Education, Leisure and Libraries

School based staff Information Security Policy

Table of Contents

1 INFORMATION SECURITY

1.1 Introduction

The Governing Body and CCBC have, and will continue to make a large investment in the use of Information Technology, which will be used to the benefit of all its staff and pupils. Information systems and the data held within them are essential for day-to-day operational, financial and general information needs. It is therefore essential that the availability, integrity, and confidentiality of these assets are protected against any potential security incident.

The Information Security Policy is relevant to all information technology services provided, irrespective of the equipment or facility in use, and applies to: -

a) All employees and agents;

b) Employees and agents of other organisations who directly or indirectly support or use the information technology services provided;

c) All use of information technology throughout the school

The Governing Body takes information security very seriously, and any breach of this policy could lead to disciplinary action being taken against employees under the Schools agreed disciplinary procedure.

1.2 Definition

Information Security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities.

We must protect the confidentiality, integrity, and availability of the schools information assets.

To protect the confidentiality of our information assets we must ensure that our information is accessible to authorised users only.

To protect the integrity of our information assets we must safeguard the accuracy and completeness of our information and processing methods.

To protect the availability of our information assets we must ensure that our users have access to information and its associated assets in conjunction with agreed service levels.

1.3 Objectives and scope

There are three main objectives of this policy, which are detailed below: -

1. To ensure that the confidentiality, integrity, and availability of the school/councils information assets, are adequately protected from all threats, whether internal or external, deliberate or accidental;

2. To ensure that staff are aware of, and fully comply with, all current and relevant security policies and legislation;

3. To create and maintain, within all departments, a level of awareness of the day to day importance of information security, and for all staff to understand their own information security responsibilities.

2 SECURITY POLICY STATEMENT

2.1 Security Policy Statement

Objective

The objective of information security is to protect the confidentiality, integrity, and availability of the organisations information assets.

Policy

- The Governing Body has approved the Security Policy Statement.
- The purpose of the Information Security Policy is to protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.
- It is the policy of the organisation to ensure that:
  - Information will be protected against unauthorized access;
  - Confidentiality of information will be assured;
  - Integrity of information will be maintained;
  - Regulatory and legislative requirements will be met;
  - Business continuity plans will be produced, maintained and tested;
  - Information security training will be available to all staff that use IT services;
  - All breaches of information security, actual or suspected, will be reported to, and investigated by the Councils Information Security Officers.
- Business requirements for the availability of information and information systems will be met.
- It is the responsibility of all staff to adhere to the Information Security Policy.

3 POLICIES, LEGISLATION, TRAINING AND AWARENESS, BUSINESS CONTINUITY, POLICY VIOLATIONS.

3.1 Policies

3.1.1 Email

EMAIL USAGE POLICY

The purpose of this policy is to ensure the proper use of the schools and Caerphilly County Borough Council's email system and make users aware of what the governing body deems as acceptable and unacceptable use of its email system. The Governing Body reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately. This policy is applicable to all school based employees and agents.

LEGAL RISKS

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- **If you send emails with any libelous, defamatory, offensive, racist or obscene remarks, you, CCBC and the School can be held liable.**
- **If you forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you, CCBC and the School can be held liable.**
- **If you unlawfully forward confidential information, you, CCBC and the school can be held liable.**
- **If you unlawfully forward or copy messages without permission, you, CCBC and the school can be held liable for copyright infringement.**
- **If you send an attachment that contains a virus, you, CCBC and the school can be held liable.**

In order to minimise the legal risks to both yourself and to the organisation, it is prohibited to:

- **Send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.**
- **Forge or attempt to forge email messages.**
- **Disguise or attempt to disguise your identity when sending mail.**
- **Send email messages using another person's email account.**
- **Access your email from anywhere other than a CCBC school or a personal home computer; never from a public access computer such as that found in a cyber café or library**

It is not necessary to obtain permission of an outside sender to forward that person's email, however please have regard for passing on indiscriminately something that was copyright or covered by the data protection act (personal data)

BEST PRACTICES

CCBC considers email as an important means of communication and recognises the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an email as they would for any other communication. Therefore the governing body wishes users to adhere where possible to the following guidelines:

- **Writing emails:**
  - **Write well-structured emails and use short, descriptive subjects.**
  - **Email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended**

with 'Best Regards'. The use of Internet abbreviations and characters such as smileys however, is prohibited.

- **External email signatures must include your name, job title and department/school. A disclaimer will be added underneath your signature (see Disclaimer)**
- **Users should spell check all emails prior to transmission.**
- **Do not send unnecessary attachments.**
- **Do not write emails in capitals.**
- **If you require any action by the recipient ensure they are included in the "To' field not the CC or BCC fields.**
- **If you forward emails, state clearly what action you expect the recipient to take.**
- **Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, or use other means of communication.**
- **Only mark emails as important if they really are important.**

- **Newsgroups:**
  - **Users need to request permission from their supervisor before subscribing to a newsletter or news group.**
- **Maintenance:**
  - **Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.**

PERSONAL USE

It is strictly forbidden to use CCBC's email system for anything other than legitimate business purposes. For example, the sending of personal emails, chain letters, junk mail, jokes and executables is prohibited. All messages distributed via the Council's email system are CCBC's property.

The Council and The Trade Unions have agreed that the email system may be used for communication between an individual and his or her trade union, or vice versa, for matters relating to the individual's employment with the Authority. This will not be classed as personal use.

CONFIDENTIAL INFORMATION

Please be aware of the security implications when sending confidential information via the email system.

PASSWORDS

The use of passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document. If requested passwords must be made known to the Council.

ENCRYPTION

Users may not encrypt any emails without obtaining written permission from their supervisor. If approved, the encryption key(s) must be made known to the council.

EMAIL ACCOUNTS

All email accounts maintained on our email systems are the property of CCBC. Network passwords should not be given to other people and should be changed on a regular basis.

SYSTEM MONITORING

The Council has the right in law to monitor the use of the email system in order to ensure the proper and lawful use of the system. Such monitoring will be undertaken in line with the Data Protection Code, Part 3 Monitoring at Work. Such monitoring will be primarily confined to address/heading unless there is a valid and defined reason to examine content.

Users expressly waive any right to privacy in anything they create, store, send or receive on the Council's computer system and accept that monitoring, as set out above will take place. If there is evidence of a failure to follow the guidelines set out in this policy, CCBC reserves the right to take disciplinary action.

3.1.2 Internet

INTERNET USAGE POLICY

The purpose of this policy is to ensure the proper use of the schools and Caerphilly County Borough Council's Internet facilities and make users aware of what the governing body deems as acceptable and unacceptable use of the Internet. The governing body reserves the right to amend this policy at its discretion, subject to consultation with relevant staff associations. In case of amendments, users will be informed appropriately. This policy is applicable to all school based employees and agents.

LEGAL RISKS

Internet facilities enable the user to access a very wide range of information, including personal data, linking to large numbers of computers and other individuals across the world. In this relatively uncontrolled environment, it is particularly important that users are aware of and conform to legal requirements:

- **If you view, create, access, download or publish material that is pornographic, libelous, defamatory, offensive, racist or obscene, you, the school and Caerphilly County Borough Council can be held liable.**
- **If you unlawfully view, create, access, download or publish confidential or personal information, you, the school and Caerphilly County Borough Council can be held liable.**
- **If you unlawfully or without permission view, create, access, download or publish material that is copyrighted, you, the school and Caerphilly County Borough Council can be held liable for copyright infringement.**

Additionally there are a number of Acts that can be applied to Internet use:

- **The Data Protection Act, 1998**
- **The Computer Misuse Act, 1990**
- **The Copyrights, Designs and Patents Act, 1988**
- **The Regulation of Investigatory Powers Act, 2000**
- **Electronic Communications Act, 2000**
- **Freedom of Information Act, 2000**
- **Monitoring at Work - Code of Practice, 2003**

ACCEPTABLE USE

The primary purpose for a user to have access to Internet facilities is to enhance the efficiency and effectiveness of that user's work for the school.
The Schools and Caerphilly County Borough Council's Internet facilities must only be used for legitimate business purposes, personal use is prohibited.
The Council and The Trade Unions have agreed that the Internet system may be used for communication between an individual and his or her trade union, or vice versa, for matters relating to the individual's employment with the Authority. This will not be classed as personal use.

UNACCEPTABLE USE

Internet facilities must not be used to view, create, access, download or publish material that is:

- **Pornographic or Adult**
- **Racist, offensive, or derogatory**
- **Obscene**
- **Bullying**
- **Violent**
- **Fraudulent**

- **Likely to cause harassment to others**
- **Confidential**
- **Prejudicial to the organisations best interests**
- **Not relevant to the business of the organisation**
- **Likely to irritate or waste time of others**
- **Likely to breach copyright**

It is unacceptable to use Internet facilities for:

- **Gambling**
- **Shopping (including online auctions, holidays, cars etc)**
- **Gaming**
- **Instant Messaging (IM) (e.g. Microsoft Messenger)**
- **Utilising Peer to Peer (P2P) applications (e.g. Napster or Kazaa)**
- **Accessing personal web mail (e.g. Hotmail, Yahoo, Wanadoo)**
- **Publishing or creating personal websites or pages**
- **Accessing chat rooms**
- **Accessing newsgroups other than those on an approved list**

It is prohibited to use Internet facilities for downloading:

- **Software** *
- **Music, videos, etc***
- **Games***

* **If required, business related software may be downloaded provided it is from a legitimate and secure source and that a member of staff from IT Services or relevant IT Support area carries out the download. The software must be virus checked before installation.**

Any accidental access to inappropriate content must be reported to Headteacher/IT Helpdesk.

SECURITY

To address the security risks posed by having access to the Internet the Council and the school has a number of security controls (Anti-Virus applications, Firewalls and Web-filtering software) in place to protect its network and information systems.

It is prohibited to:

- **Circumvent, or attempt to circumvent these or any other security controls that are in place.**
- **Gain or attempt to gain unauthorised access to information (e.g. by introducing keyloggers, spyware or malware).**
- **Attempt to test or detect weaknesses in the security infrastructure (e.g. testing firewalls, cracking passwords).**
- **Attempt or intentionally disrupt the normal functioning of the Internet or related services (e.g. by downloading illegal software or introducing viruses).**

SYSTEM MONITORING

The Council and Governing Body has the right in law to monitor the use of the Internet systems in order to ensure the proper and lawful use of the system. Such monitoring will be undertaken in line with the Data Protection Code, Part 3 Monitoring at Work.

Users expressly waive any right to privacy in anything they create, store, send or receive on the Schools and Council's computer system and accept that monitoring, as set out above will take place. If there is evidence of a failure to follow the guidelines set out in this policy, The Governing Body and Caerphilly County Borough Council reserves the right to take disciplinary action.

The Council and the school (Delete if not appropriate to school) uses web-filtering software to control access to websites and pages and to monitor user activity. The software will block access to websites, pages or content that is inappropriate or not relevant to the business of the Council.

GLOSSARY OF TERMS:

Firewall	**A system designed to prevent unauthorised access to or from a private network.**

Web mail	**An E-mail account that can be accessed from anywhere in the world via the Internet.**
Virus	**A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.**
Keylogger	**Software that has the capability to record every keystroke entered via a keyboard.**
Spyware	**Software that gathers user information through an Internet connection without his or her knowledge.**
Malware	**Short for malicious software, software designed specifically to damage or disrupts a system, such as a virus.**
Peer to Peer (P2P)	**A type of Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives or servers.**
Instant Messaging (IM)	**A communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet.**
Chat Room	**A virtual room where a chat session takes place.**

QUESTIONS

If you have any questions or comments about this Internet Policy, please contact the IT Helpdesk.

3.2 Legislation

Caerphilly County Borough Council and the Governing Body 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 future legislation that may be enacted: -

a) The Data Protection Act, 1998;
b) The Computer Misuse Act, 1990;
c) The Copyrights, Designs and Patents Act, 1988;
d) The Regulation of Investigatory Powers Act, 2000;
e) Electronic Communications Act, 2000;
f) Freedom of Information Act, 2000.

Information and guidance concerning the above Acts will be issued to all employees and agents on request.

3.3 Policy violations

Violations of security procedures established within this Information Security Policy must be reported to the Governing Body or Education IT. Violations may include, but are not limited to, any act that: -

a) Exposes Caerphilly County Borough Council or the School to actual or potential monetary loss through the compromise of information technology security;

b) Involves the disclosure of confidential information or the unauthorised use of personal and/or corporate data;

c) Involves the use of data for illicit purposes, which may include violation of the law, regulation, or any reporting requirement of any law enforcement or government body.

4 SECURITY RESPONSIBILITIES AND SECURITY INCIDENTS

4.1 Security responsibilities

Information security is the responsibility of Governing Body and all members of staff, and agents.

The Information Security Policy will apply to all staff and agents that use computer facilities, whether they are computer hosts, servers, network, PC, or mobile users.

Senior and line managers are responsible for the policing of the Information Security Policy. Any queries or question regarding the policy, please contact the Governing Body or IT Helpdesk.

4.2 Security Incidents

It is the duty of all members of staff to report any suspected breach of information security to their Head of Service and the IT Security Officers.

Examples of information security events and incidents are:

a) Loss of service, equipment or facilities;

b) System malfunctions or overloads;

c) Human errors;

d) Non-compliance with policies, guidelines, rules;

e) Breaches of physical security arrangements;

f) Uncontrolled system changes;

g) Malfunctions of software or hardware;

h) Access violations.

5 SECURITY RULES

5.1 Security rules

5.1.1 Computer Equipment

The Governing Body is responsible for the control and maintenance of all computer equipment within the school.

No equipment may be connected to the network or attached to any equipment connected to the network without prior authorisation of the Head Teacher or Governing body

> Note: This is to protect the schools network against data theft and the introduction of virus's (it is a requirement of the Data Protection Act to put in place reasonable measures to prevent data theft) If you require further guidance on this matter please contact the IT Helpdesk.

It is forbidden to install, disconnect or move any computer equipment.
It is forbidden to remove any information asset stickers.

Desktop, servers, and portable computers must not have any software installed, removed or modified without authorisation from the Head Teacher/Governing Body

Computer equipment must not be used for any personal or private work.

Computers must not be left unattended, logoff your computer when you leave your desk, power off your computer when you finish work.

5.1.2 Network Access

Access to the Schools private data network is restricted to authorised employees and agents.

Staff (agents) from outside organisations or companies must not be given access to any computer systems without permission of the Head Teacher/Governing Body. When allowing third parties to access data networks schools should ensure that all risks are carefully considered, the data protection act requires all personal data to be adequately protected. It is advised that schools seek advice on this matter by contacting the IT Helpdesk prior to allowing any third party access.

5.1.3 Data Storage Drives - Usage

Information stored on any storage drives must not breach the Data Protection Act 1998, and confidential information must not be made available for any unauthorised access.

The following must not be stored on any network drives:

- Information that is not related to the business of the school
- Pornographic, offensive, derogatory or discriminatory material.
- Unauthorised or illegal software.

- Non-business images or executable files/programs.
- Games or non-business applications.

5.1.4 Passwords

Passwords must not be disclosed to anyone, written down or displayed in a way, which would allow the password to become known to unauthorised staff or members of the public.

The use of another persons Login ID and password is strictly forbidden. Login information is specific to the user the login was created for and must not be shared with other users. Employees will be held liable for any misuse of a computer resulting from the use of their Login ID and password.

Passwords should be alphanumeric i.e. a mixture of letters and numbers. They must have a minimum length of 6 characters and a maximum length of 10 characters, and they must start with letter.

5.1.5 Information

Information held on Caerphilly County Borough Council's or the schools, information technology computers or subsequent output, for example, printed letters/tabulations, is the property of Caerphilly County Borough Council or the school respectively and is governed by the provisions of the Data Protection Act, 1988.

The Data Protection Act, 1988 requires that all computer processing of data relating to living individuals, i.e. personal data, be registered with the Crown appointed Registrar. Information required for registration includes details of the type of data, the purpose for which the data is held, and the sources and disclosure of data. There are a number of offences, which, if the provisions of the Act are not complied with, will affect the Council, School and its employees.

The general provisions of the Act are:-

- all processing of personal computer data must be registered;
- personal data must only be processed as specified in the registration;
- computer personal data must not be disclosed to an unauthorised person;
- on request, and when appropriate for a fee; individuals have a right to a written copy of the data held; requests should be directed to the Headteacher or Governing Body
- appropriate security measures must be taken to protect computer personal data.

Any queries relating to the provisions of the Data Protection Act should be directed To the Headteacher or Governing Body

The Head Teacher/Governing body are responsible for the lawful processing of information under the Data Protection Act, and are deemed under this law to be the Data Controllers. Further information on both the Data Protection Act and the Freedom of Information Act can be found on the Information Commissioners website at http://www.ico.gov.uk/

5.1.6 Virus Protection

All Caerphilly County Borough Council computers are protected by virus detection software. This software must be operational at all times and never deactivated by the users. Any detected viruses must be reported to IT helpdesk immediately.

All software (whatever media) must be virus checked before it is copied to any Caerphilly County Borough Council, personal computer, server, or laptop.

5.1.7 Software Copyright

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.

The loading of proprietary software programs for which a licence is required but not held is prohibited.

Further information on Copyright laws can be found on the Intellectual Property Office website at http://www.ipo.gov.uk

5.1.8 Computer Misuse

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 access to conduct their duties.

This following is regarded as misuse of the organisations information assets.

Fraudulent activity such as: -

- altering input in an unauthorised way;
- destroying, suppressing, misappropriating computer output;
- altering computerised data;
- altering or misusing programs.

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

Theft of data, software or hardware, including Copyright infringements.

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

Unauthorised use of the schools or Caerphilly County Borough Councils computer facilities for private gain or benefit.

Unauthorised disclosure of information from computer input or output to unauthorised personnel.

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

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

Introduction of pornographic or other unsuitable offensive material, on to the corporate network.

> Further information on Computer Misuse laws can be found on the Office of Public Sector Information website at http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

5.1.9 Acquisition and Disposal of Information Technology Equipment

All acquisitions must be in accordance with the provisions of the organisation's information technology strategy and its financial regulations and standing orders.

All acquisitions of additional hardware and software must be made via or with the approval of the Headteacher/Governing Body.

Prior to the disposal of any PCs, IT 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.

Disposals must be in accordance with the provisions of financial and environmental regulations and standing orders, which require the approval of the Headteacher/Governing Body.

6 POLICY COMPLIANCE

I have read, understood and acknowledge receipt of the Information Security Policy. I will comply with the guidelines set out in this policy (including the Email and Internet policies) and understand that failure to do so might result in disciplinary or legal action.

Signature: _____ **Date**:_____

Printed Name:_____

Designation:_____

School:_____

Site/Location:_____

Telephone Number:_____

Please tick for access required:

Network User ID ☐ _____

Email ☐ _____

Please return to Head Teacher