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

IT Security Policy

Version Control		
Version	**Date**	**Comments**
Version 2 (Version 1 was the original IT Security Policy & Advice Note)	April/May 2008	Initial redraft of policy
Version 2.1	10th June 2008	After ICTTG comments
Version 2.2	18/3/2009	Added to "Access Control"
	June 2009	Agreed with Unions
Version 2.3	Jan 2012	Review - contact details amended
Version 2.4	June 2013	Review
Version 2.4.1	October 2014	Review
Version 2.5	January 2016	Review – contact details amended
Version 2.6	June 2017	Review
Version 2.7	April 2018	Review and small amendments

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

IT SECURITY POLICY

1 INTRODUCTION 3

2 CORPORATE DIRECTORS' RESPONSIBILITIES.....3

3 HARDWARE SECURITY 5

4 SECURE AREAS 6

5 DATA SECURITY 6

6 EXTERNAL ACCESS TO THE NETWORK 7

7 AUTHORISED FILES AND PROGRAMS.....7

8 MAINTENANCE AND SUPPORT 7

9 DATA PROTECTION.....8

10 PRIVATE USE 8

11 ACCESS CONTROL.....8

12 PASSWORD ADVICE.....9

13 COMPUTER VIRUSES 10

14 INCIDENT REPORTING 11

15 HEALTH & SAFETY 11

16 POLICY REVIEW.....11

17 DISCIPLINARY ACTION.....11

18 GENERAL 11

1 INTRODUCTION

1.1 In view of the Authority's reliance on information systems, the confidentiality, availability and integrity of data are of enormous importance. In order to help maintain equipment, systems and data in a sensibly controlled and secure environment, there are a number of requirements which must be observed by all staff.

1.2 This document outlines the Authority's security policy relating to the use of ICT equipment, networks and all related devices and software and is intended to:

- Protect the council's information assets, hardware and software against unauthorised access/usage, loss, theft, virus infection or hacking
- Protect the council from prosecution against the use of unlicensed/illicit software
- Ensure that control exists regarding the purchase and disposal of hardware and software
- Ensure that all installations/amendments are carried out by authorised IT support personnel
- Protect authorised users from unintentional abuse of facilities by providing a formal document with which they should comply.

1.3 This policy applies to all users of the Authority's equipment (including members) and is intended to alert authorised users to their responsibilities for the security of data and contains advice on how some of those responsibilities can be met.

1.4 External staff (3rd party developers, external auditors, consultants, engineers, etc) requiring access to the Authority's IT equipment should do so only once authorised and must be made aware of this policy.

2 CORPORATE DIRECTORS' RESPONSIBILITIES

2.1 Corporate Directors are responsible for the security and proper use of the Council's information assets and equipment, for ensuring that staff receive appropriate training and to ensure that:

a) Computer programs and data developed or purchased for the Council, are solely for carrying out its lawful activities as authorised by it. Unauthorised access to, copying, alteration, destruction or interference with computer programs or data is expressly forbidden.

b) Computer hardware/software is only to be used for purposes directly concerned with the Council's activities and must not be taken off site without prior authorisation. Authorisation for home use to undertake official duties must be strictly controlled, and be given only in circumstances which reflect the duties and responsibilities of the individual officer concerned. Only authorised software is to be installed on the Council's hardware.

c) Procedures designed for the security of data, programs or equipment must be followed.

d) Computer rooms and other offices which house computer equipment must be adequately protected, and staff must play their part in following and monitoring the security procedures.

e) Computer manuals, media and related documentation must be properly stored.

f) Computer hardware and software must be obtained in accordance with the Authority's ICT Procurement Policy and must be assembled and tested by authorised IT personnel before use.

g) Disposal of ICT equipment must be carried out by authorised staff with regard to the Waste Electrical & Electronic Equipment (WEEE) directive.

h) Waste computer-printed output must be disposed of with due regard to its sensitivity. Confidential output must be shredded and/or destroyed by other appropriate, authorised means. Individual directorates of the Council are responsible for ensuring that the established disposal arrangements are adhered to.

i) All ICT equipment must be adequately insured. Please contact the Insurance Manager for further details.

3 HARDWARE SECURITY

3.1 Where possible, desktop equipment should be protected by only being placed in secure areas i.e. areas which are not accessible by members of the public. In offices that are more accessible to the public (e.g. ground floor offices) windows and blinds should be shut outside office hours and/or screens positioned so that the screen contents cannot be viewed.

3.2 Desktop equipment must only be moved by authorised IT Staff.

3.3 All software installation disks, licences, etc must be logged and held by the IT Service.

3.4 Where laptops or other portable/mobile devices are used, additional security is required to avoid obvious risks to the data. Laptops and other portable mobile devices should, for example, be locked away when not in use and should not be left unattended in vehicles or public places. Data which is to be held on laptops or other portable devices should be risk assessed and appropriate security employed. **Only Authority-owned, authorised, portable/mobile devices are to be used**. Contact the IT Service for advice and guidance. More information can be found in the Mobile Device Security Policy.

3.5 Removable storage media i.e. USB memory sticks, CDs/DVDs, digital cameras, MP3/MP4 players, memory cards, mobile telephones, Bluetooth/Infra-red devices, PDAs, Blackberries, etc. should only be used with due regard to:

- Maintaining the integrity of the data
- Maintaining standards of care by ensuring the privacy of privileged, personal/sensitive/confidential or third party data
- Avoidance of contravention of any legislation, policies or good practice requirements
- Preventing contamination of Authority networks
- Avoiding unauthorised distribution of data

3.6 Users of removable storage media must appreciate the high security risk they represent and must limit usage to those times when no other method of storage or transportation of data is available. All such media used with Authority equipment must be purchased by and for the Authority. Only data that is authorised and necessary to be transferred should be saved on to the removable media. Staff using removable storage media to transfer data must ensure that:

- It is the most appropriate transfer method

- They have considered the most appropriate way to transport the media
- They are able to demonstrate that reasonable care to avoid damage or loss of the media is taken.
- **No personal removable storage media should be used to transfer data to/from Authority equipment or to connect to Authority equipment.**

More information on removable media can be found in the Removable Media Policy.

3.7 Keys should be kept by authorised personnel only, and either removed from the premises when unattended or placed in a locked safe.

3.8 Property marking will be carried out by the IT Service prior to the release of the item of equipment to individual members of staff or section. Users must not remove this asset tag. If the property identification mark is accidentally removed, the IT Service should be informed and, if possible, the tag retained.

3.9 The IT Service maintains an up-to-date inventory of all the council's hardware and software and audit checks are carried out to ensure that the inventory is correct.

4 SECURE AREAS

4.1 Unauthorised persons are only allowed in secure areas, such as computer rooms, when accompanied by an authorised person and signed into the visitor access book.

4.2 The transfer of keys, identity cards, access cards, codes, key fobs or passwords to unauthorised persons is forbidden.

4.3 Any loss of access device, and breaches or attempted breaches of security must be reported to I.T. staff as soon as possible.

5 DATA SECURITY

5.1 The majority of users save files and documents to servers supported by the IT Service. The safeguarding of the data on these servers is the responsibility of the IT Service and necessary security is in place.

5.2 Where possible, data should not be stored locally i.e. on a machine's "C" drive. In instances where a valid business case exists for holding data locally, security of the data is the responsibility of the user. Each user must ensure that important

files and documents which are stored on their machines are backed up regularly with the backup media stored safely. Where data is considered critical it should not be only held locally. Guidance and advice is available from the IT Service and the Information Security Policy.

5.3 Good housekeeping procedures should be utilised whenever possible, for example, control over email retention, managing the number and relevance of stored documents, etc. Advice and guidance is available from the IT Service.

6 EXTERNAL ACCESS TO THE NETWORK

6.1 External access to the network, for example, to send or read email from an Authority email account, must be facilitated by the IT Service.

6.2 External access to systems from non-authority staff must be facilitated by the IT Service.

7 AUTHORISED FILES AND PROGRAMS

7.1 In order to ensure that all software programs and files in use throughout the authority are legitimate copies, covered by appropriate licences, no software should be installed on any computer except by authorised IT staff. This includes screensavers, shareware, freeware, demonstration products, etc.

7.2 Under no circumstances should staff install any unauthorised games on Council IT equipment.

7.3 Users with unauthorised files or programs installed on their PC must immediately remove them or report the matter to the IT Service to have the programs/files removed

7.4 The copying of software is strictly controlled under the software licensing agreement and by the *Computer Misuse Act 1990*. Under no circumstances should software be copied except by IT Staff who will undertake this function to ensure licence agreements are adhered to and necessary security copies of the product exist.

8 MAINTENANCE AND SUPPORT

8.1 In order to enable effective support to be provided, individual users must not change the standard set-up of their PCs unless directed to by IT staff.

8.2 When reporting IT Security incidents, users will be asked to give some indication of the impact of the request so that the request priority can be allocated.

9 DATA PROTECTION

9.1 The storing and use of personal data maintained on any computer system is regulated under the *Data Protection Act 1998 and 2018*. Full details of employees' responsibilities in relation to the *Data Protection Act 1998 and 2018* are available in the Data Protection Policy which can be found on the Authority's Intranet Site and all users should make themselves familiar with this policy.

10 PRIVATE USE

10.1 Private use of any of the Council's ICT equipment is prohibited except where permission has been granted by the relevant Chief Officer. This usage should be on an occasional basis and outside work time. Consumables should not be made available for private use. Full details of the time, purpose and nature of the private use should be recorded.

10.2 More information is available in the Acceptable Use of ICT Policy.

11 ACCESS CONTROL

11.1 Users will only be given access rights commensurate with the duties they will be asked to perform. User rights will be kept to a minimum at all times.

11.2 Generic user accounts will only be created to direct and distribute service mail.

11.3 Where possible no one person will have full rights to any system. The I.T. Service will control network/server passwords and system passwords will normally be assigned by the system administrator in the end-user directorate. The system administrator will be responsible for maintaining the integrity of the data and for allocating/determining user access rights.

11.4 Intruder detection will be implemented where possible. A user account will, where possible, be locked after 5 incorrect log-on attempts.

11.5 The I.T. Service and system administrators must be notified of all employees leaving the Authority or, where system access is affected, employees changing

post. Necessary steps will then be taken to remove the employee's rights to all systems.

11.6 Access to data is initially achieved through a local PC, monitor, etc. Once access to the machine is achieved the data available through the machine becomes accessible. In order to reduce the risk of unauthorised access to information the PC should be password protected at log-on and have a password protected screen saver which activates after 5 minutes.

11.7 PCs, Printers and other computing devices will only be connected to the network by authorised IT staff.

11.8 PCs must not be left unattended when logged in, as a minimum they should be locked prior to being left.

12 PASSWORD ADVICE

12.1 PCs/networks require a Login id/Password entry as a first line of protection. This gateway is secure and cannot be breached unless someone obtains or guesses the password. The guidelines below will not remove the possibility that this may happen, but they will minimise it and make your system more secure.

12.2 Passwords must be changed on a regular basis (every 80 days as a minimum) and under no circumstances should individuals divulge their passwords to anyone.

12.3 Passwords must be 7 or more characters long and include upper and lower case letters and a number or special character.

12.4 Words found in a dictionary should be avoided.

12.5 If you believe your password has been compromised it should be changed immediately.

12.6 Passwords should not be reused for twenty generations i.e. twenty password changes.

12.7 Temporary passwords should be changed on first access.

12.8 Passwords should not be written down but where this does occur i.e. where there is no alternative, the password must be held securely. If the password is a

system account with special privileges, a written copy of the password must be inserted into a sealed envelope and held in a secure area.

12.9 Individual passwords must never be divulged to anyone (in person or by telephone) regardless of who that person claims to be. Such requests should be reported to the Business Relations Manager.

12.10 Familiar words or numbers i.e. names, date of birth, etc should not be selected as a password – see Appendix A for examples of passwords which should not be used.

12.11 The resetting of a user password will be undertaken by a member of the I.T. Service Desk, but only after an authorised request has been received. A request from a line manager via email is acceptable.

12.12 The resetting of an application password will be undertaken by the appropriate officer following the designated procedure for that application.

13 COMPUTER VIRUSES

13.1 No programs or files should be loaded onto a PC except by authorised IT staff. It is recognised however that, on occasion, files will need to be transferred to storage media. In order to protect the Authority's PCs and networks from viruses no file should be loaded back onto an Authority machine until it has been virus checked.

13.2 Viruses are becoming more common and are capable of causing considerable damage to a system or network. The following actions should be taken in defence:

(i) If you are unsure about software installed on your machine or if you have any concerns about programs/emails, etc contact the IT Service Desk.

(ii) Do not ask IT support staff to install shareware/freeware. This will be refused because only validated or authorised software can be used on authority machines.

(iii) Do not attempt to use software from home or external sources.

(iv) Only allow authorised personnel to load software onto your machine.

13.3 Users must not disable the anti-virus software on any hardware.

13.4 In the event of a virus being discovered on a PC, the user should leave the PC exactly as it is and contact the IT Service Desk immediately.

14 INCIDENT REPORTING

14.1 Users are required to report any and all information system security breaches/ICT incidents. Failure to do so could result in disciplinary action.

14.2 An incident is an event which involves a breach of the principles and guidelines contained in this policy and any associated policy or guideline.

14.3 The ICT Incident Reporting Policy gives more advice on this topic.

15 HEALTH & SAFETY

15.1 Work Station Assessment advice is available in the Authority's Health & Safety Booklet, a copy of which is available on the Authority's Intranet. Please contact the Corporate Health & Safety Manager for further information.

16 POLICY REVIEW

16.1 The policy will be reviewed on an annual basis or as required.

17 DISCIPLINARY ACTION

17.1 Misuse of computer hardware and software is considered a very serious matter. Disciplinary action will, when appropriate, be taken against employees who contravene this policy and could, in certain circumstances, include dismissal. Furthermore, misuse of computer programs or data, including unauthorised access to data, could lead to prosecution under the *Computer Misuse Act 1990* or the *Data Protection Act 1998 and 2018.*

18 GENERAL

18.1 All identity cards, access cards, keys, manuals and equipment must be returned to the line manager, HR or authorised person when staff leave the employment of the Council.

18.2 When staff change posts within the Authority a review should be undertaken by a line manager to establish if items of equipment, identity cards, etc need to be returned and to discern if access rights need to be amended.

18.3 Periodic checks may be made by Internal Audit staff to ensure compliance with these rules.

18.4 The requirements contained in this policy statement are of a general nature covering all computer equipment; there may be additional requirements designed for specific locations, data or applications.

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

Appendix A

PASSWORDS TO AVOID

"Password1"

"October15"

"13/10/15"

"Monday1"

"Autumn1"

"qwerty1"

"asdfgh1"

"Temp123"

Your name.

Family names.

Your login id.

Your login id in reverse.