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

Acceptable Use of ICT Policy

Version Control		
Version	**Date**	**Comments**
Version 1	May 2008	Initial draft of policy
Version 1.1	June 2009	Amendment to "6" & Union & Personnel comments added
Version 1.2	Jan 2012	Review - small amendments and changes to contact details
Version 1.3	May 2013	Review – small amendments
Version 1.4	October 2014	Review – small amendments
Version 1.5	January 2016	Review - small amendments and changes to contact details
Version 1.6	June 2017	Review – small amendments
Version 1.7	May 2018	Review – small amendments

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

ACCEPTABLE USE of ICT POLICY

1. INTRODUCTION 3
2. EMAIL 3
3. INTERNET 4
4. CONFIDENTIALITY 5
5. MONITORING AND DATA PROTECTION 5
6. SECURITY 5
7. EQUIPMENT NOT PROVIDED BY THE AUTHORITY 6
8. PERSONAL USE 7
9. CONSEQUENCES OF A BREACH OF THIS POLICY 7
10. GENERAL QUERIES 8

1. INTRODUCTION

1.1. This Policy relates to the use and monitoring of all of the Authority's IT and communication systems, including telephones, mobile telephones, facsimile machines, computers (including laptops, iPads, smart phones and personal organisers), email, the internet and the intranet.

1.2. The Authority provides IT and communication systems for business purposes and the use of these systems at all times is subject to this policy. Breach of this Policy will be considered a disciplinary matter.

1.3. This Policy applies to all employees of the Authority, elected members, contractors, agency staff and any others with access to Authority information assets or who use the Authority's IT and communication systems

2. EMAIL

2.1 Authority email accounts are provided for work purposes only. Personal email is not to be sent using a Neath Port Talbot County Borough Council email address.

2.2 All emails sent and received from NPT email addresses are monitored by the Authority and may be read as part of any service review and /or investigation carried out by Internal Audit or Service Managers.

2.3 Email correspondence cannot be considered private. Emails can be easily intercepted, copied, forwarded and stored without the original sender's knowledge. You must take into account the fact that any email sent may be read by a person other than the intended recipient.

2.4 Any attachments sent to external email addresses which contain personal or sensitive material should be encrypted or password protected unless a secure e-mail system i.e. Government Connect Secure eXtranet (GCSx) secure mail or Criminal Justice Secure eMail (CJSM) is used. Advice on encryption can be obtained from the Business Relations Manager – Ian John, Ext 6036.

2.5 All messages and files are automatically scanned for viruses before being introduced into the network, but this does not provide a complete guarantee of

protection. All employees have an obligation to be cautious when opening emails and attachments from unknown sources. If you have any doubts about opening an email or attachment, speak to the IT Service Desk (Ext 6767) first.

2.6 Contracts can be entered into by email in the same way as they can by letter or on the telephone. You must at all times take care to ensure that you do not inadvertently enter into contracts by email which bind the Authority, and you should be aware that contracts must only be entered into in accordance with normal contract procedures.

2.7 You must not under any circumstances send messages or attachments whether within the Authority or outside the Authority which are:

- Abusive, including the use of foul language
- Malicious
- Discriminatory in any sense (e.g. sex, sexual orientation, age, race, religion, gender or disability)
- Defamatory about any other person or organization
- Bullying or intimidating in content

2.8 If you receive any such message from outside the Authority, unless you wish to report the matter to your line manager or the IT Service Desk, you must delete it and must not forward it within or outside the Authority. Sending email of the type described above is likely to be treated as a disciplinary offence in line with the Disciplinary Policy and procedures and could result in dismissal for gross misconduct.

2.9 You should only send sensitive or confidential information when the security of the data is ensured i.e. the recipient address is a known, secure address or the email is protected.

2.10 Personal email accounts should not be used to send Authority information. This includes forwarding email from Authority email accounts to personal email accounts. Where there is a requirement for access to Authority emails or information away from the office this must only be via approved methods. For more information contact the IT Service Desk or the Business Relations Manager.

3. INTERNET

3.1 The Authority has put technical measures in place to prevent access to internet web sites which contain explicit, illegal or otherwise inappropriate materials. If

you need to access a blocked site for the purposes of your job you must obtain express authorisation from your line manager who will, if appropriate, contact the IT Division.

3.2 Personal use of the Authority's Internet facilities is permitted as long as the usage is during your own time i.e. when you are clocked out and involves acceptable browsing i.e. not inappropriate websites.

3.3 It should be noted that much of the information that appears on the internet is protected by copyright. Unauthorised copying or modifying of copyright protected material, including software, breaches copyright law. Therefore, downloading software or copyright protected information is not permitted, as it may make you and/or the Authority liable to legal action.

4. CONFIDENTIALITY

4.1 You must not use the Authority's IT and communications systems whether alone or in conjunction with any other person to make an unauthorised disclosure or copy of sensitive, personal or business information belonging to the Authority.

4.2 The unauthorised disclosure or copying of information belonging to the Authority is likely to be treated as a disciplinary offence in line with the Disciplinary Policy and procedure and could result in dismissal for gross misconduct.

5. MONITORING AND DATA PROTECTION

5.1 In order to protect the interests of the Authority and to maintain the effectiveness, integrity and security of the Authority's network, the Authority has various tools in place to monitor usage of ICT systems. You should not expect that your use of the Authority's IT and communication systems is private.

5.2 The holding, processing and disclosure of personal data in electronic form is regulated by the provisions of Data Protection legislation. Personal information relating to a living individual who can be identified from that information should not be sent outside the Authority unless proper checks have been made to ensure that this will not involve any breach of that or any other legislation.

6. SECURITY

6.1 The login credential supplied to you to undertake your duties must never be shared with another member of staff or other person(s)

6.2 If you are provided with a portable computer, iPad, mobile phone, Blackberry, personal organiser and/or any related or similar equipment, you must ensure its security at all times. You must in particular:

- Never leave computer equipment including CDs, DVDs, flash drives, blackberry, key fob, etc. in an unattended vehicle unless the equipment is locked in the boot. If you have to leave the vehicle for any reason, this must be for the least time possible. It should be noted that often the data on the computer equipment is more valuable than the computer equipment itself.
- Never leave equipment unattended in public or unlocked where its screen can be viewed
- Always lock mobile equipment when not in use so that it cannot be used without entering your log-on details
- Keep your passwords confidential (IT systems will force you to change them regularly) and never, in any circumstances, attach the password to the device

6.3 If your computer equipment is lost or stolen you must report the incident immediately to your line manager/Head of Service and/or IT Service Desk who will advise you what steps to take. The incident will be fully investigated in line with the ICT Incident Reporting Policy and may be treated as a disciplinary issue if you have failed to take adequate steps to safeguard the security of equipment in your possession.

6.4 You must not attempt to access any service or function of the network unless you have been granted permission.

7. EQUIPMENT NOT PROVIDED BY THE AUTHORITY

7.1 You must not connect, or attempt to connect, any device to the network without express authority from the IT Division. You should be aware that the Authority may have measures in place to detect this activity.

7.2 In particular you should not attempt to connect any of the following devices to the Authority's network:

- A file/information storage device not issued by the Authority
- A mobile phone not issued by the Authority
- An MP3 Player or similar device not issued by the Authority
- A gaming device not issued by the Authority

7.3 A breach of the prohibition on connecting devices to the Authority's network is likely to be treated as a disciplinary offence in line with the Disciplinary Policy and procedure and could result in dismissal for gross misconduct

8. PERSONAL USE

8.1 Personal use of the Authority's Internet/Intranet facility is permitted subject to the following rules:

- Personal Internet usage is in your own time i.e. when clocked out
- Personal Intranet usage e.g. to the classifieds section is in your own time i.e. when clocked out
- You may not subscribe to any non-job related Internet service e.g. BBC tickertape.
- You may not use the Authority's systems to transfer, store or download information and files for your personal use including (but not limited to) MP3, AVI, WMV, MPEG, etc.

8.2 If your personal use exceeds an acceptable level in the reasonable opinion of the Authority or you do not comply with these rules your access may be curtailed and you may be subject to disciplinary action in line with the Disciplinary Policy and procedure and which could result in dismissal for gross misconduct.

8.3 Personal use of Authority equipment exclusive of Internet access is not permitted unless sanctioned by a Head of Service.

8.4 Unauthorised staff must not install software on Authority devices or machines.

8.5 Authority person identifiable or sensitive information or business data must not be stored on a device which is not owned by the Authority unless specifically authorised by a Head of Service.

9. CONSEQUENCES OF A BREACH OF THIS POLICY

9.1 Breach of this Policy will be considered a serious disciplinary matter and will be dealt with in line with the Disciplinary Policy and procedure. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in disciplinary action, not excluding dismissal, are:

- Excessive or persistent visiting of non-job related internet sites during your normal working day
- Excessive or persistent use of an authority email address for personal purposes

- Introducing a virus to the computer system by inserting a device, CD or DVD into an Authority computer without running a virus check, via email or from downloading an Internet file
- Misuse of a computer system which results in any claim being made against the Authority
- Accessing pornography or any other inappropriate or illegal material and/or circulating it
- Unauthorised copying or modifying of copyright material
- Unauthorised downloading/storing of software or files
- Obtaining unauthorised access to Authority systems, services, equipment, etc.
- The connection of an unauthorised device to the network

9.2 In less serious cases you may have access to the internet from your computer removed or other disciplinary action taken against you short of dismissal.

10. GENERAL QUERIES

10.1 Any questions regarding this policy or computer security in general should be addressed to Steve John, the Head of ICT, on ext. 6218 or Ian John, Business Relations Manager, on ext 6036.