APPENDIX A

ELECTED MEMBERS ICT POLICY

1. Introduction

1.1 The City of Lincoln Council promotes the effective use of ICT (Information Communication Technology) by its Elected Members. The implementation of more effective ICT for Members will assist the execution of their duties and help to provide improved community leadership.

1.2 This policy applies to all Elected Members of the Council and aims to protect Members and the Council against legal challenge, criminal liability and damage to reputation. This is supported by four key objectives, which are;

i) To prevent Council resources from being used to promote political activity;

ii) To prevent the Council's name from being used to promote a Members personal or business interests;

iii) To protect the Council's private, personal and sensitive information from all threats, whether internal or external, deliberate or accidental;

iv) To prevent unnecessary cost being incurred by the Council.

1.3 The use of all ICT equipment or systems provided, or made accessible, by the Council is subject to this policy. Any Member wishing to use the Council's ICT equipment and systems is required to undertake in writing that they observe and will comply with this policy.

1.4 ICT services and support are provided for Members through the Business Development and IT Team.

2. ICT Points of Contact

2.1 The IT helpdesk is the first point of contact for all ICT enquires, queries and support problems.

Operating hours:	Monday –Thursday	08:00 – 17:00
	Friday	08:00 – 16:30

Contact Details	Tel: 01522 873327
	Email: ithelpdesk@lincoln.gov.uk

To order consumables or reimbursement please contact Legal & Democratic Services.

For all other ICT issues or concerns, please contact:

Matt Smith, Business Development & IT Manager
Tel: 01522 873308
Email: matt.smith@lincoln.gov.uk

3. ICT Equipment

Hardware

3.1 Members may choose to either use their own ICT equipment or take advantage of council provided hardware.

Council Issued Hardware

3.2.1 The following choice of Council provided devices for accessing systems are available to Members;

i) Desktop PC (complete with monitor, keyboard, mouse), or;

ii) Laptop

Both of which will be encrypted and will require a password to be entered when the device is turned on.

Due to advances in technology alternative hardware may become available for use by Members, the Council retains the right to offer alternative hardware to those shown above should the situation arise.

3.2.2 As optional extras the following items can also be provided:

i) Monochrome laser printer

ii) Consumables (there will be a limit on usage reimbursed or provided)

3.2.3 The devices provided by the IT Section will be installed with the current standard security software that will be configured to regularly update virus and malware definitions. In order for these updates to occur Members should ensure that they regularly connect to the Council's network or that they submit their device to the IT Section on a regular basis.

3.2.4 The software and ICT equipment will be installed in the Members home at the Council's expense. The Member will be expected to provide sufficient room for the equipment, sufficient power sockets and an internet connection in the immediate vicinity.

3.2.5 The software and ICT equipment will be maintained, replaced and repaired as necessary at the Council's expense. This includes office consumables such as printer cartridges and paper, with a limit on usage.

Member's own hardware or any other device

3.3.1 Members may choose to provide their own ICT equipment e.g. desktop PC, laptop and printer. However they should be aware that only ICT equipment and software supplied by the Council will be supported. If non-Council equipment is used then the Council will not provide repairs, maintenance etc.

3.3.2 A Member could also use a computer provided to them by their employer to access the Council's systems if they wish, subject to the employer's agreement and appropriate security being in place.

3.3.3 For those Members who wish to provide their own ICT equipment a flat rate annual allowance will be made available to allow for the depreciation of the equipment and eventual replacement thereof.

3.3.4 The Council reserves the right to only allow certain types of computer, for example, devices other than relatively recent PC's/laptops running Windows operating systems are unlikely to be acceptable.

3.3.5 Where a Member accesses the Council's systems from a non Council provided device they must ensure that the device being used to access the Council's systems has appropriate security software installed and that this software has been regularly updated, in line with the Council's Mobile Working and IT Security Policies.

3.3.6 In order to access the Council's systems from a Member's own device or any other device that device will need to be configured with software provided by the IT Section.

3.3.7 When using their own device Member's are still entitled to be provided with or reimbursed for office consumables such as printer cartridges and paper, however there will be a limit on usage.

Access to Systems

3.4.1 When using their own device Members will be required to access the Council's systems via the Citrix Access Portal. This will require a two-stage process for logging into the Citrix session, firstly using their Windows username and password and secondly with a text message code delivered to a mobile phone.

3.4.2 Access to the Council's systems using a Council issued device will in the first instance be via a Virtual Private Network (VPN) connection. Members will then have a choice whether to access the systems via the Citrix Access Portal as per 3.4.1 or alternatively all applications can be installed on the device and it can be operated on a standalone basis (FAT Client). This choice of options is likely to be determined by the mobility requirements of the Member.

3.4.3 Members should be aware that if they choose to utilise their Council owned device as a FAT client device that the support provided by the IT Section will not be able to be provided on a remote basis and will require the device to be returned to the IT Section in order to resolve on issues that may occur.

3.4.4 It is not possible to store documents on the hard drive of the computer (locally) when logging on via a Citrix connection, neither using a Council supplied or own device. Members will be provided with a personal network drive and any data stored here will be secure and backed up.

3.4.5 Any information that is held locally on a Council supplied or Member's own equipment, outside of the Citrix session, will not be backed up and Members are advised to back up any such personal data. The Council accepts no liability or responsibility for the loss of any such data.

Broadband Provision

3.5.1 Members may choose to either use their own broadband provision or take advantage of a council managed and funded broadband service either via mobile broadband (data card), wireless or standard Ethernet cable.

3.5.2 Regardless of the option chosen for broadband provision, wherever a Council device is supplied a Remote Access Point (RAP) will be required; this will be provided by the Council.

3.5.3 For those Members who wish to use their own broadband provision a flat rate allowance per annum will be made available, reflecting the costs of equivalent council provision. Any wireless router to be used for the broadband provision must also be supplied by the Member.

3.5.4 For those Members who take advantage of a council supplied broadband, this will only be available where it is provisioned upon a telephone line (installed and paid for at the Council's expense), separate from any existing personal fixed telephony provision. The Council will provide any wireless router required should they provide and manage the broadband service.

3.5.5 Private usage of a Council managed and provided broadband service is permissible however Members should be aware that in certain circumstances the private usage of a Council provided broadband service may be subject to a personal taxation charge. Guidance can be found at www.hmrc.gov.uk.

3.5.6 The Council will not support or be responsible for any other device connected to a wireless router regardless of whether the router is supplied by the Council or an own device.

4. Training/Development

4.1 The Council will provide training opportunities at the Council's expense on all aspects of Council related use of the software/hardware and related issues, such as Data Protection.

5. Acceptable Use

5.1 Council ICT equipment is provided for Members to use in connection with Council business.

5.2 Council business means matters relating to a Member's duties as an elected councillor, as an Executive member, as a member of a committee, sub committee, working party or as a Council representative on another body or organisation.

5.3 Council ICT equipment is available to enable;

i) Communications with individual Members of the public, other Members, officers, and government officials in connection with those duties set out above.

ii) To facilitate discussion by a political group of the Council, so long as it relates mainly to the work of the Council and not the political party.

5.4 Members must also note the General Principles in the Members Code of Conduct with particular regard to the following principles;

i) Members should uphold the law, and on all occasions act in accordance with trust that public is entitled to place in them;

ii) Members should do whatever they are able to do to ensure that their Authorities use their resources prudently and in accordance with the law.

5.5 ICT equipment should not be used;

i) In a manner that breaches the Members Code of Conduct. The Code makes it clear that when using the resources of the Council Members must;

a. Act in accordance with the Council's reasonable requirements;

b. Ensure that such resources are not used improperly for political purposes (including party political purposes).

ii) This means that the use of the ICT equipment for purely party political purposes, designing and distributing party political material produced for publicity purposed and support of any political party or group activities, elections and campaigning is likely to amount to a breach of the Code of Conduct.

iii) For any illegal activities which may bring the Council into disrepute.

iv) For any purpose which is inconsistence with this policy.

5.6 The following do not constitute Council business and Council resources should not be used;

i) Communications for constituency party meetings, ward party meeting, etc. or letters to party member collectively or in their capacity as party Members.

ii) Documents relating to the policy and organisation of political parties, particularly regarding the conduct of elections.

5.7 The ICT equipment provided for Members is intended to assist the Member in his or her duties as a councillor. It can be used for limited personal use if this does not degrade the performance of the equipment or contravene section 1.2 of this policy, providing that the primary use of the equipment remains for conducting council business. However, the equipment is limited to software provided by the Council.

5.8 All of the ICT equipment and software provided to Members remains the property of the Council. Members therefore have an obligation to ensure that they;

i) take reasonable care to safeguard ICT equipment and software supplied;

ii) follow the instructions given by the Council, authorised contractors and manufacturers of the equipment as to its use and not allow it to be interfered with;

iii) protect ICT equipment against theft and unauthorised access;

iv) do not install any software on the ICT equipment. If Members require any software for their work, they must consult the IT Section;

v) do not modify your ICT equipment in any way; this includes any amendments to the hardware and software configuration;

vi) maintain the ICT equipment in working condition and report any faults to the IT Section as soon as is reasonably practical;

vii) allow reasonable access to the equipment for regular inspection, maintenance, upgrades or remedial work. The Council is required by legislation to inspect any provided device at least once within a 12 month period;

viii) otherwise comply with the terms of this policy and any other Information Management Policy and IT Security Policy.

6. IT Security Policy

6.1 It is necessary that Members comply with and have a working understanding of the Council's IT Security Policy and supporting guidance notes, which apply to all ICT equipment and systems.

6.2 The key elements of the IT Security Policy and supporting guidance notes are detailed in the following sections.

Email and Internet Acceptable Usage Guidance Notes

6.3.1 Email and Internet is provided to Members as a means of improving communications, knowledge and effectiveness at work. The Council's email and Internet facilities are intended for business use, although occasional personal use is permitted. Nevertheless, all usage of the Council's email and Internet facilities must be regarded as the property of the Council and must not be regarded as private.

6.3.2 Use of email and Internet access introduces security threats such as malicious code attached e.g. viruses, unsolicited or undesirable email, fraudulent attempts to acquire sensitive information such as passwords and credit card details, unauthorised content, and breaches of legislation e.g. computer misuse and copyright legislation. All Members are responsible for complying with the Council's Email and Internet Acceptable Use Guidance.

6.3.3 The Council will provide Members with a Council email address in the format "name@lincoln.gov.uk", this must used for all emails conducting or in support of official City of Lincoln Council business.

6.3.4 Non work emails e.g. webmail, hotmail, must not be used to conduct or support official City of Lincoln Council business, these forms of email will not be supported by the Council and will access to them will not be available through Council provided channels.

6.3.5 Members must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email. If Members believe they need to do this they should contact the IT Helpdesk.

6.3.6 No forwarding of emails to personal email addresses will be permitted, either automatic or manual forwarding by officers or Members.

6.3.7 The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official City of Lincoln Council business should be considered to be an official communication from the Council.

6.3.8 All official external e-mail must carry the official Council disclaimer. The disclaimer below is the current standard approved by the Council and is automatically added to outbound emails;

This transmission is intended for the named addressee(s) only and may contain sensitive or protectively marked material up to RESTRICTED and should be handled accordingly. Unless you are the named addressee (or authorised to receive it for the addressee) you may not copy or use it, or disclose it to anyone else. If you have received this transmission in error please notify the sender immediately. All GCSX traffic may be subject to recording and/or monitoring in accordance with relevant legislation.

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Under the Data Protection Act 1998 and the Freedom of Information Act 2000 the contents of this email may be disclosed. The City of Lincoln Council reserves the right to monitor both sent and received emails. If you have received this email in error please notify the system manager who can be contacted at ITHelpdesk@lincoln.gov.uk"

6.3.9 Under no circumstances should Members use email and Internet facilities for;

i) Illegal or malicious use, including downloading or transmitting copyright material

ii) Accessing, sorting or transferring illegal, pornographic or obscene material

iii) The deliberate propagation of computer viruses, or use of the Internet to attempt unauthorised access to any other IT resource.

iv) Access to or distribution of material, which does not comply with the Council's Equality and Diversity policy.

v) For potentially libellous or defamatory purposes.

6.3.10 Access to certain categories of website will be restricted e.g. adult, drugs & alcohol, gambling etc (if access to a blocked site is required this can be overridden by contacting the IT helpdesk), subject to the site being used for appropriate Council business.

6.3.11 Members must be aware that the Council reserves the right to use monitoring tools to enforce the Council's policies and to produce periodic reports detailing use of its E-mail and Internet facilities.

Information Security Incident Management Guidance Note

6.4.1 An incident is an event that could cause damage to the Council's reputation, service delivery or even an individual. This could be a lost laptop or paper case file, a virus on the network or a damaged piece of hardware.

6.4.2 Members should report any incidents or suspected incidents immediately by contacting the IT Section.

6.4.3 Members need to keep evidence of security breaches or system incidents, in case these are required later.

6.4.4 This process also applies to lost paper records as well as data on computers.

Software Guidance Note

6.5.1 Members must not install or configure any software on the Council's ICT equipment. If Members require any software for their work, they must consult the IT Helpdesk.

6.5.2 All standard software installed on Council issued ICT equipment is correctly licensed and the Council will hold the details and records. These licenses apply to a single copy of the software on one machine. The software must not be copied to any other machine.

IT Access Guidance Note

6.6 The security of ICT equipment is the responsibility of each Member as its 'custodian'. Access to the Council's information systems via ICT equipment is subject to password security. Members must ensure that no one other than themselves is given access to those council information systems and must take all reasonable steps to ensure their password remains confidential.

Removable Media Guidance Note

6.7.1 It is the Council's policy to prohibit the use of all removable media devices. Removable media devices are electronic items usually used fr storing or transporting data, for example a computer disk (CD or DVD),

USB memory stick, MP3 player, external hard drive or a camera memory card. The use of removable media devices will only be approved if there is a valid business case for its use.

6.7.2 All data stored on removable media must be encrypted where possible.

6.7.3 Any removable media device that has not been supplied by the IT Section must not be used. All ICT equipment supplied will by default have removable media facilities disabled unless there is a valid business case.

Legal Responsibilities Guidance Note

The Data Protection Act

6.8.1 The Data Protection Act (DPA), 1998 is concerned with the direct use of personal information, whether that information is a manual record or processed on a computer system. DPA applies to all types of personal information; this includes information which may not be thought to be confidential.

6.8.2 Personal data means data that relates to a living individual who can be identified from that data, or a combination of that data and other information which is in the possession of the Council. It also includes any expression of opinion about the individual.

6.8.3 The Act itself has 8 principles, all of which must be adhered to when handling personal information. Although all of the principles apply to information security, principle 7 focuses solely on the security aspect of handling personal information.

6.8.4 Members usually access the personal data of others in three different situations:

i) Viewing personal information held by the Council for a specific purpose, such as a tenancy file.

ii) Viewing and storing the personal information of their constituents through surgeries or complaints.

iii) Viewing personal information held by their political parties about Members.

6.8.5 Members should ensure that personal information held for council purposes should not be used for political or electioneering purposes.

6.8.6 Members should also be aware that the unauthorised processing or disclosure of such information is prohibited under the Act and the Member is responsible for ensuring that there is no such unauthorised disclosure of information from the ICT equipment.

6.8.7 If the Council fails to abide by DPA, it could be prosecuted and fined up to £500,000. However, the Act also imposes personal liability, so if a Member is found to be contravening the Act, he/she too could be prosecuted. In addition both the Council or individual officers or Members could face a civil action for damages for distress if there is a breach of the DPA.

6.8.8 All Members must comply with DPA, and the Council's supporting DPA policies, procedures and guidelines. It is the Member's responsibility to be familiar with and to adhere to the requirements of DPA.

6.8.9 Members are advised to read the Information Commissioner's *Advice for the elected and prospective members of local authorities* for further details:
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/advice_elected_and_prospective_members_local_authorities.pdf.pdf

The Freedom of Information Act

6.9.1 The Freedom of Information Act (FOIA) gives a right of public access to information held by the Council. In terms of the Freedom of Information Act:

i) Individual Members are not authorities for the purposes of the FOIA.

ii) Correspondence between Members or information held by a Member for their own private, political or representative purposes will not usually be covered by the Act.

iii) Information received, created or held by a Member on behalf of the Council will be covered by the Act, for example, where a Member is acting in an executive role as part of the Council Executive.

iv) Information created or received by a Member, but held on a council's computer system or at its premises will only be covered by the Act if it is held for the council's own business.

v) Members are advised to read the Information Commissioner's *Information produced or received by councillors* for guidance on what information held or produced by Members can be requested and disclosed under the Freedom of Information Act. http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/fep109_information_produced_or_received_by_councillors_v1.0.pdf.

6.9.2 If Members require advice or assistance on the provisions of the Data Protection Act or the Freedom of Information Act they should contact Legal & Democratic Services Manager or Head of Corporate Support Services.

7. Health and Safety

7.1 Members are required to ensure they use all facilities with due regard to their own and others' health and safety. Members should be aware of how they position their equipment to minimize hazards such as trailing power cables, glare for lighting or posture when working. Members should contact Legal & Democratic Services for arrange further advice regarding best practice for health and safety.

8. Insurance

8.1 A proportion of the cost of replacement following theft or damage of the Council's ICT equipment is covered under the Council's current insurance arrangements. There is an expectation from the insurer that reasonable care is taken in the use and security of equipment, particularly portable laptops, failure to do so may invalidate any insurance claim. The Council may, at its discretion, require the Member to pay all or some of the cost incurred, if it resulted from their wilful neglect.

i) Security – reasonable care must be exercised in order to prevent theft, loss or damage at all times. Specifically any mobile devices, e.g. laptops must not be left unattended. An appropriate carrying case should be used to prevent damage to the equipment. All ICT equipment should be kept out of sight overnight in secure location.

ii) Transit – ICT equipment must be kept out of sight and secured in a locked boot where available. ICT equipment must not be left in an unattended vehicle and must be removed from the vehicle overnight. When using hotel accommodation Members should consider the use of the hotel reception safe when a mobile device is not in use and where not available, the use of a room safe or lockable cabinets within the room.

iii) Travelling abroad – it is not envisaged that there will be a regular requirement to take Council provide mobile devices abroad. In such cased mobile devices must be taken as hand luggage. Legal & Democratic Services should be advised, in good time, prior to oversees travel in order to ensure insurance arrangements are in place. Members should also consult the Foreign and Commonwealth Office (http://www.fco.gov.uk/en/travel-and-living-abroad/) website for further guidance prior to travel.

8.2 The Council accepts no responsibility for the theft or damage of the Members own ICT equipment and Members should ensure that they have their own appropriate insurance arrangements in place.

9. Privacy

9.1 It is the policy of the Council that email and internet use may be monitored. Inappropriate use or content will be bought to the attention of the Monitoring Officer and may result in a referral to the Standards Committee. The Council reserves the right to inspect the equipment at any time. Members are required to give Council officers access at any reasonable time for inspection and audit, which may be undertaken remotely and without notice to the Member.

9.2 Any inappropriate use made of Council ICT equipment will be considered to have been made with the knowledge and co-operation of its custodian.

9.3 All incoming and outgoing data (both internet and email) is automatically monitored and filtered. Any suspect traffic is quarantined and IT services notified of the sender and intended recipient.

10. Confidentiality

10.1 Members may be able to access confidential council information using the ICT equipment and are responsible for ensuring the continuing security of any such confidential information that they receive, including the security of any storage of such information on the computer.

10.2 Members are reminded of their obligations under the Council's Code of Conduct for Members not to disclose confidential information to any third party.

11. Restriction of Use

11.1 The Council reserves the right to restrict the use of ICT equipment if it has reason to believe that the use of the ICT equipment is likely to be in breach of the Council's IT Security Policy and supporting guidance. In particular, the Council reserves the right to:

i) remove or disable any software or equipment;

ii) remove any information stored on the computer.

12. Return and Recovery of Equipment

12.1 All ICT equipment and software assigned remains the property of the Council. The Council reserves the right to require the Member to return the ICT equipment at any time and the right to recover the ICT equipment from the Member.

12.2 Any Member to whom ICT equipment has been supplied and ceased to hold office, for whatever reason, will be required to return it all to Legal & Democratic Services within two weeks of ceasing office. All information held on the equipment will be deleted and the equipment maybe re-issued

MEMBERS AGREEMENT

I, Councillor……., have read and understood the Members ICT Policy as set out above and hereby agree to comply with the terms of the policy.

Signed……..

Date…….

In the presence of…… (Officer of City of Lincoln Council)

Signed……..