



## Library and IT Suite – Acceptable Use Policy

### Introduction

The Acceptable Use Policy (AUP) for IT Systems is designed to protect Bodywork Company, our staff, students, and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infections (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works and studies at Bodywork Company is responsible for the security of our IT systems and the data on them. As such, all employees and students must ensure they adhere to the guidelines in this policy at all times. Should any employee or student be unclear on the policy or how it impacts their role they should speak to the Course Leaders, Line Manager or IT security officer.

### Definitions

‘Users’ are everyone who has access to any of Bodywork Company’s IT systems. This includes permanent employees and also temporary employees, students, contractors, agencies, consultants, suppliers, customers and business partners.

‘Systems’ means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party, networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

### Scope

This is a universal policy that applies to all Users and Systems.

This policy covers only internal use of Bodywork Company’s systems, and does not cover use of our products or services by our customers or other third parties.





Some aspects of this policy affect areas governed by local legislation in certain countries (e.g. employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

Staff members at Bodywork Company who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

### *Use of IT Systems*

All data stored on Bodywork Company's system is the property of Bodywork Company. Users should be aware that the company cannot guarantee the confidentiality of information stored on any Bodywork Company system except where required to do so by local laws.

Bodywork Company's systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users own or their colleague's productivity and nor should it result in any direct costs to Bodywork Company other than for trivial amounts (e.g. an occasional short phone call).

Bodywork Company trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain they should consult their manager.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent, or risk preventing, legitimate access by all properly authorised parties.

Bodywork Company can monitor that use of its IT systems and the data of it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

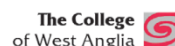
Bodywork Company reserves the right to regularly audit networks and systems to ensure compliance with this policy,

### *Data Security*

If data on Bodywork Company's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorised access to confidential information.

Bodywork Company Dance Studios, 25-29 Glisson Road, Cambridge CB1 2HA

Telephone: 01223 314461 • Email: [admin@bodyworkds.co.uk](mailto:admin@bodyworkds.co.uk) • Web: [www.bodyworkcompany.co.uk](http://www.bodyworkcompany.co.uk)





Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-Bodywork Company system any information that is designated as confidential, or that they should reasonably regard as being confidential to Bodywork Company, except where explicitly authorised to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users who are supplied with computer equipment by Bodywork Company are responsible for the safety and care of that equipment, and the security of software and data stored it and on other Bodywork Company systems that they can access remotely using it.

Information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, therefore special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft or of disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All worktops (desktops and laptops) should be secured with a lock-on-idle policy active after, at most, 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g. viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Bodywork Company's systems by whatever means and must report any actual or suspected malware infection immediately.

### *Unacceptable Use*

All employees and students should use their own judgement regarding what is unacceptable use of Bodywork Company's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

Bodywork Company Dance Studios, 25-29 Glisson Road, Cambridge CB1 2HA

Telephone: 01223 314461 • Email: [admin@bodyworkds.co.uk](mailto:admin@bodyworkds.co.uk) • Web: [www.bodyworkcompany.co.uk](http://www.bodyworkcompany.co.uk)





- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of Bodywork Company. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation for the company.
- All activities for personal benefit only that have a negative impact on the day-to-day functioning on the business. These include activities that slow down the computer network (e.g. streaming video, playing networked video games).
- All activities that are inappropriate for Bodywork Company to be associated with and/or are detrimental to the company's reputation. This includes but is not limited to, pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the IT security systems and protocols which Bodywork Company has put in place.

### *Enforcement*

Bodywork Company will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgement regarding acceptable use. While each situation will be judged on a case-by-case basis, employees and students should be aware that consequences may include the termination of their employment or tuition.

Use of any of Bodywork Company's resources for any illegal activity will usually be grounds for summary dismissal, and Bodywork Company will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Bodywork Company Dance Studios, 25-29 Glisson Road, Cambridge CB1 2HA

Telephone: 01223 314461 • Email: [admin@bodyworkds.co.uk](mailto:admin@bodyworkds.co.uk) • Web: [www.bodyworkcompany.co.uk](http://www.bodyworkcompany.co.uk)

