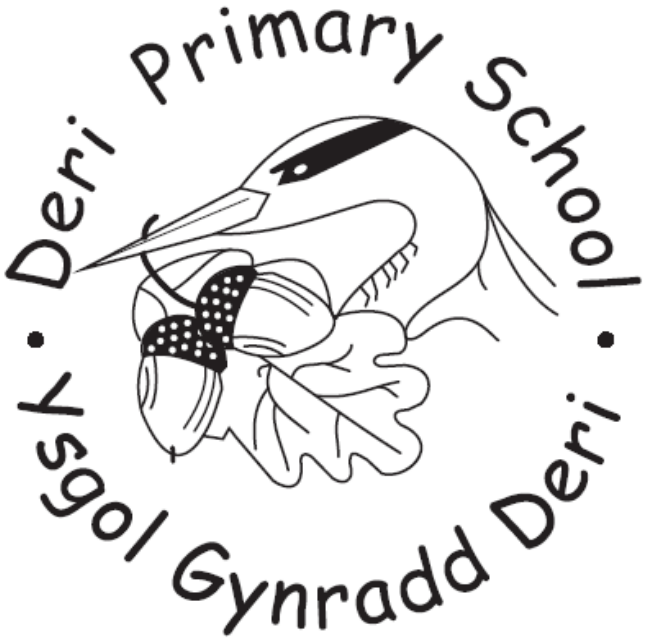
Internet Security Policy



Policy Reviewed: July 2020
Policy Review Date: July 2023
Signed

Headteacher: S E Martin

Chair of Governors:

Deri Primary School

Introduction

1.1 Caerphilly County Borough Council and Deri Primary School have, and will continue to make a large investment in the use of Information Technology which will be used to the benefit of all directorates. In most areas the use of Information Technology is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the Information Technology systems and data are maintained at levels which are appropriate for our organisation's needs. This security policy includes the key controls over information as defined in the new UK security standard BS7799.

2. Policy Objectives

2.1 There are three main objectives of this policy, which are detailed below: -
2.11 to ensure that all of Caerphilly County Borough Council's assets, staff, data and equipment are adequately protected on a cost-effective basis against any action that could adversely affect the Information Technology services required to conduct our business;
2.1.2 to ensure that staff are aware of, and fully comply with, all relevant legislation;
2.1.3 to create and maintain, within all divisions, a level of awareness of the need for Information Technology security to be an integral part of our day to day operations, so that all staff understand the need for Information Technology security and their own responsibilities in relation to it.

3 Application

3.1 The security policy is relevant to all Information Technology services irrespective of the equipment or facility in use and applies to: -
3.1.1 all employees and agents;
3.1.2 employees and agents of other organisations who directly or indirectly support or use the Information Technology services;
3.1.3 all use of Information Technology throughout Caerphilly County Borough Council.

4 Responsibility for Security

4.1 Information Technology security is the responsibility of Caerphilly County Borough Council as a corporate entity and all members of staff. The policy has been approved and adopted by the Corporate Management Team, Personnel Committee, the Council and the Trade Unions.
4.2 The Information Technology security policy will apply to all staff who use computer facilities, whether they be computer hosts, servers, network or PC users. All members of staff are to be issued with computer security instructions, which will specify their responsibilities and draw their attention to the penalties for not complying with the instructions.

4.3 Senior and line managers in Service Areas must be responsible for the implementation and policing of the Security Policy and will receive procedural notes to cover the key areas and their responsibilities.
4.4 All providers of Information Technology services must ensure the security, integrity and availability of data within the service provided.

5 Legislation

5.1 Caerphilly County Borough Council has to comply with all UK legislation affecting Information Technology. All employees and agents must adhere in the provisions detailed in the Acts detailed below, and they may be held personally responsible for any breach of current legislation and any future legislation that may be enacted:-
5.1.1 Data Protection Act, 1984
5.1.2 Copyright Designs and Patents Act, 1988
5.1.3 Computer Misuse Act, 1990
5.2 Information and guidance concerning the above Acts will be issued to all employees and agents on request.

6 Standards and Procedures

6.1 Physical Access

6.1.1 Precautions should be taken to ensure access to PCs and host terminals are restricted at all times to authorised personnel.
6.1.2 Equipment should be sited to reduce the risk of damage, interference and unauthorised access, this is of particular relevance to Service Area application and file servers.
6.1.3 All computer equipment must be security marked (with at least the organisation's post code) and be recorded on both the Service Area and Head of Information Technology services' inventories.
6.1.4 Where computer equipment is removed from buildings, for example, for use at home:-
6.1.4.1 prior approval in writing should have been obtained from the Head of Service specifying the reason for removal and the duration. Appropriate mechanisms should be employed by management to ensure the timely return of all equipment and that no damage has occurred; and
6.1.4.2 all of the provisions of this policy document equally apply.
6.1.5 No equipment purchased, leased or hired by a Service Area may be connected to the network or attached to any equipment connected to the network without prior authorisation of the Head of Information Technology Services or the Information Technology Operations Manager . This restriction also applies to any not owned, leased or hired by the organisation.
6.1.6 Users must not install, disconnect or move any Information Technology equipment themselves, this is the responsibility of the Information Technology Installation and Support team. All requests for movement of equipment should be directed to the Senior Installation and Support Officer.

6.2 Network Access

6.2.1 Access to the Council's private corporate data network is restricted to authorised employees and agents. Where access is required from external sources e.g. modem or laptop then prior authorisation from Head of Information Technology Services or the Information Technology Operations Manager will be necessary.

6.3 Software Access

6.3.1 Requests to provide access to the network or application systems must be made in writing, in advance, to the appropriate system controller by the relevant Service Area Manager. These requests must be made on the appropriate form, User Profile request (USR01),
6.3.2 Boot passwords must be set on laptop/notebook PCs to secure locally held information as they are highly portable and less physically secure. Boot passwords may be known by several users within an office to enable access to the PC. Adequate mechanisms should exist to ensure access to a PC by authorised personnel can always be achieved.
6.3.3 Terminals/PCs should not be left 'logged in' when unattended for any length of time e.g. at coffee breaks or lunchtime.
6.3.4 Passwords should be used to protect all systems and should not be written down or disclosed to others. Employees will be held liable for any misuse of a computer resulting from use of their password/username.
6.3.5 Passwords must be changed to a previously unused password when automatically prompted by the relevant system. Passwords should be set wherever possible to automatically expire if not changed at a pre-determined frequency.
6.3.6 Proper mechanisms should be in place to notify the Information Technology Security Officer of all leavers to facilitate the prompt removal of all access rights.
6.3.7 Passwords should be specific to individual staff and comprise of a minimum of 6 alpha/numeric characters arranged in such a fashion as will not be easily guessed.

6.4 Information

6.4.1 Information held on Caerphilly County Borough Council Information Technology facilities or subsequent output, for example, printed letters/tabulations, is the property of Caerphilly County Borough Council and is governed by the provisions of the Data Protection Act. Any purpose for which personal information is held about people must be registered under the Act by the nominated Data Protection Officer.
6.4.2 Information held should only be released to authorised persons, and Information Technology facilities supplied must only be used for authorised purposes. Information Technology facilities must not be used for personal or private work.
6.4.3 Any personal or sensitive data displayed upon unattended equipment must be protected, particularly in a public area, to ensure it may not be seen by anyone unauthorised to do so. This is applicable to information displayed

on visual display units, printed output and computer produced media such as microfiche.
6.4.4 All computer output no longer required by the organisation should be disposed of with due regard to its sensitivity. Confidential output should be disposed of in accordance with Caerphilly County Borough Council's current procedures.
6.4.5 Any queries relating to the provisions of the Data Protection Act and how it affects your operations should be directed via your line manager to the Head of Information Technology Services.
6.4.6 It is the responsibility of the Head of Service or other nominated officer to inform the Data Protection Officer of the need to register or notify under the Data Protection Act.

6.5 Internet Access

6.5.1 Only authorised users will be allowed access to the Internet via the Authority's network and only then for proper purposes. Internet site access must be relevant to the Council's business. Internet access will be available to authorised users subject to the necessary security firewall and content filters being in place.
6.5.2 Users must be aware that it is unacceptable to visit pornographic sites or to download this or any other form of unsuitable or offensive material from the Internet.

6..6 Virus Protection

6.6.1 All PCs (including laptops/notebooks) should be protected by virus detection software (obtainable from Information Technology Services) which should be subject to regular updates to guard against new viruses. This software must be operational at all times and never deactivated by the user. Any detected viruses must be reported to Information Technology Services immediately.
6.6.2 All disks/CD-ROMS must be virus checked prior to use in any of the organisation's computers. This especially applies where disks have been received from an external source.
6.2.3 Disks/CD-ROMS must not be inserted into PCs until the computer has either reached:-
6.6.3.1 the point where you log into the network, or
6.6.3.2 the windows screen on stand alone computers.

6.7 Software Copyright

6.7.1 The copying of proprietary software programs or the associated copyrighted documentation is prohibited and is an offence which could lead to personal criminal liability with the risk of a fine or imprisonment.
6.7.2 The loading of proprietary software programs for which a licence is required but not held is prohibited, and this is also an offence which could lead to a large fine or imprisonment. All software system disks and licences should be held by Information Technology Services.

6.7.3 Personal software should not be loaded onto organisation computers under any circumstances. If the software is deemed to be of use to the organisation then it should be duly acquired under licence via Information Technology Services.
6.7.4 Spot checks may be conducted by Information Technology Services and/or Internal Audit personnel to ensure compliance with these provisions. Authorised personnel from both Service Areas have rights of access to all systems, the power to seek explanations from members of staff concerned and the right to remove any unauthorised software found to have been installed.

6.8 Computer Misuse
6.8.1 All employees should be aware of their access rights for any given hardware, software or data and should not experiment or attempt to access hardware, software or data for which they have no approval or need to conduct their duties.

6.9 Contingency Planning
6.9.1 Security copies (back ups) should be taken at regular intervals dependant upon the importance and quantity of the data concerned. In the case of computer hosts and servers operating on the network these will be taken on behalf of users by Information Technology Services and other authorised personnel at agreed predefined frequencies.
6.9.2 In the case of networked personal computers the prime copy of all data files must be held on the network file server(s).
6.9.3 In the case of stand alone computers, users should be aware that internal fixed disks are susceptible to failure and should hold a copy of all data files on back-up media which should be stored securely, preferably in a different location to the equipment.
6.9.4 Arrangements must be made by the relevant Service Area Manager in conjunction with the Head of Information Technology Services, for critical systems/operations to continue in the event of complete computing failure.
6.9.5 Security copies should be stored away from the system to which they relate in a restricted access fireproof location. Security copies should be regularly tested to ensure that they enable the system/relevant file to be re-loaded in an emergency.
6.9.6 Security copies should be clearly marked as to what they are and when they were taken. Depending upon the system concerned they should provide for system recovery at various different points in time over a period of several weeks.

6.10 Acquisition and Disposal **of Information Technology Equipment**
6.10.1 All acquisitions should be in accordance with the provisions of the organisation's Information Technology strategy and its financial regulations and standing orders. All acquisitions of hardware and software must be made via or with the approval of the Head of Information Technology Services. All purchases of Information Technology equipment must be made via

Information Technology Services and accompanied by a business case justification.
6.10.2 The disposal or permanent handing over of equipment, media or output containing personal or sensitive data must be arranged via Information Technology Services to ensure confidentiality.
6.10.3 Prior to the disposal of any PCs, Information Technology Services should be consulted to arrange for the permanent removal of all data and programs unless the recipient is taking over the software licence or is authorised to use it.
6.10.4 Disposals must be in accordance with the provisions of financial regulations and standing orders which require the approval of Information Technology and Head of Procurement Services. Disposals will be conducted by Information Technology Services.

6.11 Suspected Security Incidents

6.11.1 It is the duty of all members of staff to report any suspected irregularities/fraud to their Head of Service and the Information Technology Security Officer, or Internal Audit as soon as possible. All employees involved shall regard such information as confidential.

7 Violations

7.1 Violations of this Information Technology security policy may include, but are not limited to, any act that:-
7.1.1 exposes Caerphilly County Borough Council to actual or potential monetary loss through the compromise of Information Technology security;
7.1.2 involves the disclosure of confidential information or the unauthorised use of personal and/or corporate data;
7.1.3. involves the use of data for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government body.
7.2 Any individual who has knowledge of a violation of this Information Technology security policy must report that violation immediately as detailed in the previous Section "Suspected Security Incidents".

8 Information Technology fraud & abuse

8.1 Definition of Incidents
Listed below are examples of fraudulent and abusive use of Information Technology, however such incidents are not limited to those listed.

8.1.1 Fraud

8.1.1.1 Fraud is defined as any act undertaken by an individual which results in, for example, private gain or benefit:
a) altering input in an unauthorised way
b) destroying/suppressing/misappropriating computer output
c) altering computerised data
d) altering or misusing programs (excluding virus infections)

8.1.2 Virus

8.1.2.1 Distributing a program with the intention of corrupting a computer process.

8.1.3 Theft

8.1.3.1 of data, software, or hardware. Copyright infringements may also be considered as theft.

8.1.4 Use of Unlicensed software

8.1.4.1 Using illicit copies of software, which may also infringe copyright law.

8.1.5 Private work

8.1.5.1 Unauthorised use of Caerphilly County Borough Council's computing facilities for private gain or benefit

8.1.6 Hacking

8.1.6.1 Deliberately gaining unauthorised access to a computer system, usually through the use of communications facilities

8.1.7 Sabotage

8.1.7.1 Interfering with the computer process by causing deliberate damage to the processing cycle or to equipment.

8.1.8 Misuse of personal data

8.1.8.1 ficial "browsing" through computer records and breaches of data protection legislation.

8.1.9 Producing pornographic, or other unsuitable offensive material

8.1.9.1 Introducing pornographic or other unsuitable offensive material, for example, by downloading from the internet.

8.2 Disciplinary Process

8.2.1 Caerphilly County Borough Council views computer security very seriously and any breach of this policy could lead to disciplinary action being taken against employees under the Council's agreed disciplinary procedure.

9 Procedural Notes on Security Policy for Senior and Line Management

9.1 It is your responsibility to ensure correct implementation and continuation of the Information Technology Security Policy in your division.

9.2 Regular reviews must be undertaken to ensure this policy is being adhered to, we suggest these reviews are performed at least every 6 months.

9.3 Detailed implementation requirements can be found in the document "Computer Security Instructions".

9.4 All staff must be made aware that any breach of this Security Policy could lead to action being taken under the Council's agreed disciplinary procedures.

9.5 Information Technology equipment should only be removed from Caerphilly County Borough Council's premises with appropriate authorisation from a Section Manager. The Section Manager should specify the reason for the removal, the duration, serial number(s), date required, expected return date, actual date returned and checked for any damage. An appropriate form is attached, which should be completed by both the user and Section Manager.

9.6 Proper mechanisms must be in place to notify the Information Technology security officer of all leavers to ensure the prompt removal of all access rights.

9.7 The effective operation of controls should prevent most incidents from occurring.

9.8 Section Management must convey to staff the commitment necessary to ensure that the security policy is adhered to at all times.
9.9 Good staff supervision is necessary to ensure security levels are maintained.
9.10 Section Management has a responsibility to ensure adequate division of duties.
9.11 Section Management must ensure that staff receives adequate training on relevant systems.
9.12 Section Management must ensure security responsibilities are assigned to specific individuals and defined clearly.
9.13 It is the responsibility of line managers to encourage staff to adhere to the Information Technology security policy.

Equipment Loan

Equipment:

Serial Number:

Loaned to:

Loan Date:

Expected Return Date:

Service Area:

Designation:

Request Made By:

Signature: **Date:**

Authorised By:

Signature: **Date:**

Returned:

Signature: **Date:**

Serial Number:

Checked By:

11 Computer User Security Instructions

11.1 All Information Technology users will be issued with a unique user profile and password for network access and relevant application access.
11.2 Users should change passwords every 30 days or when automatically prompted by the relevant software to maintain confidentially.
11.3 All profile requests for new, amendments and deletions must be provided to Information Technology on the user profile request form (USR01) and authorised by appropriate Section Managers.
11.4 No user must disclose their password to another user in order for them to gain access with their profile. Non compliance could lead to action being taken against employees under the Council's agreed disciplinary procedure.
11.5 All users must conform to the following acts, and any subsequent acts:
11.6 Data Protection Act 1984
11.7 Copyright, Designs and Patents Act 1988
11.8 Computer Misuse Act 1990
11.9 All business critical and confidential data should be stored on the appropriate network server drive to ensure unauthorised access is avoided and to ensure a backup is created on a regular basis, providing a recovery path in an emergency.
11.10 All information held by Caerphilly County Borough Council and subsequent output, e.g. tabulations, letters is confidential and users should not convey this to unauthorised personnel.

Appendix A

INFORMATION TECHNOLOGY
USER PROFILE REQUEST

Usr0

Contact Name:

Telephone Number:

Service Area:

Action required: **Create / Change / Delete** (*Delete as appropriate)*

User Full Name:

User profile: *(Change / Delete action only)* ***Not to be used for new user***

Software Application:

Access Required or Existing user to copy:

Date required:

Authorised Signature: **Date***:*

For Information Technology use only:

Date request received: **Signature***:*

Date profile updated: **Signature***:*

Date application updated: **Signature***:*

Date user informed: **Signature***:*

13 Glossary of Terms

13.1 Information Technology equipment

Personal computers, host terminals, printers, modems, telephones, PC servers, host computers, laptops, notepads.

13.2 Data

All information held on