Acceptable Use of IT Systems Policy

Document title	Acceptable Use of IT Systems Policy		
Reference No.	POL	**Version**	0.3
Author	Luke Muscat, Managing Director		
Reviewed by	Ben Waite		
Authorised by	Alison Dann, Director of Quality and Performance		
Issue date	01.04.2020		

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 Due for Review on: 01.04.2021	01.04.20

Acceptable Use of IT Systems Policy

1. General

1.1. 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.

1.2. ICT exists within the Company for the primary purpose of supporting our role in providing vocational training and assessment. ICT assists the company in discharging these functions and provides learners, 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

1.2.1. accessing or transmitting offensive or unacceptable material

1.2.2. accessing or transmitting extremist or radicalising content

2. Scope

2.1. This policy applies to all users of The B2W Group's ICT facilities and in relation to IT facilities owned, leased, hired or otherwise provided by the company, as well as those connected directly or remotely to the Company's network or IT facilities.

2.2. It also covers any personal equipment used on our premises, or individuals connecting their own equipment to our network i.e. personal laptops connecting wirelessly to the internet. ICT facilities include all networks, computer systems and/or computing hardware and software made available by the company.

3. Roles and Responsibilities

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

4. Policy Implementation – Auditing and Privacy

4.1. The company reserves the right to:

4.1.1. Conduct checks on internet usage, user files stored on the shared and cloud drives, company owned or leased computers, and their usage, where such action is justified for the purposes of system administration, investigation of suspected breaches of the Acceptable Use Policy, to comply with Prevent Duty, or any other lawful purposes.

4.1.2. Compress, archive, or delete files stored on computing and IT resources, such as shared drive, company cloud storage or the hard drives of company owned or leased computers, by existing or past users.

4.1.3. Access, and, where necessary, to examine the content of user files held on any Company computing and IT resources, private computers connected to the Company network, or otherwise downloaded onto personal computers, discs or separate drives for the purposes of investigating suspected breaches of the Acceptable Use Policy, or other lawful purposes.

4.1.4. Monitor use of company Wi-Fi by any device including but not limited to computers, laptops, smart phones, tablets, notebooks for the purposes of investigating suspected breaches of the Acceptable Use Policy, or other lawful purposes including Prevent.

4.1.5. Log and retain records of all electronic communications (web browsing activities, email exchange etc.) between users of company ICT and computing facilities and all external organisations for a period of no more than 18 months.

4.1.6. Monitor any and all aspects of its telephone and computer system that are made available to staff, learners and visitors, and to monitor, intercept and/or record any communications including telephone, e-mail or Internet communications.

4.1.7. To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice Interception of Communications Regulations 2000), employees, learners and visitors are hereby required to expressly consent to the company doing so.

5. Policy Implementation – Breaches of Policy

5.1. The list below provides examples of potential ways in which a user may contravene this policy. This list is not exclusive or exhaustive and there may be other matters of a similar nature which would be considered as a breach of this policy. The consequences of the breach will depend on the level of severity:

5.1.1. Playing computer games

5.1.2. Sending nuisance (non-offensive) email

5.1.3. Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area

5.1.4. Assisting or encouraging unauthorised access

5.1.5. Sending abusive, harassing, offensive or intimidating email

5.1.6. Maligning, defaming, slandering or libelling another person

5.1.7. Misuse of software or software licence infringement

5.1.8. Copyright infringement

5.1.9. Interference with workstation or computer configuration

5.1.10. Theft, vandalism or wilful damage of/to IT facilities, services and resources

5.1.11. Forging email. i.e. masquerading as another person

5.1.12. Loading, viewing, storing or distributing pornographic or other offensive material

5.1.13. Unauthorised copying, storage or distribution of software

5.1.14. Any action, whilst using the Company's computing services and facilities deemed likely to bring the Company into disrepute

5.1.15. Attempting unauthorised access to a remote system

5.1.16. Attempting to jeopardise, damage circumvent or destroy IT systems security at the Company

5.1.17. Attempting to modify, damage or destroy another authorised user's data

5.1.18. Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities

5.1.19. Attempting to use the company's ICT facilities, systems and resources to draw people into acts of terrorism or extremism or promoting terrorism/extremism.

6. Security of Data

6.1. The Company will endeavour to take reasonable care to ensure that users' data is safe and secure, however this is done in good faith, and no responsibility can be taken for any loss or damage howsoever caused. Facilities are provided "as-is" without any warranty or guarantee of suitability for any purpose, implied or otherwise.

6.2. The company requires all users to store and backup their own work onto the supplied cloud portals.

7. Enforcement

7.1. 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.

7.2. 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.

7.3. 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 e-mail 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.

7.4. Employees that identify a suspected breach of the Acceptable Use Policy are responsible for reporting the incident immediately to the Managing Director, and preserving any evidence.

7.5. For employees, 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.

8. Appeals

8.1. 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 their appeal.

9. Usage – Company Devices

9.1. Employees, learners and others in receipt of a company owned device should be aware that the device, accessories, software and operating system remain the property of the company and are provided on a loan basis only. Additional software MUST NOT be installed, nor hardware modifications made, without authorisation from the Managing Director or Department Manager.

9.2. 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, learners and Associates are responsible for exercising good judgement regarding the reasonableness of personal use.

9.3. Learners issued with laptops to help them with their studies are not permitted to take the laptop home without the express permission of the Managing Director. All devices must be returned at the end of to the tutor facilitating the session.

10. Usage – Social Networking

10.1. Access to social networking sites has the potential to use significant IT resources at key times of the day and deny access to other users. The company reserves the right to limit access to these sites (e.g. Facebook) from company owned device.

10.2. B2W recognise the educational potential of mobile technology and the use of social media is recognised, and their safe use is encouraged and developed where possible.

11. Usage – Computer and Digital Facilities

11.1. When using The Company's computing and ICT facilities users must not:

11.1.1. Alter any settings

11.1.2. Allow other people to use their account

11.1.3. Give their password to someone else to use, and/or disclose their password to someone else, and/or be otherwise careless with their password (N.B. personal passwords should be changed regularly)

11.1.4. Disrupt the work of other people

11.1.5. Corrupt or destroy other peoples' data

11.1.6. Violate the privacy of other people

11.1.7. Offend, harass or bully other people

11.1.8. Break the law

11.1.9. Waste employee effort or resources,

11.1.10. Store files not related to their or work at the Company's computing resources,

11.1.11. Engage in software piracy (including infringement of software licences or copyright provisions)

11.1.12. Generate messages which appear to originate with someone else, or otherwise attempting to impersonate someone else

11.1.13. Physically damage or otherwise interfere with computing facilities, including attaching any un-approved hardware

11.1.14. Waste computing resources by playing games or using software which is not needed for studies or work

11.1.15. Engage in any activity which is rude, offensive or illegal

11.1.16. Use the ICT facilities to draw people into terrorism and/or extremism

11.1.17. Download and/or run programs or other executable software from the Internet or knowingly introduce viruses or other harmful programmes or files

11.1.18. Enable unauthorised third party access to the system

11.1.19. Use the ICT facilities for commercial gain without the explicit permission of the Managing Director

11.1.20. Engage in any activity that denies service to other people or brings the Company into disrepute

12. Company Provided Mobile Phones – Telephony System

12.1. The Company acknowledges that from time to time employees or learners may need to make personal calls, this is permissible with permission from a Director or Manager. All telephone calls are logged and checked on a regular basis.

12.2. Employees with company provided mobile telephones must remember the phone is for company's business use only and keep personal calls to a minimum. Employees will be obliged to reimburse the company for excessive private calls made on a phone, when requested to do so.

12.3. The Company does not allow any members of staff to use mobile telephones when driving on company business without a hands-free kit. An employee who fails to comply with these procedures may be subject to the Disciplinary Procedure.

12.4. All company mobile telephones must use passcode, PIN or pattern lock protection at all times to ensure security of the data held upon the device.

13. Employee Laptops

13.1. When issued with a company loan laptop, employees will be required to agree to a number of insurance conditions which will include:

13.1.1. The laptop will at no time be left in a visible position in any unattended, unlocked vehicle but will be placed in the locked boot of a vehicle

13.1.2. The laptop will only be kept at the Company's premises, a private residence or a locked hotel bedroom when away on company business, but will not be taken on a private holiday

13.1.3. Any room in which the laptop is kept will be secured when unoccupied

13.1.4. Agreement to make the laptop available for inspection by directors or managers at any time

13.1.5. Agreement to inform the company immediately if the laptop is lost, stolen or damaged

13.1.6. Agreement to return the laptop to the employee's line manager on their last day of service with the company,

13.1.7. Accept responsibility for any damages caused by neglect, misuse etc. excluding reasonable wear and tear,

13.1.8. Accept responsibility for the cost of repair/replacement of the laptop in the event of a breach of the above conditions.

14. Legal Conformity

14.1. Some of the UK legislation applicable to computer use is listed below. This is by no means an exhaustive list and users are reminded of their responsibility to be aware of their legal obligations.

14.1.1. Obscene Publications Act 1959

14.1.2. Sex Discrimination Act 1995

14.1.3. Race Relations Act 1976

14.1.4. Protection of Children Act 1978

14.1.5. Data Protection Act 2018

14.1.6. Telecommunications Act 1984

14.1.7. Interception of Communications Act 1985

14.1.8. Copyright, Designs, Patents Act 1988

14.1.9. Computer Misuse Act 1990

14.1.10. Criminal Justice and Public Order Act 1994

14.1.11. Defamation Act 1996

14.1.12. Disability Discrimination Act 1998

14.1.13. Data Protection Act 1998

14.1.14. Human Rights Act 1999

14.1.15. Regulation of Investigatory Powers Act 2000

14.1.16. Malicious Communications Act 1988

14.1.17. Counter-Terrorism and Security Act 2015