Acceptable Use of IT Systems Policy

Document title	Acceptable Use of IT Systems Policy		
Reference No.	IT-AU	**Version**	5.0
Author	Pete Faulkner – IT Manager		
Reviewed by	Saul Muscat, Head of Enrolments (DCO)		
Authorised by	Luke Muscat, Managing Director		
Issue date	27.04.2022		
Review due	27.04.2023		

DOCUMENT CONTROL

Version	Name	Comment	Date
0.1	L Muscat	New Issue	09/07/2018
0.2	A Dann	Updated- Social media encouragement for educational purposes.	01/04/19
0.3	A.Dann	Review	01.04.20
0.4	S Muscat	Annual review completed, clarification in wording in points 4.1.1 and 4.1.2	01.04.2021
0.5	Pete Faulkner	Full policy re-write	27.04.2022

Acceptable Use of IT Systems Policy

1 Introduction

B2W Group takes the subject of information security very seriously. We have a duty to protect the information that we collect and use for the benefit of the organization and its customers. As an employee, you will be expected to comply fully with all of the information security policies that are in place and to report any breaches of these policies of which you may become aware.

This document gives a summary of the main points of the relevant policies. Where a role involves tasks or access to information that is the subject of a more detailed topic-specific policy, staff will be made aware of their additional responsibilities as part of their role. Anyone breaching information security policy may be subject to disciplinary action. If a criminal offence has been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, please seek advice from your immediate manager in the first instance.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to B2W Group systems.

The following topic-specific policies and procedures are relevant to this document:

- *Information Security Policy*
- *Electronic Messaging Policy*
- *Internet Acceptable Use Policy*
- *Mobile Device Policy*
- *BYOD Policy*
- *Teleworking Policy*
- *Privacy and Personal Data Protection Policy*
- *Cloud Computing Policy*
- *Asset Handling Procedure*
- *Software Policy*
- *Access Control Policy*
- *Anti-Malware Policy*
- *Information Security Incident Response Procedure*
- *IP and Copyright Compliance Policy*
- *Social Media Policy*
- *HR Security Policy*
- *Asset Management Policy*

2 Usage – Company Devices

Employees, Associates and learners in receipt of a company owned device should be aware that the device, accessories, software and operating system remain the property of B2W Group and are provided on a loan basis only. Additional software MUST NOT be installed, nor hardware modifications made, without authorisation from the IT Team.

Personal use of the ICT system is authorised within reasonable limits as long as it does not interfere with or conflict with business use. Employees, Associates and learners are responsible for exercising good judgement regarding the reasonableness of personal use.

Learners will only be issued with ICT equipment to help them with their studies when expressly approved at Director-level. All devices must be returned at the end to the tutor facilitating the training.

3 Acceptable use policy

The B2W Group is committed to bringing the maximum benefits of ICT to its staff and associates, and to equipping them with the knowledge, skills and attitudes that will enable them to thrive in the digital age.

ICT exists within the Company for the primary purpose of supporting all roles and providing vocational training and personal development. ICT assists the Company in discharging these functions and provides staff and associates with an opportunity to become familiar with ICT. However, the company recognises that misuse of ICT can occur. This can be by, for example:

- Accessing or transmitting offensive or unacceptable material
- Accessing or transmitting extremist or radicalising content

Please ensure you have read and understood the following summary of the main points of the organization's policies regarding information security.

3.1 General

You are expected to make yourself familiar with, and follow, the organization's security policies and procedures and any special instructions relating to your work.

Be aware that your use of B2W Group computer and communications systems may be monitored and/or recorded for lawful purposes.

Staff and associates are responsible for their own actions and are thus liable for any consequences thereof. The B2W Group cannot accept responsibility for ensuring that actions of users are acceptable.

You must comply at all times with the legal, statutory or contractual obligations that the organization informs you are relevant to your role.

Access to and use of the company's computing and IT facilities must comply with UK and EU laws.

Whilst we will take steps to monitor use of facilities, we cannot police them absolutely. In all cases the user, or users, concerned will be considered liable for their actions.

3.2 Access Control

You are responsible for the use and protection of the user credentials with which you are provided (user account and password, access token or other items you may be provided with).

Use strong passwords that comply with organization policies and take reasonable precautions to ensure that your passwords are only known by you (for example, not sharing passwords or writing them down).

Don't use the same password (or close variation of the same password) for multiple user accounts.

Never use anyone else's user account and password to access the organization's systems. You must not use privileged user accounts (user accounts with higher-than-normal system access) for business-as-usual activities.

You must not attempt to access any computer system to which you have not been given authorised access.

Never attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.

You must not connect unauthorised devices to the organization network.

3.3 Classified information

Ensure that you label any classified material that you create appropriately according to published guidelines so that it remains appropriately protected.

Always protect any classified material you send, receive, store or process according to the level of classification assigned to it, including both electronic and paper copies.

Don't send classified information over the Internet via email or other methods unless appropriate methods (for example encryption) have been used to protect it from unauthorised access.

Always ensure that you enter, and check that you have entered, the correct recipient email address(es) so that classified information is not compromised.

Take care that you are not overlooked by unauthorised people when working and exercise appropriate precautions when printing classified information. Raise any concerns with your immediate line manager in the first instance.

Securely store classified printed material and ensure it is correctly destroyed when no longer needed.

Never leave your computer unattended such that unauthorised access can be gained to information via your user account while you are away from your workstation.

On leaving the organization, you must inform your manager prior to departure of any important information held in your user account or in a location to which the organization has no, or limited, access.

3.4 Electronic messaging

Electronic messaging covers email and various forms of instant and store-and-forward messaging such as SMS texts, messaging apps, web chats and messaging facilities within social media platforms.

The organization-provided electronic messaging facilities must always be used when communicating with others on official business. You must not use a personal account for this purpose.

All organization messages should be considered to be official communications from the organization and treated accordingly.

You must not send messages containing material, which is defamatory, obscene, does not comply with the organization's equality and diversity policy or which a recipient might otherwise reasonably consider inappropriate. In particular, organization electronic messaging facilities must not be used:

- For the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organizations
- To send material that infringes the copyright or intellectual property rights of another person or organization
- For activities that corrupt or destroy other users' data or otherwise disrupt the work of other users
- To distribute any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- To send anything which is designed or likely to cause annoyance, inconvenience or needless anxiety to others
- To convey abusive, threatening or bullying messages to others
- To transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs
- For the transmission of defamatory material or false claims of a deceptive nature
- For activities that violate the privacy of other users
- To send anonymous messages - i.e. without clear identification of the sender
- For any other activities which bring, or may bring, the organization into disrepute

If you are not sure whether your intended message falls into this category, please consult your line manager before sending.

You should be aware that many information security breaches occur as a result of "phishing", where an email or other type of message is sent which either has a malicious attachment or includes links to websites which are set up to steal information. If you are suspicious about a message, report it by emailing itrequests@b2wgroup.com without opening any attachments or clicking on links, so that the message can be investigated.

3.5 Internet browsing

Your Internet access on organization-owned devices is primarily provided for tasks reasonably related to your work including:

- Access to information and systems that is pertinent to fulfilling the organization's business obligations
- The capability to post updates to organization-owned and/or maintained web sites and social media accounts
- An electronic commerce facility (e.g. purchasing equipment for the organization)
- Research
- Other tasks that are part of your job role

The organization permits personal use of the Internet in your own time (for example during your lunch break), provided it does not interfere with your work. Any exception to this is at the discretion of your line manager.

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must not use the Internet access provided by B2W Group to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files
- Subscribe to, enter or utilise real time chat facilities
- Subscribe to, enter or use online gaming or betting sites
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business
- Download any software that does not comply with the organization's software policy

The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material will include data, images, audio files or video files the transmission of which is illegal and material that is against the rule, essence and spirit of this and other organizational policies.

You must also avoid websites that are flagged by anti-malware or browser software as being potentially unsafe, or which appear suspicious.

If there is a business justification for requiring access to any potentially unsafe or suspicious looking websites you must email itrequests@b2wgroup.com and your request will be reviewed.

3.6 Mobile devices

Mobile devices include items such as laptops, notebooks, tablet devices, smartphones and smart watches.

Unless specifically authorized, only mobile devices provided by the organization may be used to hold or process classified information.

An organization-provided device is for your business use only; it must not be shared with family or friends or used for personal activities.

You must not remove equipment or information from the organization's premises without appropriate approval. ***See Procedure for Taking Assets Offsite***.

You must take precautions to protect all mobile devices and computer media when carrying them outside the organization's premises (for example, not leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft).

The device must not be connected to non-corporate networks such as public Wi-Fi or the Internet unless a VPN (Virtual Private Network) is used. See section **2.7 Working from home for an exception to this rule**.

All information assets should be hosted in Microsoft's Cloud Services SharePoint or OneDrive.

Anti-virus software is updated directly by the vendor when the device is connected to the internet.

Do not remove any identifying marks on the device such as a company asset tag or serial number. Ensure that the device is locked away when being stored and that the key is not easily accessible.

Do not add peripheral hardware to the device without approval.

Permission must be obtained before the device is taken out of the country. This is to ensure that it will work and to consider any insurance implications.

Where possible, the device will be secured so that all of the data on it is encrypted and so is only accessible if the password is known. If the device is supplied with encryption, do not disable it. Where corporate data becomes stored on a mobile device, a central policy script will run to move the data into the account's OneDrive, where it will be cloud hosted and safely stored and backed up, in line with the backup policy.

3.7 Working from home

A homeworking (also called teleworking or simply working from home) arrangement is a voluntary agreement (unless subject to government guidance such as on the basis of public health) between the organization and the employee. It usually involves the employee working from home in a separate area of their living accommodation, whether this is a house, apartment or other type of domestic residence.
Before a homeworking arrangement can be put in place it must be agreed by both the organization and the employee and an initial risk assessment carried out, considering the proposed work environment and nature of the tasks to be performed as part of the job role.

When working from home, you must ensure that the controls specified by the risk assessment (such as physical security and use of organization-provided communications) are complied with at all times.

It is the employee's responsibility to ensure their home network is secure, with the home router admin password changed from the factory default setting, and fully up to date. B2W Group reserves the right to cancel any homeworking agreement if it feels that security is below the standard expected or required.

3.8 Privacy and compliance

B2W Group has a legal obligation to comply with all applicable legislation affecting its business operations, and every employee must play their part in meeting these requirements, in areas such as data privacy, intellectual property, and governance.

You must ensure that you follow organization policies and rules for the processing of personal data at all times.

Take care to understand the rules surrounding the use of the intellectual property of others, such as software, videos, music, books, documentation, photographs and logos so that copyright and other protections are not infringed.

Ensure that the intellectual property of B2W Group is protected when dealing with third parties.

3.9 Cloud computing

B2W Group makes extensive use of cloud services to enable business processes in a responsive and flexible way. These services are subject to a due diligence procedure to ensure that they meet our business, security and legal requirements.

As part of your job role, you must only make use of cloud services that have been put in place by B2W Group. The storing of classified information in unapproved cloud services is strictly prohibited.

3.10 Use of social media

B2W Group makes extensive use of social media to communicate directly with our customers as part of our marketing activity, to provide support for our products and services, and to obtain useful feedback on how our organization is perceived.

You must be authorised to use corporate social media accounts and to represent the organization to the general public, and only if that is part of your job role.

Only authorised accounts should be used to publish messages and respond to other users of relevant social media channels. Do not use your own personal accounts.
B2W Group respects your personal online activity as a medium of self-expression, but remember you continue to have responsibilities to the organization outside of working hours.

When using social media to engage on matters relevant to B2W Group, make it clear it is your own opinion you are expressing and not that of the organization.

3.11 Information security incidents

If you detect, suspect or witness an incident that may be a breach of security, or if you observe any suspected information security weaknesses in systems or services, you should in the first instance inform your line manager, or contact the IT Team.

Unusual or unexplained events, such as messages appearing on your device, can indicate that an incident is happening, and these should be reported as soon as possible.

If an incident is detected by B2W Group, you may be asked to take specific action, such as logging off systems or closing your device down. You should comply with such requests as soon as possible.

3.12 Malware protection

Your device will be protected by organization-supplied anti-malware software.
You must not attempt to disable anti-malware protection provided to protect your device.
You must take care not to introduce viruses or other malware into the system or network, for example by inserting unknown peripherals or media into your device.

3.13 Usage – Computer and Digital Facilities

When using B2W Group's computing and ICT facilities users must not:

- Alter any settings
- Allow other people to use their account
- Give their password to someone else to use and/or disclose their password to someone else, and/or be otherwise careless with their password
- Disrupt the work of other people
- Corrupt or destroy other people's data
- Violate the privacy of other people
- Offend, harass or bully other people

- Break the law
- Waste employee effort or resources
- Store files not related to their own work on B2W Group's computing resources
- Engage in software piracy (including infringement of software licenses, or copyright provisions)
- Generate messages which appear to originate from someone else, or otherwise attempt to impersonate someone else
- Physically damage or otherwise interfere with computing facilities, including attaching any unapproved hardware
- Waste computing resources by playing games or using software which is not needed for work or study
- Engage in any activity which is rude, offensive or illegal
- Use the ICT facilities to draw people into terrorism and/or extremism
- Download and/or run programs or other executable software from the internet or knowingly introduce viruses or other harmful programs or files
- Enable unauthorised third-party access to the system
- Use the ICT facilities for commercial gain without the explicit permission of the Managing Director
- Engage in any activity that denies service to other people or brings the company into disrepute

4 Enforcement

In the event of a known or suspected breach of policy, the company may take immediate action to ensure both the security and accessibility of its computing and ICT resources. Breaches of the Acceptable Use Policy will be dealt with according to their severity.

Incidents which are deemed to be in contravention of this policy will be assessed for their severity and as a result may lead to formal disciplinary action. In extreme circumstances, the Police may be called. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

Action may consist of (but is not limited to) warnings; suspension or removal of user access to computing and ICT resources, including (but not limited to) services such as Email, and/or internet access; and suspension or termination of the user's account. Immediate action does not constitute any judgement of guilt, and appeals may be made.

Employees that identify a suspected breach of the Acceptable Use Policy are responsible for reporting the incident immediately to their line manager in the first instance, and preserving any evidence.

Upon receipt of a reported suspected breach of policy, an investigation will be carried out, in confidence, and the findings will be considered in accordance with the company's Disciplinary Policy and Procedures.

4.1 Appeals

All users are entitled to the right of appeal and any user wishing to appeal must write to the Managing Director stating the basis for the appeal.