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

Bryncoch Church in Wales Primary School
Ysgol Gynradd yr Eglwys yng Nghymru Bryncoch

Information Security Policy

Version Control		
Version	**Date**	**Comments**
Version 0.5	June 2008	Initial draft of policy
Version 1	June 2009	Personnel comments added and Union agreement
Version 1.1	Jan 2012	Review - Small amendments and update of contact details
Version 1.2	June 2013	Review and small amendments
Version 1.3	October 2014	Review and small amendments
Version 1.4	January 2016	Review - Small amendments and update of contact details
Version 1.5	June 2017	Review and small amendments
Version 1.6	April 2018	Review and small amendments

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

INFORMATION SECURITY POLICY

1 INTRODUCTION 3

2 SCOPE OF THE POLICY 4

3 POLICY OBJECTIVE AND BASIC PRINCIPLES 4

4 ROLES AND RESPONSIBILITIES 5
- 4.1 Corporate Directors 5
- 4.2 Heads of Service 5
- 4.3 System Owners 5
- 4.4 Line Managers 6
- 4.5 Employees 6

5 POLICY 7
- 5.2 Physical and Environmental Security 8
- 5.3 Communications & Operations Management 8
- 5.4 Access Control 9
- 5.5 System Development, Acquisition and Maintenance 9

6 LEGISLATIVE COMPLIANCE 10

7 SECURE DISPOSAL OF INFORMATION 10

8 AUDIT LOGGING 10

9 BREACH OF THIS POLICY 11

10 POLICY REVIEW 11

11 GENERAL QUERIES 11

1 INTRODUCTION

1.1 Information, whether printed or written on paper, stored electronically or sent by post or electronic means, is an asset which, like other important business assets, has value and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity and reduce the possibility of business damage.

1.2 Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security is characterised here as the preservation of :-

a) **Confidentiality**: ensuring that information is accessible only by those authorised to have access

b) **Integrity**: safeguarding the accuracy and completeness of information and processing methods

c) **Availability**: ensuring that authorised users have access to information and associated assets when and where required.

1.3 Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and/or software functions. These controls need to be established to ensure that the specific security objectives of the Authority are met and maintained.

1.4 The key aspects of Information Security include:

- Information Assets – identification of Neath Port Talbot County Borough Council assets and owners and ensuring that required security measures are in place (including asset classification and security marking of documents)
- Personnel security – performing staff security vetting, ensuring staff awareness of and compliance with security responsibilities
- Physical Security – protection of physical assets
- IT security – ensuring Neath Port Talbot County Borough Council systems and processes are secure so that information held electronically is protected
- Business continuity – measures are in place to ensure accidents, fire, flood, theft, etc. do not compromise Council business so that the Authority can maintain services.

2 SCOPE OF THE POLICY

2.1 This Information Security Policy applies to all information assets and information systems owned or administered by the Authority.

2.2 The policy applies to all those who are responsible for initiating, implementing or maintaining security in the Authority as well as all users of information systems, including:

- All employees of the Council and elected members
- All employees and agents associated with organisations who directly or indirectly support or use the Authority's ICT services and resources
- All temporary staff directly or indirectly employed by the Authority
- All users of Authority ICT systems, networks and resources

2.3 All future information systems must comply with this policy. Systems already installed at the time of issue will be reviewed for compliance, and appropriate action taken.

2.4 It is the responsibility of all users of Authority ICT systems, networks and resources to comply with this policy. Each user must, therefore, ensure that they are familiar with and understand its content.

3 POLICY OBJECTIVE AND BASIC PRINCIPLES

3.1 The main objective of this policy is to provide management direction and support for information security within the Authority in accordance with business requirements and relevant laws and legislation by setting a clear policy direction and demonstrating management support for, and commitment to, information security across the Authority through the issue and maintenance of this information security policy.

3.2 This policy is owned by the Director of Finance & Corporate Services. It is the high-level statement of security objectives, processes and evaluation of the effectiveness of security measures. There will be a number of detailed Security Policies and other security guidance documents for staff. These more detailed security documents will be fully consistent with this policy.

3.3 The implementation of this security policy and the more detailed security measures in supporting security documents is the responsibility of the Head of ICT.

3.4 It is important that people working in and for the Authority understand the importance of sustaining a security regime and that their comments about the impact of security measures on their working practices are communicated to and responded to by management. One of the main success factors for the Neath Port Talbot County Borough Council security regime is that employees are committed to applying and adhering to the necessary security measures disseminated through the various security documents. Contractors providing development, support and maintenance for information systems are to be fully committed to the Neath Port Talbot County Borough Council security regime.

4 ROLES AND RESPONSIBILITIES

4.1 *Corporate Directors*

4.1.1 Corporate Directors will ensure:

4.1.1.1 Compliance with this policy and with all relevant practices and procedures.

4.1.1.2 All staff understand their obligations via training and awareness programmes.

4.1.1.3 Security incidents are reported to the Authority's Business Relations Manager as soon as practicable.

4.2 *Heads of Service*

4.2.1 Heads of Service are responsible for:

4.2.1.1 Ensuring that all major applications, systems and information resources are identified and that a "system owner" is appointed for each.

4.2.1.2 Addressing security at recruitment stage, ensuring that adequate screening takes place in relation to potential recruits and, where appropriate, for ensuring that security matters are included in job descriptions and contracts.

4.2.1.3 Ensuring that procedures are in place to maintain business continuity in the event of a disruption of service.

4.3 *System Owners*

4.3.1 System owners are responsible for all security issues including access permissions, back-ups and security of information.

4.4 *Line Managers*

4.4.1 Line managers are responsible for ensuring:

4.4.1.1 Employees receive appropriate security awareness training.

4.4.1.2 All of their staff are aware of and adhere to security requirements in relation to the use of information assets in their areas of responsibility.

4.4.1.3 Staff observe legal requirements regarding copyright and licensing of software.

4.4.1.4 Employee's access rights are reviewed (and revoked where necessary) and any identity/access cards, equipment, etc. are returned when staff change post or leave the Authority.

4.5 *Employees*

4.5.1 Employees and all other users of Neath Port Talbot County Borough Council ICT Systems, equipment and information resources are responsible for:

4.5.1.1 Ensuring awareness of and compliance with this and associated security policies.

4.5.1.2 Assisting in the security and protection of Council paper-based and electronic information, systems, equipment, documents, etc by complying with security requirements and guidelines contained in this and associated policies, etc.

4.5.1.3 Following ICT security incident reporting procedures when a suspected breach of security occurs.

4.5.1.4 Ensuring that appropriate security measures are employed to protect systems, data files and equipment.

4.5.1.5 Ensuring that confidential or sensitive information is protected from unauthorised disclosure.

4.5.1.6 Ensuring that they do not attempt to bypass security mechanisms which have been employed to protect Council information assets.

4.5.1.7 Ensuring that they do not install unauthorised programs/applications, store unauthorised files or play games on Authority ICT equipment.

4.5.1.8 Adhering to Authority policy in connection with the use of Internet and e-mail usage.

4.5.1.9 Ensuring that only ICT equipment which is purchased by and for the Authority is connected to Authority equipment, network, etc. This would include, but is not limited to, USB flash drives/memory sticks, mp3/mp4 players, mobile telephones, memory cards, etc.

4.5.1.10 Ensuring that Authority equipment is not connected to unauthorised machines or networks.

4.5.1.11 Not using Authority equipment for improper or unauthorised uses.

4.5.1.12 Ensuring that business critical data is not stored on a machine's local drive i.e. c: drive. All business critical data should be saved to a server.

4.5.1.13 Ensuring adherence to password guidelines i.e.:

- Not disclosing, sharing or writing down passwords,
- Ensuring passwords are sufficiently difficult to guess,
- Are at least 7 characters, capital and lower case (with at least one number),
- Are changed regularly and
- Are not reused for a minimum of 20 password changes

4.5.1.14 Ensuring that virus procedures are adhered to in the event of a contamination or possible infection i.e. do not disable any anti-virus product, do not transfer files from home (or any other external source) without confirming they are virus free and, if an infection is suspected, call the helpdesk immediately and do not use the machine until instructed to by IT support personnel.

5 POLICY

5.1 The majority of areas covered in this section are contained in specific corporate policies in more detail but are briefly touched upon here due to their relevance to Information Security.

5.2 *Physical and Environmental Security*

5.2.1 **Clear Screen/Clear Desk**

5.2.1.1 The Authority is working towards a clear screen and clear desk policy. Staff should, where possible, ensure that sensitive data is not accessible or viewable by unauthorised persons.

5.2.2 **Equipment Security**

5.2.2.1 All ICT hardware must be based in secure areas and be protected from damage, interference or screens being viewed by unauthorised persons.

5.2.2.2 Computers should be "locked" when left unattended and password protected screen savers should be utilised which are set to run after 5 minutes inactivity.

5.2.2.3 Portable devices must have appropriate security employed, for example, laptops should be stored in secure drawers or cabinets when not in use.

5.2.2.4 Digital media e.g. camera cards, DVD/CD, etc. must be stored securely.

5.2.2.5 Computer output should be held securely and not be viewable by unauthorised persons.

5.3 *Communications & Operations Management*

5.3.1 **Operational Procedures**

5.3.1.1 All regular operating procedures should be documented and access should be restricted.

5.3.1.2 Backups of critical data must be taken and tested to ensure that essential information can be recovered following a disaster or media failure.

5.3.2 **Change Control**

5.3.2.1 Any change to system programs and data, should be undertaken in a controlled manner. All changes should be documented and tested prior to implementation.

5.3.2.2 A separate 'test' environment should be set up for all systems. All new programs/systems should be acceptance tested and signed off by users before being implemented in a “live” environment.

5.3.3 **Segregation of Duties**

5.3.3.1 Line management must ensure that segregation of duties is in place wherever possible. This will minimise the risk of negligent or deliberate misuse of information systems.

5.3.4 **3rd Party Service Delivery**

5.3.4.1 Services being delivered by third parties should include agreed security arrangements, service definitions and service delivery agreements.

5.3.5 **Information Exchange**

5.3.5.1 Any exchanges of information between the authority and other organisations must be based on a formal exchange agreement and be compliant with relevant legislation and the Wales Accord on the Sharing of Personal Information (WASPI).

5.4 *Access Control*

5.4.1 Users will 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.

5.5 *System Development, Acquisition and Maintenance*

5.5.1 Security requirements should be agreed prior to the development or implementation of information systems to safeguard the confidentiality, integrity and availability of the data.

5.5.2 Security requirements (including how Person Identifiable Information (PII) is to be protected) should be included in specifications being drafted in connection with the acquisition of Information systems and the purchase must follow the conditions of the ICT Procurement Policy.

5.5.3 All ICT System development and acquisition should involve ICT staff at least in a consultancy role. Please contact the IT Helpdesk for advice and support.

6 LEGISLATIVE COMPLIANCE

6.1 All Neath Port Talbot County Borough Council employees must comply with legislative requirements, licensing agreements, etc.

6.2 This includes ensuring compliance with:

- Computer Misuse Act 1990
- Copyright Designs & Patents Act 1998
- Civil Contingencies Act 2004
- Data Protection 2018 (incorporating the General Data Protection Regulations)
- Electronic Communications Act 2000
- Equality Act 2006
- Freedom of Information Act 2000
- Health & Safety Act 1992
- Human Rights Act 1998
- Obscene Publications Act 1964
- Race Relations Act 1976 & 2000
- Regulation of investigatory Powers Act 2000

7 SECURE DISPOSAL OF INFORMATION

7.1 To prevent disclosure of personal, sensitive or business orientated data to unauthorised persons all electronic hardware must undergo data eradication prior to disposal. This can be carried out within the Authority or by an Authority approved contracted third party.

7.2 Digital media which is to be disposed of must be physically destroyed. Digital Media Disposal Cabinets have been obtained from the company contracted for confidential waste. Location of the cabinets can be obtained from the Facilities Management Section/Information Governance Team.

7.3 Non-electronic data must be disposed of confidentially and/or shredded.

8 AUDIT LOGGING

8.1 Audit logging is the process of recording various operational or security related events. Audit logs recording user activities, exceptions and information security

events should be produced and retained for a minimum of six months to assist in future investigations and access control monitoring.

8.2 The audit log must hold sufficient detail to allow the transaction events to be reconstructed and should include:

- The date and time of the event
- The users logon identification and IP or MAC address of the machine
- Event type and success or failure of the event
- Identification of the resource accessed
- Before and after the event information (if applicable)

9 BREACH OF THIS POLICY

9.1 Any breach of this Policy will be considered a serious disciplinary matter and will be dealt with in line with the disciplinary policy and procedures. A breach of this policy includes, but is not limited to, any act that:

- Exposes the Authority to actual or potential financial loss through the circumventing of IT security
- Involves the disclosure of confidential or sensitive information to unauthorised persons or the unauthorised use of corporate data
- Exposes the Authority to actual or potential legal action through the circumventing of IT security
- Involves the use of Authority data, which causes, for example, the law to be broken.

9.2 Any individual who suspects that this policy is being breached by another individual must report the violation immediately to a Line Manager, Head of Service or IT Help Desk. The incident will then, if appropriate, be reported to the Business Relations Manager who will maintain a log of all security incidents. The log will record reported incidents and any action taken in line with the ICT Incident Reporting Policy.

10 POLICY REVIEW

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

11 GENERAL QUERIES

11.1 Any questions regarding this policy or computer security in general should be addressed to Mrs Kath Phillips, bryncochciwprimary@npt.school
.