Acceptable Use Policy for IT Systems

1. Introduction

This Acceptable Use Policy (AUP) for IT systems is designed to protect The Friends of Castle Green and all customers and other partners- from harm caused by the misuse of out IT systems, equipment and data. Misuse includes both deliberate and inadvertent actions.

Everybody who uses this building – The Castle Green Pavilion – is responsible for the security of our IT system and all data. So everyone is required to adhere to the guidelines in this policy at all times. If anybody is unclear about any detail or how this policy impacts on their role it is their duty to check and be safe.

2. Definitions

“Users” are everyone who has access to any of The Friends of Castle Green IT systems. This includes all users of the building as well as : agencies, volunteers, suppliers, partners.

“Systems” means all IT equipment that is in use in the building. 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.

3. Scope

This is a universal policy that applies to all Users and all Systems. It does not cover use of our products or services by customers or other third parties – for example people who use the website, or rent stalls.

4.Use of IT systems

All data stored on The Friends of Castle Green system is the property of FoCG. Users should be aware that we are not able to guarantee the confidentiality of information stored on any system except where required to do so by law.

FoCG systems exist to support and enable the business of the building. A small amount of personal use is allowed. However it must not be detrimental to the work being carried out or to any user. It should also not result in any direct costs being borne by FoCG unless authorized and agreed at committee level.

FoCG trusts all users to be fair and sensible when judging what constitutes acceptable level of personal use, if in any doubt please ask. This covers printing, looking up information as well as all use of equipment.
FoCG will ensure that any information that is sensitive will be stored safely with limited access.
FoCG can monitor the use of its IT systems and the data on it at any time. This can include emails and the history of use and any user.
Some sites accessible via the Internet may contain material that is inaccurate, defamatory, illegal or offensive to some people. FoCG complies with CEOP guidelines and policies protection children and young people. We also update our e-safety advice from http://www.thinkuknow.co.uk/.
We are not responsible for any objectionable material viewed by a child or young person whether intentionally or by accident.
The IT equipment is available to be booked by groups or individuals.
A printing service is also available on request.

5. Data Security

If data on FoCG's systems is classified as confidential this will be clearly indicated with in the data. We will take all necessary steps to prevent unauthorized access to confidential information.
Users are expected to exercise reasonable personal judgment when deciding which information is confidential.
Users must not send, upload, remove on portable media or any other device or in any way transfer to a non – FoCG system, any information that is designated as confidential or they reasonably decide is confidential, except where they are explicitly authorized to so in the performance of their regular duties.
Users must keep passwords secure and not allow other people access to their account.
Any user who is supplied with a piece of FoCG equipment is responsible for the care and safety of that piece of equipment as well as the security of any data stored on it or any other system they can access remotely.
Because information on portable devices such as tablets and laptops is especially vulnerable, special care should be taken with these devices. All sensitive information should be stored in encrypted folders. Users will be held responsible for the consequences of theft or disclosure of information on any portable system, if they have not taken reasonable precautions to secure it.
All laptops, iPads will be protected with a lock-on-idle policy active after at most 10 minutes of inactivity. The user will not leave the machine unattended. All Users who have been charged with the management of those systems are responsible for ensuring they are at all times properly protected against unknown threats and vulnerabilities as far as is possible.
Anybody who detects any malware infection or is suspicious, must notify a committee member or person in charge immediately.
Nothing is to be saved to a computer by a user renting equipment that they would want to return to at a later date.

6. Unacceptable Use

The activities listed are provided as examples of unacceptable use, however it is not exhaustive.

- All illegal activities – including theft, computer hacking, contravening copyrights and patents, using illegal software, malware distribution and anything that contravenes data protection regulations.

- All activities detrimental to the success of FoCG.
- All activities for personal benefit that will have a negative impact on the day-to – day business.
- All activities that are inappropriate for FoCG to be associated with and might be detrimental to our reputation.
- Circumventing the IT security systems we have put in place
- Harassing any individual via the internet.

7. Enforcement

FoCG will not tolerate any misuse of its systems or equipment. While each situation will be judged on a case–by-case basis all users must note consequences might include referring the matter to the police or a termination of their contract/ arrangement.