ICT Access for Members Protocol

September 2011

Document Control

Organisation	Newcastle-under-Lyme Borough Council
Title	NULBC Members ICT Provision Policy
Author	J Hilton, D Elkington
Filename	"\\svfs1\ICT Dept\Procedures and Policies\Policies\
Owner	Head of Customer & ICT Services
Subject	Provision of ICT to elected members
Protective Marking	None required
Review date	September 2012

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Executive Management Team		
Head of Central Services		

Document Distribution

This document will be distributed to:

All Members
All ICT Staff

Contents

1. **Protocol Statement**

    Technology is used in every aspect of council business to improve efficiency and effectiveness and to provide facilities that are more accessible and understandable by the public who use them. Councillors are on the front line of local public service provision; there is an expectation by the public and council that elected members are confident and adept in the use of ICT (Information and Communication Technology); be it email, web or utilising software. To that end ICT Services will provide a number of ways in which to help and support members in getting the most out of ICT.

2. **Purpose**

    The purpose of the Protocol is to ensure that members have adequate access to ICT equipment and services to allow them to carry out their duties.

    This document describes the core services that ICT Services will provide for members in order to ensure that they can better use technology to serve their constituents safely, securely and efficiently.

3. **Scope**

    The Protocol applies to all Newcastle-under-Lyme Borough Council (NULBC) elected Members and ICT staff. All elected members and ICT staff must comply with the requirements of the Protocol.

4. **Provision of Services**

    ➢ *Secure Access to email*
    Each member is automatically issued with a secure @newcastle-staffs.gov.uk email address upon election. This address will be the only email contact listed on the Authorities' website. It is expected that as email becomes an increasingly important part of everyday communications for a growing proportion of the population, all members will be expected to use email as a method of communication.

    Each member's mailbox is limited to 700mb in line with the Council's

4

adopted mailbox policy[1]. When a mailbox is nearing the size limit, a warning email will appear. Upon reaching the maximum mailbox size, the member will be able to receive but not send emails until such time as the mailbox size decreases below 700mb. Guidance on how to manage your mailbox is available from ICT Services.

It is also anticipated that Members Services will have an active role in ensuring that email good practice guidelines are adhered to as part of member training and development.

ICT Services will provide secure access to email using the member's dedicated website, directly from corporate PCs, members own pcs or, where appropriate, using other remote access technology.

➢   *Member's Dedicated Website*
NULBC provides a dedicated website designed for members use. This area is restricted through the use of a secure certificate, which is issued to new members after election. Access to the site will also be provided using other means, such as secure remote access technology,

Members are encouraged to use the site as their main source of NULBC information. Members can also gain secure access to their email through the site. The site also contains a notice board, highlight information and committee reports, agendas, the forward plan and meeting schedules created using the modern.gov software. [2]

ICT and Member Services will continue to develop this site in order to ensure that important information continues to be delivered to support members. In the future, access to Geographic Information Systems (GIS), the capability to log service requests for customers and the ability to send SMS text messages directly to members of the public will be added.

---

[1] Microsoft Outlook – Mailbox Policy July 2011

[2] modern.gov is a computer system that is used by democratic services to manage forward plans, agendas, minutes, and decisions, and publishes to the Intranet and Internet.

> *Alternative Access Methods*

The default method of providing access to Council services will be through the members' website. This is provided using a secure certificate which restricts access to dedicated devices.

It is recognised that this may not be appropriate for all members, who may have to work from different locations, using different devices. Access will therefore be provided through one of the following methods:

    i. Reusable IT equipment
   ii. Councillor's own equipment

Links to, and the use of, mobile devices (e.g. smartphones) is under review.

Member Services and ICT will also offer guidance on how to ensure that information remains safe and how "footprints" left on devices can be easily removed.

> *Printing Facilities*

ICT recognises the importance of providing members with access to printing services. This will be done using the Authority's Multi-Functional printers and scanners (MFDs). This removes the need for dedicated printers for members use.

These devices will allow members to print their work, including confidential items, and then collect them from any printer at the Civic Offices, Guildhall or Kidsgrove Customer Service Centres. Printing can also be facilitated through arrangements with Member Services.

Work which is un-printed after 7 days is automatically deleted. Printed materials for collection which are confidential should be indicated as such to Member Services.

Members will be issued with a tag which uniquely identifies them to the printer and ensures they have access to their printed work. This tag will form part of their ID card and is completely invisible.

The Council's printing policy will also apply to any members who choose to use the printing facilities and full training will be provided in conjunction with Member Services.

A multifunction printer (MFD) will be located in the members' room on the 1st floor for your convenience.

➢   *Scanning Facilities*

As part of the drive towards greater efficiency, the Council is committed to increasing the use of electronic document scanning and storage; ensuring that all documents are scanned and stored electronically whenever possible. This has the advantages of avoiding excessive storage costs, the convenience of electronic filing, enabling greater flexible/mobile working, ensuring documents are not lost in a disaster recovery situation and the ability to benefit from the speed of email when a traditional paper document is received.

Members will be provided with access to document scanning services on both an ad-hoc and continual basis. This will be facilitated through the use of the authority's multifunction printers (MFDs).

Where appropriate, members will be offered the opportunity to have any post received for them at the Civic Offices securely scanned and emailed to their @newcastle-staffs.gov.uk email address, giving instant access to the document. Once scanned, members will be able to choose between having the document dispatched with the regular courier service, or after a set period of time, securely destroyed. Where scanning would be inappropriate, such documents will remain available for collection from the Customer Support Office or distributed by the Courier Service.

If members need to scan ad-hoc documents, this can be done using the Council's multifunctional devices (MFDs). Members can scan documents and have them sent back to their own email address to take appropriate action or store securely.

Scanning will be supported by both ICT and Member Services.

➢ *Reusable IT equipment*

Where members are unable to provide their own ICT equipment such as a laptop or PC for use in connection with their council business, ICT Services will provide a suitable PC for the duration of the member's term or until they procure suitable equipment of their own.

The equipment will be a desktop PC with 17" flat screen monitor, keyboard and mouse. The equipment will be from ICT stock of a suitable specification and quality, and will include Microsoft Office. ICT Services will support this equipment for the duration should members experience any difficulties.

The equipment will be configured such that members are not at risk of losing data if the device is stolen or lost.

Members may also request the use of Council projectors, screens or other suitable equipment for Council business. This should be arranged through Member Services.

➢ *Remotely Accessible PCs*

Where members provide their own ICT equipment such as a laptop or PC for use in connection with their council business, ICT will provide the use of a Council PC at the Civic Offices which the member's pc will connect to. This is termed as a Remotely Accessible PC.

This remotely accessed PC will have a full suite of applications such as Microsoft Office and will be part of the Councils secure network. Documents and emails created on the PC will be stored on the Council's servers.

Remotely Accessed PCs will require the use of an additional small hardware device called an Identification Token. This will identify you as a valid user of the Councils systems and allow access.

Additionally, members can request a Secure Memory Stick. This will enable the easy transfer of documents etc, and will be password protected. This will ensure that if the memory stick is lost, the information contained on it cannot be accessed by anyone finding it.

These items will be provided to members in the first instance. Loss of either of these items will incur replacement costs totalling the purchase and yearly support costs of the item, chargeable to the member.

➢ *Training and Support*

ICT in conjunction with Member Services will support:

- The members secure website
- Remote access through each members chosen method
- Secure certificate issuing and use
- Reusable IT equipment
- Remotely Accessed PCs
- Printing / scanning in relation to the council's multifunctional devices.
- Secure memory sticks.
- Outlook Web Access Issues

ICT Services will provide training in the effective use of the specific ICT equipment and software listed above. ICT services will also provide signposting to suitable courses provided through the STeP gateway or external providers, such as Newcastle College or Learning Direct Member Services will provide specific training to new members with support from ICT as required. This will be part of the new Members Induction Programme.

5. **Services which NULBC will not provide**

➢ *Email Forwarding*

Email forwarding cannot be provided automatically by ICT Services due to the security implications in doing so. ICT Services provide a secure email account for each member, remotely accessible through a variety of methods. NULBC does not support automated email forwarding from members @newcastle-staffs.gov.uk email accounts to other external providers.

Whilst we will not prevent members from forwarding emails, should they so choose. In order to do this a member will be required to agree a disclaimer, indemnifying NULBC from any consequences associated with the practice.

> *Individual Printers*

NULBC will not provide individual printers or printing supplies for members or groups.

All members and groups will be expected to comply with NULBCs printing policies using the authorities centralised printing functions.

> Support for non-Council devices

Due to the complexity and variety in the IT equipment market, ICT will not provide support for any hardware or software which is not Council issued.

> *Software for use on non-Council devices*

NULBC will not provide software such as Microsoft Office for use on individual members PCs. If members require access to products such as Microsoft Office, this will be facilitated through access to a loan PC or remotely accessible Council PC.

> *Mobile Devices*

NULBC does not currently provide mobile devices such as Blackberry's iPhones, PDA's, etc. However, as the use of ICT by members evolves, this is likely to be reviewed.

ICT services will also not currently support access to the Council's services using members own mobile devices.

> *Broadband / Wi-Fi*

NULBC will not provide or support member's private broadband connections or Wi-Fi access points.

6.   **Registration with the Information Commissioners Office**

The information Commissioners Office (ICO) has recently published guidance for members of local authorities, with regards to their obligations under the Data Protection Act.

In summary, the ICO recommends that if you handle personal information, you may need to register as a data controller with the ICO.

Notification is a statutory requirement and every organisation that processes personal information must notify the ICO, unless they are exempt. Failure to notify is a criminal offence.

Registration with the ICO incurs a £35.00 annual fee.

There is a dedicated section on the ICO website http://www.ico.gov.uk/ titled: Do I need to notify and how do I maintain my register entry? . Members can visit this site for further clarification. Members can also take part in an on-line self-assessment.

NULBC recommends that all members who process constituency casework electronically register with the ICO.

7.   **Remuneration**

ICT and Members Services will be recommending to the Independent Remuneration Panel that whilst discussing future member's allowances, consideration is given to the need for ICT equipment.

8.   **Individual Responsibilities**

All members should be aware of and comply with the principals of the Data Protection Act.

Members are responsible for ensuring the safekeeping of all ICT equipment loaned to them, during the period of the loan. This includes software and hardware.

Members will also be required to attend any mandatory ICT awareness sessions such as information security principles, email and internet usage, etc.

9.   **Risks**

The Council recognises that there are risks associated in providing external access to its network.

The Protocol aims to mitigate the following risks:

11

1   Insecure access to members email;
2   Inadequate ICT provision to members;
3   Uncontrolled use of ICT services or equipment;
4   Risk of non-compliance with legislation such as Data Protection Act, and storing information other than in accordance with agreed retention and disposal schedules - resulting in financial penalty and loss of reputation.

Non-compliance with the Protocol could have a significant effect on the efficient operations of the Council and may result in financial loss and an inability to provide necessary services to its customers.

10.   Protocol Compliance

Protocol compliance will be monitored by ICT and Member Services.

If members do not understand the implications of this Protocol or how it may apply to you, please seek advice from the Head of Customer & ICT Services or Member Services.

11.   Policy Governance

The following table identifies who within the Council is Accountable, Responsible, Informed or Consulted with regards to this Protocol The following definitions apply:

1   **Responsible** – the person(s) responsible for developing and implementing the Protocol.
2   **Accountable** – the person who has ultimate accountability and authority for the Protocol.
3   **Consulted** – the person(s) or groups to be consulted prior to final implementation or amendment.
4   **Informed** – the person(s) or groups to be informed after implementation or amendment.

Responsible	ICT Operations and Development Manager
Accountable	Head of Customer & ICT Services
Consulted	EMT, Member Services, Portfolio Holder for Resources & Efficiency
Informed	Head of Central Services, ICT Staff

12.   Policy Commencement

The recommended start date for the Protocol will be **1 December 2011**. This will allow time for staff and members to adopt the principles and make the necessary arrangements.

13.   Review and Revision

The Protocol will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Protocol review will be undertaken by the Information Security Group and the Member Development Working Group