

Part 8 Codes and Protocols

8.7 Protocol on Use of Council Resources and Support for Members

Introduction

The Council does not have the power to provide resources, including Officers, other than use for Council business. It does not have the power to provide resources for political¹ purposes.

Council business relates to a Member's duties as an elected Ward Councillor, a Cabinet Member, as a member of a committee, sub-committee or working party/task group or as a Council representative on another body.

The Council's resources include:

1. any equipment,
2. office/premises or stationery, and
3. the Council's Officers.

Special rules² apply to the use of the Council's resources in relation to publicity. The Council is not able to publish or arrange for the publication of party political material.

¹ The Oxford English Dictionary (OED) defines politics and politicking – to engage in political activity especially in order to strike political bargains or seek votes. The OED also defines political – to belong to or take a side of an individual, organisation etc; supporting particular ideas, principles or commitments in politics; relating to, affecting or acting according to, the interests of status or authority in an organisation etc, rather than matters of principle.

² Section 2 of the Local Government Act 1986 provides that:

- (1) A local authority shall not publish or *arrange for the publication of*, any material which, in whole or in part, appears to be designed to affect public support for a political party.
- (2) In determining whether material falls within the prohibition regard shall be had to the content and style of the material, the time and other circumstances of publication and the likely effect on those to whom it is directed and, in particular, to the following matters:
 - a. Whether the material refers to a political party or to persons identified with a political party or promotes or opposes a point of view on a question of political controversy which is identifiable as the view of one political party and not of another;
 - b. Where the material is part of a campaign, the effect which the campaign appears to be designed to achieve.
- (3) A local authority shall not give financial or other assistance to a person for the publication of material which the authority are prohibited by this section from publishing themselves.

Section 2 applies to all publicity produced by the Council but by Section 2(3) (in italics above) is applicable to the support provided to Members in relation to the materials/newsletters that Members produce.

Publicity is defined as ‘any communication in whatever form addressed to the public at large or to a section of the public’. This definition therefore includes press releases, ward bulletins and letters to the media etc but does not include letters to individuals, unless this was on a scale which could constitute ‘a section of the public’.

General Principles for the use of Council Resources

There are a number of general principles that are applicable irrespective of the type of Council resource that is being utilised:

- Council resources may only be used in accordance with the Council’s Code of Conduct for Members³, this protocol and the law;
- The use of the Council’s resources must always be able to be justified;
- Apply common sense – it is likely to be a good barometer of what is likely to be acceptable and what is not; and
- If you are concerned always seek advice particularly where use could be considered to be on the margins of what is acceptable.

Further information in relation to the use of the Council’s resources can be found in the guidance note issued to support this protocol.

Main resources available to Members:

1. The Customer and Members Services Team

1.1 The Customer and Members Services team (CMS) provides a dedicated service for Members making enquiries on behalf of a constituent or organisation. Members are allocated support from a particular Officer who should be their first point of contact. The Council also has a computerised Members’ enquiries system through which enquiries on various issues are referred to service areas for response within particular predetermined time scales.

1.2 The CMS Officer’s role includes:

- a) the provision of certain support services to help Members in carrying out their roles. The support services they provide include carrying out research, providing information, administrative support, and making travel and conference arrangements;
- b) support in ward work including arranging Members’ surgeries, including hiring premises, producing booklets and posters to advertise the surgeries. CMS Officers cannot provide support for any party political work;
- c) acting as a contact point for Members’ general enquiries; and
- d) maintaining the Members’ enquiries system.

³ The Council’s Code of Conduct for Members states that a Member must, when using or authorising the use by others of the resources of the Authority: “act in accordance with the Authority’s requirements”.

1.3 Officers from the CMS Team can only undertake work that relates to Council business. Where there is any concern in relation to requests for support and assistance that might be considered to be for political purposes this will be referred to the Monitoring Officer for determination.

2. Council Stationery, Printing/Photocopying and Mail

2.1 It is important to make sure that any stationery provided for Members to use when carrying out their duties as a Member (or a Member of Cabinet, a committee or sub-committee) including headed note paper is used only for those duties and not for other purposes.

2.2 Members are permitted to generally sign their correspondence using their name, their party group membership and their ward. Where a Member holds a particular office or position they may also use the appropriate title, specifically, Mayor, Cabinet Member, Group Leader, Chair or Deputy Chair of a particular committee where appropriate.

2.3 The copyright of photographs taken by the Council is owned by the Council. Such photographs may be used in Council publications and Members wishing to use the photographs may do so only with the agreement of the Council. To avoid concerns arising that the Council is providing resources for political publications, on occasions when photographs are provided by Members for use in Council publications such photographs must not subsequently be used by Members in other publications without the Council's consent.

2.4 Where Members produce a Ward newsletter for distribution, provided reference to the party group to which the a Member belongs is used only with their name and Ward on a single occasion in the newsletter and no other 'banner' reference to a political party is used it is permissible to include the Member's Council contact details (i.e. Council e mail address, mobile and land line numbers). In addition such a newsletter must not contain 'party political' or election campaign material.

3. Travelling and Subsistence Allowances

3.1 The Council has made provision for Members in its Members' Allowances Scheme for the payment of travelling and subsistence allowances to its Members, including any co-opted Members.

3.2 The Regulations that govern the payment of travelling and subsistence allowances provide that such allowances may be paid for the following only:

1. The attendance at a meeting of the Authority or of any Committee or Sub-Committee of the Authority, or of any other body to which the Authority makes appointments or nominations, or of any Committee or Sub-Committee of such a body.

2. The attendance at any other meeting, the holding of which is authorised by the Authority, or a Committee or Sub-Committee of the Authority, or a Joint Committee of the Authority and at least one other local authority within the meaning of section 270(1) of the Local Government Act 1972, or a Sub-Committee of such a Joint Committee provided that:
 - (i) where the Authority is divided into two or more political groups it is a meeting to which members of at least two such groups have been invited, or
 - (ii) if the Authority is not so divided, it is a meeting to which at least two members of the Authority have been invited.
- 3.3 The attendance at a meeting of any association of authorities of which the Authority is a member.
- 3.4 The attendance at a meeting of the executive or a meeting of any of its Committees, where the Authority is operating executive arrangements.
- 3.5 The performance of any duty in connection with the discharge of any function of the Authority conferred by or under any enactment and empowering or requiring the Authority to inspect or authorise the inspection of premises.
- 3.6 The performance of any duty in connection with arrangements made by the Authority for the attendance of pupils at any school approved for the purposes of Section 342 of the Education Act 1996 (approval of non-maintained Special Schools).
- 3.7 The carrying out of any other duty approved by the Authority, or any duty of a class so approved, for the purpose of, or in connection with, the discharge of the functions of the Authority or of any of its Committees or Sub-committees (other than political meetings), including:
 - the attendance at a meeting of a Working Group or Panel of the Authority.
 - the attendance at site visits and inspections.
 - the attendance at ward surgeries.
 - the attendance at meetings with tenants or community groups.
 - the attendance at meetings with officers.
 - the attendance at meetings as invited observers or attendees officially recognised as such in the official invitation list e.g. Citizenship Ceremonies, Civic Events, hospitality functions, exhibitions, open days or similar events.
 - the attendance at meetings in some other formal representational capacity e.g. at the specific request of local residents to represent their views.

- the attendance at formal or informal briefings/presentations about matters related to the functions and work of the Authority.
- the attendance at training events for Members arranged as part of the Member Development programme.

DRAFT

4. Data Protection Legislation

- 4.1 The legislation on data protection applies to everyone who processes, stores or uses personal information. It is important to be aware of its requirements and how it affects individual Members as not keeping to the act is a criminal offence, and it could also break the Code of Conduct for Members.
- 4.2 Members' responsibilities under the legislation flow from the usage that Members may make of the Council's systems in the discharge of their role as a Councillor. These responsibilities are covered by the Council's data protection registration in the same way as they apply to Council Officers. For this reason, it is important to keep to the Council's policies and procedures.
- 4.3 Members have additional responsibilities under the legislation in relation to any information they hold on their own systems concerning constituents. Members are required in relation to this information to register themselves with the Information Commissioner as data controllers. Advice in relation to registration with the Information Commissioner is available from the Monitoring Officer.
- 4.4 Members should note that where Council information is transferred outside the secure environment of the Council's ICT systems, for example by sending an email from a Member's Council email account to a private email account, the responsibility for the security of that information rests with the Member. In that regard Members should encrypt the information before it is released outside the Council's secure environment. Please also refer to section 6.6 of the ICT Security Policy regarding the use of email.
- 4.5 In order to safeguard against breaches of the legislation, Members should seek advice from the Monitoring Officer before disclosing confidential information. Generally personal information cannot be released without the consent of the person to whom it relates. Improper disclosure can put the Member and the Council at legal and financial risk.

5. Council Rooms

- 5.1 Members can use committee rooms and other rooms to help them carry out their duties (for example, to hold meetings with constituents) when they are available.

6. Information Technology and other Equipment

- 6.1 The Council provides ICT equipment for Members to help them carry out their duties more effectively and efficiently. The Council will provide support for Members in the operation of Council supplied equipment so that it can be used to the best effect. In general terms, a Member can use the equipment providing that it is used in line with the Information Computer Security policy. Members should note that the Council has an obligation to investigate misuse of Council supplied equipment. Indeed any criminal activity would require referral to the Police for investigation. Furthermore, the Council is required to supply

information requested under the Freedom of Information Act and the Data Protection Act that is held by the Council on its systems. If a request for information is submitted and it appears that information held on the Council's systems may be disclosable and is held by a Member, the Member will be advised in advance and requested to supply the information. Other information may be held by Officers that has been provided by Members and this may be disclosable subject to statutory exemptions. Members will be advised where any such disclosure is anticipated. Further information on the requirements of the Freedom of Information Act is provided in the guidance that supports this protocol.

6.2 Equipment supplied by the Council, which includes Council systems that a Member may access remotely via their own ICT equipment is not available for use for political purposes. The following sets out some basic guidance:

- The Council's equipment is for work relating to his/her duties as a Member. Use of the equipment is exclusive to the Member, it is not for use by other members of their household. Where Members share domestic arrangements joint use of the equipment is permitted. Sharing of user accounts is NOT permitted. Members should use the ICT equipment responsibly.
- Any use of ICT equipment must conform with the Council's Information Computer Security Policy – this can be found on the Council's Intranet using the following link:
http://november.northtyneside.gov.uk:7777/intra/security-policy/secpol_ver6.html
- ICT equipment is valuable. Members should act responsibly while equipment is in their possession to prevent loss or damage.
- Members should ensure that where ICT equipment is allowed to be used for personal purposes, all personal use is paid for in accordance with the Council's procedures.
- Each Member will be given a user code and password to allow access to computer facilities. These must not be disclosed to another person. The individual Member will be responsible for any consequences arising from the use of the code or password by another person.
- It is important to consider the effect of an e mail message, and be careful to avoid sending e mails which could be regarded as vulgar, abusive, sexist, racist, anonymous or likely to damage a person's reputation. If a Member sends any inappropriate e-mail the Council, may withdraw e-mail facilities.
- In relation to the above the Council's security software automatically monitors and examines material stored on its systems or sent across its networks.

- When using the computer facilities Members should be conscious of the fact that some information held on the computer systems is confidential and releasing it could lead to legal action being taken against the Member involved or the Council.
- Where Council information is transferred outside the secure environment of the Council's ICT systems, for example by sending an email from a Member's Council email account to an private email account, the responsibility for the security of that information rests with the Member. In that regard Members should encrypt the information before it is released outside the Council's secure environment. Please also refer to section 6.6 of the ICT Security Policy regarding the use of email.
- Members should ensure that where equipment such as mobile telephones are allowed to be used for personal purposes, all personal use is paid for in accordance with the Council's procedures.

6.3 ICT Equipment Options:

- Provision of access to Council computer systems via:
 - Thin Client Device, Monitor & Printer;
 - Thin laptop (no remote printing) & Anytime key-fob;
 - Anytime key-fob to use with own IT equipment;
 - Use of a device in Council premises.

6.4 It should be noted that the options for accessing the Council's computer systems remotely can be combined i.e. if you have a thin laptop you can also access the systems via your own equipment using the key-fob.

6.5 Access to council systems is through "Anytime Access" (sometimes referred to as "Citrix"). Anytime Access is a secure method of accessing the councils systems and also ensures that information and documents are stored in a safe and secure way, and that information is not stored on local drives, for example on personal computers. By using Anytime Access you are not restricted to a particular device, and this therefore enables flexibility to work at different locations. To use this Anytime Access a small piece of client software must be added to your internet browser, this is installed automatically on council provided equipment and can be downloaded for use on personal desktops and laptops. It is not permitted to add additional software to council provided equipment.

- Provision of a mobile phone:
 - Basic mobile phone
 - Smart Phone (PDA) - subject to available budget.

All of the above options can be demonstrated to Members via workshops.

ICT Support is provided by ICT Services. Contact details are as follows:

- ICT Help Desk – 0191 643 544
- Sending an email to ict.help@northtyneside.gov.uk – email must be sent from a council email address only.

6.7 The following sets out in table form details of the provision of ICT equipment. The first four columns relate to the provision of Council ICT equipment. The final column relates to the provision of a keyfob that provides remote access to the Council's systems via a Member's own ICT equipment.

6.8 Members should note that when using their own ICT equipment (which for these purposes includes programmes on Members' own equipment such as e mail) to undertake their own private business or political activities the restrictions detailed in this protocol and the Information Computer Security Policy do not apply. These restrictions and requirements only apply to a Member where they are accessing remotely the Council's system via a keyfob and are using their own ICT equipment.

DRAFT

Description	Thin Client solution	Thin Laptop solution	Access to kit in Council premises	PDA / Smart phone	Keyfob for accessing Council systems
(1) The equipment is the property of North Tyneside Council.	✓	✓	✓	✓	✓
(2) At the end of the period as an elected Member, the equipment is to be returned to the Council in full working condition.	✓	✓	✓	✓	✓
(3) The equipment must be installed by an ICT Officer of the Council.	✓		✓	✓	
(4) Members are required to undergo training provided by the Council in the use of equipment.	✓	✓	✓	✓	✓
(5) The services, including access to the internet and Email system, are provided for use as a Member only. However, personal use is permitted provided it does not conflict with official business, but political use is not permitted. Please refer to sections 06 (use of email) and 21 (Use of the Internet) of the Council's Information Computer Security policy for more detail.	✓	✓	✓	✓	✓
(6) The installation of software is only carried out by the ICT Service.	✓	✓	✓	✓	✓
(7) No unauthorised software or software not related to Council business is to be installed. ICT Services is authorised to remove all such software.	✓	✓	✓	✓	✓
(8) The copying of licensed software and data is illegal and prohibited.	✓	✓	✓	✓	✓
(9) Software and data files are to be checked for viruses before being loaded on council equipment.	✓	✓	✓	✓	✓
(10) Members must not attempt to repair equipment themselves.	✓	✓	✓	✓	✓
(11) It is a Members responsibility to save data he or she wishes to keep. All data saved on the corporate network is backed up centrally.	✓	✓	✓		✓
(12) It is a Members responsibility to save data he or she wishes to keep and ensure the data is backed up on a memory card. Any device that is used to store confidential, sensitive or personal information must store the information in an encrypted format.				✓	

Description	Thin Client solution	Thin Laptop solution	Access to kit in Council premises	PDA /Smart phone	Keyfob for accessing Council systems
(13) Members should only use the official Council e-mail address for Council business, and should only ask officers to e-mail them Council information via the Council e-mail address.	✓	✓	✓	✓	✓
(14) Members are required to sign and keep an up to date inventory of all equipment supplied to them.	✓	✓		✓	✓
(15) Security: <ul style="list-style-type: none"> • Passwords are not to be disclosed to anyone. • The use of someone else's password is not permitted. • Passwords should conform to recommended formats. Please refer to section 14 (password Controls) of the Councils Information Computer Security policy for more detail.	✓	✓	✓	✓	✓
(16) Members should have regard to the privacy of other Members and should not access another Members Council e-mail or Council data.	✓	✓	✓	✓	✓
(17) Insurance: <ul style="list-style-type: none"> • The Council maintains insurance on the equipment provided to Members. However, all reasonable care must be taken to prevent loss and damage so that all items are to be secured as far as practical. • Portable devices such as thin laptops and smartphones / PDA's must not be left unattended or unsecured wherever they may be. • Please ensure portable equipment is transported in their carry case and never left on display in a vehicle. Laptops should be carried in the boot of a vehicle where practical. • Any loss or damage to equipment must be reported as soon as possible. 	✓	✓	✓	✓	✓
(18) When returning portable devices such as thin laptops and Smartphones / PDA's for repairs it shall be returned in the carrying case together with all accessories provided.		✓		✓	

Description	Thin Client solution	Thin Laptop solution	Access to kit in Council premises	PDA / Smart phone	Keyfob for accessing Council systems
<p>(19) Information Computer Security Policy: Members must comply with the Council's Information Computer Security Policy. In particular Members attention is drawn to the particular sections: Section 06 – Use of Email</p> <ul style="list-style-type: none"> • The sender of an email is responsible for the communication and does not contain any libellous or defamatory statements. • Automatic forwarding of Council emails to personal accounts is prohibited. Emails that are of a personal nature or received of a party political nature can be individually forwarded to be dealt with away from the Council arena. Members should encrypt emails before they are released outside the Council's secure environment. • Under no circumstances should a council email address have an auto-forwarding facility set up to forward all emails to an external / personal email account. <p>Section 21 – use of the Internet: Users must not:</p> <ul style="list-style-type: none"> • Access or transmit any offensive, obscene or indecent images. • Receive or transmit material that is designed or is likely to cause inconvenience or distress. • Create, receive or transmit any defamatory material. • Transmit any material that infringes the copyright of another person. • Transmit any unsolicited, commercial or advertising material to any other person or organisation. <p>Members should note that references to email here include sms text messages and that rules about the internet apply to access via mobile phones, or any other mobile device, PC or Thin Client device.</p>	✓	✓	✓	✓	✓

Description	Thin Client solution	Thin Laptop solution	Access to kit in Council premises	PDA / Smart phone	Keyfob for accessing Council systems
(20) If a Member has chosen to use his or her own PC or other IT device, the Council will provide software for Council business via remote access facilities (keyfob). At the end of the period as an elected Member, access will be revoked and the keyfob returned to the Council.					✓

DRAFT