Neath Port Talbot
Castell-nedd Port Talbot
County Borough Council Cyngor Bwrdeistref Sirol

MEMBERS ICT SCHEME

(For Members who access ICT Equipment supplied via NPTCBC)

MAY 2022

Democratic Services and Digital Services Divisions

The Service Desk numbers below are for Members who require assistance when using their Council-owned ICT. Please identify yourself as a Councillor when making your enquiry/request.

Office Hours Help line: 01639 686767

Monday to Thursday: 8.30am – to 5.00pm
Friday: 8.30am – to 4.30pm

Email: ITservicedesk@npt.gov.uk

Out of Hours Help line 07815 795220

Monday to Thursday: 5.00pm to 9.00pm
Friday: 4.30 to 9.00pm

1. Introduction

1.1 Neath Port Talbot County Borough Council ("the Council") promotes the effective use of ICT (Information Communication Technology) by its Elected Members. Effective implementation of 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 Digital Services Team

1.5 To ensure the right level of support is offered to all elected members, equality screening sessions will be offered to all Members as part of their initial induction. The objective of the screening is to identify Members at a very early stage who may have disabilities or other needs where the provision of specialist technology may be of assistance in carrying out the role of Councillor. This will ensure that additional measures are put in place to assist individual Members, where necessary, with additional support and advice provided via the UK Government's 'Access to Work' scheme.

2. ICT Equipment

2.1 All Members have access to docking stations with Monitors, keyboards and mice at the Civic Centres. If Members are not aware of these details they should contact Democratic Services.

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

(i) iPad with keyboard cover and mobile connectivity
(ii) Laptop, with separate Screen, Keyboard, Case and Mouse

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

2.3 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.

2.4 The devices provided by the Digital Services Section will be installed with the current standard security software that will be configured to regularly update virus and malware definitions.

2.5 Optional hardware can also be provided on request:

(i) Printer
(ii) Access to Secure Council email on a Personal Mobile Phone Device

2.6 Where a Member accesses emails 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.

2.7

2.8 Outside corporate buildings the connection to NPT services will be via the Member's own Broadband connection or any other publically available Wi-Fi service. Members are able to use the Members remuneration scheme to support broadband costs.

2.9 This Scheme also includes appropriate software i.e. Anti-virus, equipment and software updates, plus support from the Digital Services team via a help line & out–of–hours support arrangements.

2.10 Saving of Work: any documents created under Council Services (i.e. using Word, Excel etc), should be saved to a secure Council server where they will be automatically backed up each evening. For security and confidentiality reasons, all work undertaken as part of a Member's elected duties should be saved in this way.

2.11 Members have a "cllr@npt.gov.uk" e-mail address. Note that this e-mail address should not be used by Members for personal purposes. As well as the corporate e-mail address, any Member can, at no extra cost to themselves, have their own personal e-mail address.

2.12 To facilitate the use of the Modern.Gov system that has been installed to improve access to the Council's Committee business, Members will use Modern.Gov as an alternative to receiving information through traditional paper-based channels

2.13 The services available when members connect to the Council will vary depending upon the method used to connect. The current ways to link to the Council are:

(i) Using the ICT facilities in the Member's Room
(ii) Using Council provided Wi-Fi connection in Council buildings
(iii) Using public Wi-Fi services
(iv) Using a home broadband connection
(v) Using a cellular enabled iPad
(vi) Using a personal smart phone

2.14 When connected via a NPT issued laptop, the Member will be able to access:

(i) Member application toolkit as set out at Appendix 1
(ii) The Council's Intranet – an array of information including staff contact information, corporate policies, etc.
(iii) Member's Hub – Containing Member's Seminar information, key documents, resources, Consultations, etc.
(iv) Modern.Gov – Committee Documents, Committee Membership, etc.
(v) Electoral Register Search Facilities.
(vi) Secure document storage area.
(vii) Secure printing.
(viii) HR and Payroll systems.

2.15 When using an NPT issued iPad the services available to Members differ and using the mobile capability of the device allows access to information whilst Members are on the move and also within meetings. The iPad allows Members to:

(i) Access the Members iPad application toolkit - Appendix 2.
(ii) Securely receive and send email from their corporate email address.
(iii) Access the Modern.Gov Application – which allows Members to securely access Committee Documents (including restricted documents) and to annotate those documents.
(iv) Access the Authority's Intranet Site – where an array of corporate information is available (including access to the Members Knowledge Hub).
(v) Securely store documents.
(vi) Access the Internet for research, etc
(vii) Download and install applications which could aid them to carry out their Member duties – requests to be made via the Service Desk.

3 Training/Development

3.1 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. Such training will be undertaken by members upon election.

4 Acceptable Use

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

4.2 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.

4.3 Council ICT equipment is also available to enable to fulfill Council business through:

(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.

4.4 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 Council's use their resources prudently and in accordance with the law.
(iii) ICT equipment should not be used in a manner that breaches the Members Code of Conduct. The Code makes it clear that when using the resources of the Council Members that such resources are not used improperly for political purposes (including party political purposes). 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.
(iv) Members should ensure that such ICT equipment is not used for any illegal activities that may bring the Council into disrepute.
(v) Members shall ensure that they do not use any ICT equipment for any purpose that is inconsistence with this policy.

4.5 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.

4.6 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 Cyber Security Policy (copies of which will be provide to members)

5 IT Security Policy

5.1 It is necessary that Members comply with and have a working understanding of the Council's IT Security Policy, Information Management Policy and Cyber Security Policy and supporting guidance notes, which apply to all ICT equipment and systems – copies of which will be provided to members and training provided.

Email and Internet Acceptable Usage Guidance Notes

5.2 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.

5.3 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.

5.4 The Council will provide Members with a Council email address in the format "name@npt.gov.uk", this must used for all emails conducting or in support of official Neath Port Talbot County Borough Council business.

5.5 Non work emails e.g. Gmail, Outlook, Hotmail must not be used to conduct or support official Neath Port Talbot County Borough 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.

5.6 Members must ensure that any emails containing sensitive information must be sent from an official council email.

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

5.8 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 Neath Port Talbot County Borough Council business should be considered to be an official communication from the Council.

5.9 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 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.

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 2018 and the Freedom of Information Act 2000 the contents of this email may be disclosed.

A copy of the privacy notice for elected members is available at www.npt.gov.uk or on request to myself

5.10 Under no circumstances should Members use email and Internet facilities for any uses that are unacceptable involve the access, use, submission, publication, display, downloading or transmission of any information which:

(i) Violates any of the Council's regulations, policies or procedures.
(ii) Violates or infringes on the rights of any other person, including the right to privacy.
(iii) Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
(iv) Restricts or inhibits other users from using the system or the efficiency of the Council's computer systems.
(v) Results in the unauthorised editing of the Council's web pages.
(vi) Encourages the use of controlled substances or uses the system for purposes with criminal intent.
(vii) Uses the system for any other illegal purpose.
(viii) Solicit the performance of any activity that is prohibited by law.
(ix) Conduct any unapproved business
(x) Transmit material, information, or software in violation of any law.

(xi) Make any unauthorised purchases or commitments in the name of the Council.
(xii) Use by non-Councillors.

5.11 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.

5.12 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

5.13 All users of the Internet and/or corporate email must be aware that all activity on the Council's Data Network is the property of the Authority and that, therefore, no such activity can be considered private.

5.14 All Members are reminded to ensure that they adhere to the separate guidance in relation to their usage of Social Media platforms during their term of office.

Information Security Incident Management Guidance Note

5.15 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.

5.16 Members should report any incidents or suspected incidents immediately by contacting the Digital Services Section and the Head of Legal and Democratic Services.

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

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

Software Guidance Note

5.19 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.

5.20 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

5.21 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

5.21 It is the Council's policy to prohibit the use of all removable media devices. Removable media devices are electronic items usually used for 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. All data stored on removable media must be encrypted where possible.

5.22 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 2018

5.23 The Data Protection Act (DPA), 2018 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. Members will note that they are their own data controller for these purposes and the Head of Legal and Democratic Services will register all elected members with the Information Commissioner's Office.

5.24 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.

5.25 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.

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

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

5.28 If the Council fails to abide by DPA, it could be prosecuted and fined up to £17,000,000. However, the Act also imposes personal liability, so if a Member is found to be contravening the DPA they could be prosecuted or fined to a similar amount. 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.

5.29 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.

5.30 Members are advised to read the Information Commissioner's *Advice for the elected and prospective members of local authorities* for further details, copies of which be provided to members on induction

5.31 Members should note from paragraph 5.23 that they are their own data controller for information that they generate in the course of their work i.e. constituency work. However, the Council remains the data controller for any information that is supplied by the Council to elected members to enable them to fulfill their role. In accepting and utilising Council ICT equipment and utilsing software provided by the Council, members hereby agree that the Council shall be entitled to act at a data processor for such information, providing rights of access for any information that is held pursuant to this Members ICT Scheme.

The Freedom of Information Act 2000

5.32 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 FOIA

(iii) Information received, created or held by a Member on behalf of the Council will be covered by the FOIA, 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 FOIA if it is held for the council's own business.

5.32 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 – copies of which will be provided to members on induction.

5.33 If Members require advice or assistance on the provisions of the DPA or FOIA they should contact the Head of Legal and Democratic Services.

6 Health and Safety

6.1 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. The responsibility though for ensuring compliance with the same rests with the elected member. Members should contact Legal & Democratic Services to arrange further advice regarding best practice for health and safety.

7 Insurance

7.1 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 willful neglect.

7.2 Security – reasonable care must be exercised in order to prevent theft, loss or damage at all times. Specifically any mobile devices, e.g. laptops or tablet devices 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.

7.3 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 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.

7.4 Travelling abroad – it is not envisaged that there will be a regular requirement to take Council-provided 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 overseas 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.

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

8 Privacy

8.1 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 Public Service Ombudsman for Wales. 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.

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

8.3 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.

9 Confidentiality

9.1 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.

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

10 Restriction of Use

10.1 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.

11 Return and Recovery of Equipment

11.1 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.

11.2 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 Digital

Services within two weeks of ceasing office. All information held on the equipment will be deleted and the equipment may be re-issued.

12 General Advice

Password Advice:

12.1 Passwords should never be divulged to anyone.

12.2 Passwords should not be written down.

12.3 Passwords should be minimum of 8, complexity enforced (3 items from the 4 -of uppercase, lowercase, numeric, special char). If a Member believes a password has been compromised it should be changed immediately. Please contact the Service Desk if assistance is required to change a password.

Computer Viruses

12.4 Viruses are common and can, in some instances, cause considerable damage to a system or network. The following actions should be taken in defence:

(i) If Members are unsure about software installed on their NPT machine or if any program or email causes concern they should contact the Service Desk immediately.
(ii) If a Member believes a virus has infected their NPT device, the device should be powered off and the Service Desk should be contacted immediately.
(iii) Members must not attempt to disable any anti-virus software on NPT machines.

Confidentiality

12.5 Members must ensure that sensitive/confidential information is treated in the strictest confidence. No Council-related sensitive information should be stored locally (on a laptop hard drive or USB stick). It is more secure if all Council documents are stored on Council servers.

Support

12.6 ICT Support details are shown on the front of this document. Members may also e-mail the Service Desk on Itservicedesk@npt.gov.uk (this address is already included in the contact list on your laptop).

12.7 Support and assistance **will be** provided on:

(i) Technical difficulties and queries in relation to Council supplied equipment.
(ii) Network connectivity of Council supplied equipment.
(iii) The Members application toolkits, which comprises; MS Office suite, Modgov, remote hybrid meeting applications pertaining to participation in Council meetings e.g. MS Teams, Zoom.

(iv) Any new software identified by the Members ICT reference group that supports Members in their duties and added to the Members application toolkits for access by all Members.
(v) Council business Data retrieval from Council supplied equipment.

12.8 Support **will not** be provided for personal queries such as:

(i) Setting up of personal IT equipment such as laptops, pc's, mobile phones.
(ii) Remote meetings with friends and family.
(iii) Personal Data retrieval or personal use.

12.9 **Problems/Technical Enquiries -** Any Member who is not satisfied with the service received or is experiencing problems which are not being addressed should contact the IT Officers below:

Jules Payne – Head of Digital Operations
e-mail j.payne@npt.gov.uk

Chris Owen – Chief Digital Officer
e-mail: c.m.owen@npt.gov.uk

12.10 **Other Assistance -** If a Member wishes to discuss the provision of Members ICT generally, they may contact:

Craig Griffiths, Head of Legal and Democratic Services:
c.griffiths2@npt.gov.uk

Stacy Curran, Democratic Services Manager
s.curran@npt.gov.uk

Appendix 1

Windows application toolkit

Intune Company Portal
Ms Outlook
MS Word
MS Excel
MS Powerpoint
One Drive
Edge
Chrome
Intranet link
Teams
Zoom
Authenticator
MiPermit
Mod Gov
BBC News
Met Office
Google Earth
Facebook
Messenger
Twitter
Instagram
What3words

Appendix 2

Ipad application toolkit

Intune Company Portal
Ms Outlook
MS Word
MS Excel
MS Powerpoint
One Drive
Edge
Chrome
Intranet link
Teams
Zoom
Authenticator
MiPermit
Mod Gov
BBC News
Met Office
Google Earth
Facebook
Messenger
Twitter
Instagram
What3words