


Information Security Policy

Owner and version control

Responsibility:	Simon Little, Managing Director	Date doc. created:	V4 February 2022
Print name sign off:	Simon Little, Managing Director	Last review date of doc:	March 2023
Signature:		Next review date:	March 2024

Introduction

Computer systems, networks and the information held on them are an integral part of business at Best Practice Network. In a knowledge-driven organisation such as ours, information relating to learning and teaching, research, administration and management is a substantial and valuable asset which needs to be protected.

Information access & security principles

Appropriate information access and security involves knowing what information exists, permitting access to all who have a legitimate need and ensuring the proper handling of information.

Information should be protected in line with relevant legislation, notably those laws relating to data protection and freedom of information. In particular, this means that the data stored on Best Practice Network systems must be accurate, complete and consistent with other information.

This statement has been established in order to:

- Protect our asset
- Safeguard the information contained within our systems.
- Reduce business and legal risk
- Protect the good name of the company

Violations

Failure to comply with this policy may result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

Statement of responsibility

Managers must:

1. Ensure that all appropriate personnel are aware of and comply with this policy
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy
3. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives
4. Monitor implementation and provide appropriate support and guidance to assist personnel to fulfil their responsibilities under this directive

Everyone who uses BPN-provided internet or internet email should:

1. Ensure that all communications are for professional reasons and that they do not interfere with their productivity
2. Be responsible for the content of all text, audio, or images that they place or send over the internet. All communications should have their name attached
3. Not transmit copyrighted materials without permission
4. Know and abide by all applicable company policies dealing with security and confidentiality of company records
5. Run a virus scan on any executable file(s) received through the internet (this is normally done automatically by our installed anti-virus software but if in doubt rerun the scan and act on any warnings)
6. Avoid transmission of confidential client or supplier information. However, if it is necessary to transmit this, employees are required to take reasonable steps to ensure that information is delivered to the right person and that they have a legitimate use and are authorised to receive such information and that **where that information includes personal data that it is encrypted appropriately.**

The internet and email

The internet is a very large, publicly accessible network that has millions of connected users and organisations worldwide. Access to the internet and email is provided to employees for the benefit of Best Practice Network, its consultants and clients. However, the internet is also a source of risks and inappropriate material. BPN-provided access to the internet may not be used for any activity that is not related to BPN business.

Policy

All Best Practice Network personnel need to be responsible and productive internet users. To protect the company's interests, the following protocol has been established for using the internet and email.

Acceptable use

Best Practice Network personnel using the internet are representing the company and are responsible for ensuring that the service is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial websites
- Accessing databases for information as needed
- Using email for business contacts

Unacceptable use

Best Practice Network personnel must not use the internet for purposes that are illegal, unethical, harmful to the company, or non-productive. Examples of unacceptable use are:

- Sending or forwarding chain email, i.e., messages containing instructions to forward the message to others
- Conducting a personal business using company resources
- Transmitting any content that is offensive, harassing, or fraudulent

File downloads which are not resources from our own or stakeholder websites are **not** permitted unless specifically authorised by the IT Manager.

Copyrights

Employees using the internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the company and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the internet are the property of the company and *may be regarded as public information*. Best Practice Network reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

The basic principle is **don't** put anything into your email messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.

Computer viruses

Computer viruses are programs designed to make unauthorised changes to programs and data. Viruses can destroy corporate resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure
- Defences against computer viruses include protection against unauthorised access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software

Best Practice Network will therefore:

1. Install and maintain appropriate antivirus software on all computers
2. Respond to all virus attacks, destroy any virus detected, and document each incident

Individual's responsibilities

These directives apply to all Best Practice Network personnel:

1. You shall not knowingly introduce a computer virus into company computers
2. You shall not load discs, USB drives or data cards of unknown origin
3. Incoming media shall be scanned for viruses before they are read

4. If you suspect that your workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IT Manager

Spyware

Spyware and adware can compromise system performance and allow sensitive information to be transmitted outside the organisation. Spyware installation programs can launch even when users are performing legitimate operations, such as installing a company-approved application. As a result, combating spyware requires user vigilance as well as ICT management and control.

Best Practice Network will therefore

1. Install and update appropriate anti-spyware software on all computers
2. Respond to all reports of spyware installation, remove spyware modules, restore system functionality, and document each incident

Therefore:

1. Do not knowingly allow spyware to install on company computers
2. Immediately report any symptoms that suggest spyware may have been installed on their computer

Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. More often than not the attacks are triggered by downloading and running an executable from an email disguised as something else. The key here is that these attacks usually start at the user level so you must take care when opening attachments and clicking on links. If you believe that you have triggered a ransomware attack then you must:

1. Remove your network cable as quickly as possible
2. Power down your machine
3. Contact helpdesk to report the issue

Access codes and passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorised personnel have access. This access shall be restricted to only those areas that are appropriate to their specific role and duties.

Best Practice Network's IT Manager shall be responsible for the administration of access controls to all company computer systems.

The IT Manager will be responsible for the secure storage of any administrative passwords that need to be documented.

When using BPN systems and internet:

1. You are responsible for all computer transactions that are made with your username and password
2. You should not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained
3. You should not use passwords that will be easily guessed by others
4. You should log out when leaving a workstation for an extended period (use of the Windows key + L will lock Windows computers)
5. You should not attempt to access the accounts of other users

Physical security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorised access, and environmental hazards. A separate business continuity plan is in place to ensure data is securely backed up daily to minimise data loss in the event of a disaster or system failure. All backup data is encrypted in transmission and whilst in storage to protect it from unauthorized access.

1. Discs and portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up
2. Discs should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS)
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided
5. The IT Manager is responsible for all equipment installations, disconnections, modifications, and relocations, and other personnel are not to perform these activities unsupervised. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT Manager
6. Best Practice Network personnel shall not take shared portable equipment such as laptop computers out of the office without the informed consent of their manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used
7. Best Practice Network personnel should exercise care to safeguard the valuable electronic equipment assigned to them. Those who neglect this duty may be accountable for any loss or damage that may result

Legal Responsibilities

It is Best Practice Network's policy to comply with all laws regarding intellectual property including the General Data Protection Regulation 2016, Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Freedom of Information Act 2000, Computer Misuse Act 1990, Official Secrets Acts 1911-1989, The Terrorism Act 2000, The Anti-Terrorism, Crime and Security Act 2001 and the Copyright, Design and Patents Act 1988.

Best Practice Network is aware that violations of copyright law expose the company and the responsible personnel to the civil and criminal penalties which may include fines and a prison sentence.

Best Practice Network will

1. Maintain records of software licenses owned by the company
2. Periodically (at least annually) scan company computers to verify that only authorised software is installed

Best Practice Network personnel shall not:

1. Install software unless authorised by IT Manager. Only software that is licensed to or owned by Best Practice Network is to be installed on Best Practice Network computers
2. Copy software unless authorised by IT Manager
3. Download software unless authorised by IT Manager

Email

Email is routed through 3rd party scanning service Mimecast for virus and spam scanning. Mail is further scanned by a Sophos SG firewall which includes sandbox scanning for behaviour analysis of attachments that may contain zero-day malware. The same is done in reverse for outgoing mail. Mimecast also keeps an archive copy of all incoming and outgoing mail that can be accessed should there be an issue with the internal Exchange mail server.

Firewall

The Sophos SG firewall acts as a transparent proxy server to scan web traffic for malware. Users authenticate their connection to the proxy server with their Active Directory credentials using Single Sign On where possible.

The firewall also features Intrusion Prevention and Advanced Threat Protection scanning to monitor for known threats and behaviour patterns in internet traffic passing through it.

Server Anti-Virus

The servers are protected with Sophos Central Server Advanced. This includes Cryptoguard ransomware protection to protect files against encryption by locally and remotely run ransomware.

Desktop Anti-Virus

Endpoints are protected by Sophos Central Endpoint Standard with Intercept-X added for extra protection against zero-day malware, ransomware, browser exploits etc.

Remote access

Remote access to the network is controlled via an SSL VPN, protected with 2 factor authentication.

Acknowledgment of Data Security - ICT Statement

This form is used to acknowledge receipt of, and compliance with, the Information Security Policy

Procedure

Complete the following steps:

1. Read the Data Security Statement
2. Sign and date in the spaces provided below
3. Return **this page only** to the IT Manager

Signature

By signing below, I agree to the following terms:

- i. I have received and read a copy of the "Data Security Statement" and understand the same
- ii. I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and confidential information about Best Practice Network and its clients or its suppliers, and that this is and remains the property of the company at all times

iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at Best Practice Network) otherwise disclose, or allow anyone else to copy or duplicate any of this information or software

iv. I agree that, if I leave Best Practice Network for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control

Signature: _____

Name: _____

Date: _____