings, reading/annotating agendas, reports, minutes and

accessing City of York Council emails and for constituent work related to the Council and Council business. It is not to be used for purely political purposes or private business purposes. Where members are also appointed to other bodies, arrangements may be made to share equipment.

2.3 All reasonable steps must be taken to ensure that equipment is kept secure and protected from theft/damage. Particular care must be taken to ensure that equipment is not left on view in cars or in public transport, etc. In the event of theft, loss or damage to any part of the equipment, members must inform the ICT Service Desk, by telephone (01904 552222) or email (ictservicedesk@york.gov.uk) immediately. In the event of theft of the equipment, the theft must be reported to the Police without delay in order to obtain an Incident Number and then provide this information to the ICT Service Desk and Insurance @ insurance.claims@york.gov.uk.

2.4 The member will only grant access to any 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 or any other third party is not permitted, 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.

2.5 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 10 working days.

Lending any equipment to a third party is strictly forbidden.

3. Software

3.1 Members ICT equipment is configured to comply with the Council's ICT Security Policy and to meet the requirements of 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 to any equipment.

3.2 If any additional applications are required, these can be requested by contacting the ICT Service Desk. Each request will be evaluated on its merits. Members should never delete any of the Council supplied software or any applications.

3.3 In the event of any maintenance or updates becoming necessary, the ICT Service desk may be able to do this upon request remotely, but where this is not possible the equipment must be returned to West Offices at an agreed time for such works to be carried out.

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

3.5 All software provided by the Council with any equipment remains the property of the Council, or the licensing organisation and may not be shared or copied to another computer/device.

4. Access to Systems

4.1 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 adhere to the Council's password policy. Regular audits of all passwords are undertaken as part of the security audits of the Council. Care must be taken to keep passwords secure and passwords must not be disclosed to anyone and must be changed when required by ICT should security concerns be identified.

4.2 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.

4.3 Members are permitted to connect their equipment to their home or third party Wi-Fi, subject to any provisions of the Council's ICT policies.

5. Storage

5.1 Various places are available to store electronic data and specific guidelines will be provided as part of Member training/Member induction. All council meeting papers will be accessible by Modern.gov. Members are discouraged from printing off meeting papers. Members are encouraged to be as paperless as possible and should only print essential material.

5.2 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 where possible to central storage. Council data should not be transferred to removable media, should it be necessary only City of York Council items that are provided by the Council and are encrypted are to be used and this must not then be transferred to personal or third party equipment

without the necessary permissions from the Corporate Governance Team.

6. Internet Access

6.1 Do not access any area that could be construed as unfit, obscene or would otherwise be considered inappropriate for a Member of the Council. All internet sites visited by any user (Member or Officer) when connected via Council equipment will be 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 the Monitoring Officer.

6.2 Care must be taken when downloading files via the internet. Computer viruses may be contained in files and/or emails 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.

6.3 The equipment provided to Members should not be used to access personal social media sites such as Facebook or 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 provisions of any Council ICT policies around social media. Passwords for social media accounts must never be the same as the passwords used for logging onto the device or any CYC system.

7. Email

7.1 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 any unsolicited emails (e.g. junk or chain mail) do not forward to any other recipients and delete them or move them into the junk folder.

7.2 You must not use anonymous emailing services to conceal your identity when sending emails, falsify emails to make them appear to originate from someone else, or provide false information to any internet service which requests a name, email address or other details.

7.3 Members must not automatically forward emails from a Council email account onto a webmail 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 can lead to Council data being placed on an insecure domain.

7.4 All Council ICT policies are available on the Council's Intranet. These policies must be adhered to at all times.

8. Cameras

8.1 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 practice is to ensure that any person to be photographed has given their consent.

9. Monitoring

9.1 The Council has the capability to monitor all use of the internet and intranet and retains logs of all use. The reason

that monitoring takes place is to ensure compliance with legislation and the standards and rules set by the Council. We record and 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).

9.2 The Council has the capability to monitor, log and retain email correspondence. Any email and internet traffic being sent or received through the Council system will be scanned for potential viruses.

10. Complying with legislation

10.1 The following is a summary of areas to be aware of:

a. 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 Governance has copies of all of the Council's Data Protection registrations and can give Members advice if necessary.

b. 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. The 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.

c. Harassment – The Protection from Harassment Act 1997 covers harassment either by using email 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 email is that, written communication can be misinterpreted and offence may be caused where none was intended.

d. 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.

e. 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 emails a libellous or false email 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 email 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 email or an attachment, which you would not put in a normal letter on Council headed paper. Treat email as you would a postcard going through the open post.

f. 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 who 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. Members must be aware of these issues and make sure that the Council has correct licences for any software used.

g. Contracts – Electronic communication, such as email, 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.

h. 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. Points of Contact

11.1 The ICT Service Desk is the first point of contact for all ICT enquiries, queries and support problems. Calls can be logged via the ICT Self Service Portal icon that you will see on your CYC desktop or by telephoning 01904 552222.

11.2 Further assistance on the issues covered in this protocol may be obtained from the Council's Monitoring Officer or the Council's Head of ICT, or by consulting the ICT Policies page on the Council's Intranet website.